DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") forms part of the Agreement between 1) Hitachi Energy for itself and for the benefit of any Hitachi Energy Affiliate and 2) the Customer.

- Agreement: means the main agreement under which the Processor provides services to the Controller and of which this DPA becomes part.

- Hitachi Energy: means the Hitachi Energy contracting entity providing services to Customer under the Agreement and processing Personal Data on behalf of Customer.

Parties agree that this DPA sets forth their obligations with respect to the processing and security of Personal Data in connection with the services that Hitachi Energy provides in a capacity as Processor in accordance with the Agreement.

In the event of any conflict or inconsistency between this DPA and the Agreement, this DPA shall prevail.

SECTION I

Clause 1 Definitions

a) "Controller" means the entity, which alone or jointly with others, determines the means and purposes of the processing of the Personal Data;
b) "Data subject": an identified or identifiable natural person.
c) "Personal Data" means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
d) "Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
e) "Processor" means the entity which processes Personal Data on behalf of the controller.

SECTION II

OBLIGATIONS OF THE PARTIES

Clause 2 Description of processing(s)

The details of the processing operations, in particular the categories of Personal Data and the purposes of processing for which the Personal Data is processed on behalf of the controller, are specified in Annex II.

3.1. Instructions

(a) The processor shall process Personal Data only on documented instructions from the controller. Subsequent instructions may also be given by the controller throughout the duration of the processing of Personal Data. These instructions shall always be documented and the parties shall comply with the change control procedures as described in the relevant SOW

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe applicable data protection legislation.

3.2. Purpose limitation

The processor shall process the Personal Data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

3.3. Duration of the processing of Personal Data

Processing by the processor shall only take place for the duration specified in Annex II.

3.4. Security of processing

(a) The processor shall at least implement the technical and organizational measures specified in Annex III to ensure the security of the Personal Data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to the data (Personal Data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the Personal Data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the Agreement. The processor shall ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.5. Sensitive data

If the processing involves Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

3.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with this DPA.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of Personal Data in accordance with this DPA.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in this DPA and applicable data protection legislation. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by this DPA, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

Audit(s) will be carried out during normal business hours without disruption of Hitachi Energy' business operations, taking into account a reasonable lead time, which shall in no case be less than thirty (30) days unless there is an urgent need for an earlier audit. Hitachi Energy may make the audit conditional upon the signing of a confidentiality agreement with regard to the data of other customers and the technical and organizational measures set up. Customer may not appoint a third party auditor that is in a competitive relationship with Hitachi Energy. Customer will not exercise its audit rights more than once in any twelve (12) month period, except (i) if and when required by instruction of a competent data protection authority or other

regulator with jurisdiction over Customer; or (ii) Customer believes a further audit is necessary due to a breach or suspected breach of security suffered by Hitachi Energy. Hitachi Energy may claim remuneration for its efforts when enabling Customer's audits according to the then current rates of Hitachi Energy on a time and material basis.

3.7. Use of sub-processors

(a) The processor has the controller's general authorization for the engagement of the sub-processors listed in Annex IV. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 7 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object. The obligation to inform controller of any changes is not applicable to the use of Hitachi Energy Affiliates that are involved in the provision of the Services and the Professional Services.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with this DPA. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to applicable data protection legislation.

(c) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

Clause 4 Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorized to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 4(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of Personal Data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that Personal Data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the Personal Data it is processing is inaccurate or has become outdated;

Clause 5 Notification of Personal Data breach

5.1 Data breach concerning data processed by the controller

In the event of a Personal Data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the Personal Data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the Personal Data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information:

(1) the nature of the Personal Data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;

(2) the likely consequences of the Personal Data breach;

(3) the measures taken or proposed to be taken by the controller to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying with communicating the Personal Data breach to the data subject, when the Personal Data breach is likely to result in a high risk to the rights and freedoms of natural persons.

5.2 Data breach concerning data processed by the processor

In the event of a Personal Data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor became aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the Personal Data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

6. California Consumer Privacy Act (CCPA)

If Hitachi Energy is processing personal data within the scope of the California Consumer Privacy Act (CCPA), 1) Hitachi Energy acts as a CCPA Service Provider and 2) Hitachi Energy makes the following additional commitments to Customer: Hitachi Energy will not retain, use, or disclose that data for any purpose other than for the purposes set out in this DPA and as permitted under the CCPA, including under any “sale” exemption. In no event will Hitachi Energy sell any such data. These CCPA terms do not limit or reduce any data protection commitments Hitachi Energy make in this DPA or the Agreement.

SECTION III

FINAL PROVISIONS

Clause 7 Non-compliance with this DPA and termination

(a) In the event that the processor is in breach of its obligations under this DPA, the controller may instruct the processor to suspend the processing of Personal Data until the latter complies with this DPA or the Agreement is terminated. The processor shall promptly inform the controller in case it is unable to comply with this DPA, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of Personal Data in accordance with this DPA if:

(1) the processing of Personal Data by the processor has been suspended by the controller pursuant to point (a) and if compliance with this DPA is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of this DPA;

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of Personal Data under this DPA where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with clause 3.1 (b) of this DPA, the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all Personal Data processed on behalf of the controller and confirm to the controller that it has done so, or, return all the Personal Data to the controller and delete existing copies unless applicable law requires storage of the Personal Data. Until the data is deleted or returned, the processor shall continue to ensure compliance with this DPA.

Clause 8 Limitation of liability

(a) Subject to clause (b) below, Processor shall be liable for damage caused by its processing of personal data under this DPA only where it has acted outside or contrary to lawful instructions of the Controller or Processor's obligations under this DPA or the Agreement.

(b) This DPA shall be subject to the exclusions and limitations of liability agreed between the Controller and the Processor in the Agreement. The limitation on Processor's liability shall apply in aggregate for all claims under both the Agreement and this DPA.

APPENDIX

ANNEX I

A) LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s):

Name, address and contact details: the Customer, and Customer's details, as defined in the Agreement

Activities relevant to the data transferred under these Clauses: to receive the Services and Professional Services as set out in the Agreement

Effective date: as mentioned in the Agreement

Role: Controller

Data importer(s):

The Hitachi Energy entity as defined in the Agreement.

Contact person's name, position and contact details:

- For matters related to the provision of Services and Professional Services:

  ch-contract_administration_emea.pges@hitachienergy.com

- For data protection matters: privacy@hitachienergy.com

Activities relevant to the data transferred under these Clauses: to provide the Services and the Professional Services to Customer as set out in the Agreement.

Effective date: as mentioned in the Agreement

Role: Processor

B. DESCRIPTION OF TRANSFER

	Lumada APM	Lumada EAM	Lumada FSM	nMarket I-SEM	TRM Tracker
Categories of data subjects whose personal data is transferred **Note: each category includes current, past and prospective data subjects. Where any of the following is itself a business or organisation, it includes their staff.**					
Customer's users	X	X	X	X	X
Customer's prospects, customers, business partners and/or vendors	X	X	X	X	X
Categories of personal data transferred					
Personal data for Customer and Agreement account management					
First- and last name	X	X	X	X	X
Company	X	X	X	X	X
Role / position	X	X	X	X	X
Business address	X	X	X	X	X
Email address	X	X	X	X	X
Phone number	X	X	X	X	X
Personal data to register an individual as user of the Software and to assign access rights					
First- and last name		X	X		X
Employer			X		
Role / position		X	X		X
Business address		X	X		
Email address		X	X		
Unique identifier	X	X	X	X	
Login credentials		X		X	X
IP address	X				X
Information regarding access to and use of the Software	X	X	X	X	X
Debug logs			X		X
Personal data that can reside in the Software (when populated by the Customer)					
Employee status (employee, contractor / active, non-active etc.)			X		
Professional qualifications			X		
Skillsets used to assign work (f.e. meter reader vs. lineman)		X	X		
Home address			X		
Home phone number			X		
Contact details			X		
Start location for work assignments			X		
The location where a user is assigned to work			X		
Precise geolocation data (f.e. GPS vehicle tracking) of the employee			X		
Job statuses (f.e. enroute to a job, arrived on site, unavailable to receive new work, suspended an order, tech in emergency, Job-on/ Job-off, acknowledged a new emergency work order etc.)			X		

Timekeeping history (days and times worked)			X		
Travel and expense reports			X		
Employee absences and leave requests			X		
Training attendances			X		
Safety events			X		
Safety checklists (to be) completed			X		
Sensitive data transferred					
	n/a	n/a	n/a	n/a	n/a
Frequency of the transfer and further processing					
Personal data is processed / transferred on a continuous basis during the term of the Agreement.					
Nature and Purpose(s) of the data transfer and further processing					
Customer and Agreement account management					
Contract management	X	X	X	X	X
Responding to Customer questions, queries and support requests	X	X	X	X	X
Register an individual as user of the Software and to assign access rights					
	X	X	X	X	X
Providing the software and support/maintenance					
Hosting	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement
Data migration	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement
Functional testing	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement
Performance testing	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement
Providing (remote or on-site) support and maintenance	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period					
Hitachi Energy will return Customer Data (including personal data) upon Customer request within 30 days after termination or expiration of the Agreement. Hitachi Energy will have no obligation to maintain or return Customer Data after such 30-day period, and Hitachi Energy will thereafter delete or destroy all copies of Customer Data in its control, unless legally prohibited.					
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing					
Microsoft Azure For Hosting & infrastructure purposes Duration: for the term of the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement

	Asset Suite	Ellipse	ERSuite	Service Suite	eSOMS
Customer's users	X	X	X	X	X
Customer's prospects, customers, business partners and/or vendors	X	X	X	X	X
Categories of personal data transferred					
Personal data for Customer and Agreement account management					
First- and last name	X	X	X	X	X
Company	X	X	X	X	X
Role / position	X	X	X	X	X
Business address	X	X	X	X	X
Email address	X	X	X	X	X
Phone number	X	X	X	X	X
Personal data to register an individual as user of the Software and to assign access rights					
First- and last name	X	X	X	X	X
Employer	X	X			
Role / position	X	X	X	X	X
Business address	X	X		X	
Email address	X	X	X		
Unique identifier	X	X	X	X	X
Login credentials	X	X		X	X
IP address			X		
Information regarding access to and use of the Software	X	X	X	X	
Debug logs	X	X		X	X
Personal data that can reside in the Software (when populated by the Customer)					
Employee status (employee, contractor / active, non-active etc.)	X	X		X	
Employee start- and end date with the company	X	X		X	
Seniority date	X				
Date of birth	X	X			
Country of birth		X			
Sex	X	X			
Nationality		X			
Citizenship		X			
Marital status		X			
Disability		X			
Ethnicity		X			
Veteran status		X			
Smoker		X			
Professional qualifications	X	X		X	X
Skillsets used to assign work (f.e. meter reader vs. lineman)	X	X		X	X
Training exam scores	X	X			X
Home address	X	X			
Home phone number	X	X			
Contact details	X	X		X	

Emergency contact information		X			
Dependents information		X			
Employee photo		X			
Salary / pay slip details		X			
Hourly rate	X	X			
Benefits information		X			
Personal bank account number	X	X			
Social Security Number	X	X			
National identification number	X	X			
Travel Docs (Passport and Visa)		X			
Start location for work assignments		X		X	
The location where a user is assigned to work	X	X		X	
Precise geolocation data (f.e. GPS vehicle tracking) of the employee				X	
Job statuses (f.e. enroute to a job, arrived on site, unavailable to receive new work, suspended an order, tech in emergency, Job-on/ Job-off, acknowledged a new emergency work order etc.)		X		X	
Timekeeping history (days and times worked)	X	X		X	
Employee absences and leave requests	X	X		X	X
Training attendances	X	X		X	X
Safety events	X			X	X
Safety checklists (to be) completed	X				
Radiation exposure measurements	X				
Medical and rehabilitation data		X			
Medical review date	X	X			
Performance appraisals		X			
Recruitment history		X			
Workers compensation claims		X			
Sensitive data transferred					
Data concerning health	X	X			

Data revealing ethnic origin		X			
Personal data is processed / transferred on a continuous basis during the term of the Agreement.					
Nature and Purpose(s) of the data transfer and further processing					
Customer and Agreement account management					
Contract management	X	X	X	X	X
Responding to Customer questions, queries and support requests	X	X	X	X	X
Register an individual as user of the Software and to assign access rights					
	X	X	X	X	X
Providing the software and support/maintenance					
Hosting	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement
Data migration	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement
Functional testing	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement
Performance testing	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement
Providing (remote or on-site) support and maintenance	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement	To the extent set out in the Agreement
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period					
Hitachi Energy will return Customer Data (including personal data) upon Customer request within 30 days after termination or expiration of the Agreement. Hitachi Energy will have no obligation to maintain or return Customer Data after such 30-day period, and Hitachi Energy will thereafter delete or destroy all copies of Customer Data in its control, unless legally prohibited.					
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing					
	n/a	n/a	n/a	n/a	n/a

C. COMPETENT SUPERVISORY AUTHORITY

Autoriteit Persoonsgegevens

Bezuidenhoutseweg 30

2594 AV DEN HAAG

The Netherlands

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

- Scenario 1: the SaaS or Software products hosted by Hitachi Energy listed in Annex I.
- Scenario 2: the software products listed in Annex I that are either on Customer's premises or hosted by Customers in their own cloud environment.

For all scenario, Hitachi Energy provides (remote) maintenance and support

Data importer's (Hitachi Energy's) technical and organisational measures – for the 2 scenarios listed above - cover at least the areas below:

	Scenario 1	Scenario 2
Information Security Policies		
Hitachi Energy maintains and follows IT security policies and practices that are integral to Hitachi Energy's business and mandatory for all Hitachi Energy personnel. IT security policies are reviewed periodically and amended if needed.	X	X
Certification		
Hitachi Energy's operations, policies and procedures are audited regularly against relevant internationally recognized and globally applicable standards in the area of cyber- and information security. An overview of Certificates assigned to Hitachi Energy is available via Certificates | Hitachi Energy	X	X
Physical Security Measures		
Hitachi Energy facilities are secured through access control systems	X	n/a
Buildings, individual areas and surrounding premises may be further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and access control systems	X	n/a
Guests and visitors to Hitachi Energy buildings must register their names at reception and must be accompanied by authorized Hitachi Energy personnel	X	n/a
All data center facilities adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and data center facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the data center facilities. To protect proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.	X	n/a
Environmental controls are in place to protect systems inside datacenter facilities, including temperature and heating, ventilation and air conditioning controls, fire detection and suppression systems, and power management	X	n/a
System Access Controls		
Authorization levels are used when granting access to systems storing and processing personal data.	X	X
All personnel access Hitachi Energy's system with a unique identifier (user ID)	X	n/a

In case of termination of an employment contract with Hitachi Energy, access rights are revoked	X	n/a
Hitachi Energy maintains a password security instruction that applies to all IT assets that store, process or transmit information. The instruction sets minimum requirements for password character, password length, password complexity, password history, password storage, password lifetime and a requirement to change default passwords.	X	n/a
Hitachi Energy's network is protected from the public network by firewalls	X	n/a
Hitachi Energy uses up-to-date anti-virus software at access points to the company network (for e-mail accounts), as well as on all file servers and workstations	X	n/a
Security patch management processes are in place to deploy relevant security updates on a regular and periodic basis	X	n/a
Remote access to Hitachi Energy's corporate network is protected by authentication	X	n/a
Data Access Controls		
Access to personal data is granted on a Need to Know and Least Privilege basis. Personnel have access to the information that they require in order to fulfill their duty	X	X
All access to data (including personal data) is logged	X	n/a
Production servers are operated in data centers or in secure server rooms. Security measures that protect applications processing personal data are regularly checked. Hitachi Energy conducts internal and external security checks and/or penetration tests on its IT systems	X	n/a
Hitachi Energy uses the technical capabilities of the deployed software (for example: multi- tenancy, or separate system landscapes) to achieve data separation among personal data originating from multiple customers	X	n/a
Data Exporter has access only to its own data	X	X
Data Transmission Controls		
Hitachi Energy continuously and systematically monitors IT systems, applications and relevant network zones to detect malicious and abnormal network activity by:		
- firewalls	X	n/a
- proxy servers	X	n/a
- Intrusion Detection Systems and/or Intrusion Prevention Systems	X	n/a
- URL Filtering	X	n/a
- Security Information and Event Management (SIEM) systems	X	n/a
Cryptographic controls		
Hitachi Energy uses the 256 AES encryption algorithm for data at rest in its SaaS offerings.	X	n/a
Hitachi Energy uses TLS version 1.2 or 1.3 for data in transit encryption.	X	X
Availability Controls		
Hitachi Energy deploys regular backup processes to provide restoration of business-critical systems as and when necessary. The restoration of data from backups is tested regularly based on the criticality of the IT system or application	X	n/a
Hitachi Energy uses uninterrupted power supplies (for example, UPS, batteries, generators etc.) to protect power availability to the data centers.	X	n/a
Backup storage media will be protected against unauthorized access and environmental threats	X	n/a
Backups are stored in a physical location different from the location where the production system is hosted	X	n/a
Hitachi Energy shall develop and maintain business continuity impact analyses and disaster recovery plans, designed to prevent personal data	X	n/a

loss as well as maintain Hitachi Energy's delivery of the services with minimal interruption		
Operations security		
Hitachi Energy logs security-related events such as user management activities (e.g., creation, deletion), failed logons, changes on the security configuration of the system on IT systems and applications	X	n/a
Hitachi Energy continuously analyzes IT systems and applications log data for anomalies, irregularities, indicators of compromise and other suspicious activities	X	n/a
Hitachi Energy scans and tests IT systems and applications for security vulnerabilities on a regular basis	X	n/a
Hitachi Energy implements and maintains a change management process for IT systems and applications.	X	n/a
Hitachi Energy maintains a process to update and implement vendor security fixes and updates on IT systems and applications	X	n/a
Hitachi Energy irretrievably erases data or physically destroys the data storage media before disposing or reusing of an IT system	X	n/a
Hitachi Energy has processes in place to detect the installation of unapproved software on production systems	X	n/a
Incident Management		
Hitachi Energy will maintain an incident response plan and follow documented incident response policies including personal data breach notification to Data Exporter without undue delay where a personal data breach is known or reasonably suspected to affect Data Exporter's personal data	X	X
Human Resources Security		
Hitachi Energy personnel with access to personal data are bound by confidentiality obligations and the Least Privilege principle.	X	X
Hitachi Energy shall provide appropriate information security awareness and training programs, so that Hitachi Energy personnel understand their security responsibilities	X	X

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

- Hitachi Energy Affiliates that are involved in the provision of the Services and the Professional Services. An overview of Hitachi Energy Affiliates is available here.
- Microsoft Corporation (Microsoft Azure) for the provision of hosting & infrastructure services.