ENERZYZ

Autopilot for Energy Assets

DATA PROCESSING AGREEMENT

Global Data Protection & Cross-Border Transfer Terms

This Data Processing Agreement ("DPA") forms part of, and is incorporated by reference into, the Facility Licence Agreement, Master Subscription Agreement, or other written or electronic agreement between the Customer and Enerzyz governing the Customer's access to and use of the Enerzyz Platform (the "Principal Agreement").

Document reference
ENZ-LEGAL-DPA-001 · Version 3.0 · Global Edition
Effective from the date of the Principal Agreement · Issued June 2026

Contents

Background and Construction

A. Enerzyz operates an AI-native operating system for energy assets (the "Enerzyz Platform" or the "Services") comprising the Enerzyz Edge device and associated hardware (if applicable), the Enerzyz Cloud and console, physics-informed digital twins, predictive machine-learning models, and autonomous optimisation agents that acquire, normalise and analyse equipment telemetry in order to reduce energy waste, extend equipment life and deliver auditable sustainability outcomes.

B. In delivering the Services, Enerzyz Processes data that may, in certain jurisdictions and use cases, include limited categories of Personal Data. This DPA sets out the data-protection terms on which such Processing is conducted and is designed to satisfy the requirements of the data-protection laws of the global markets in which Enerzyz operates.

C. This DPA reflects the architecture of the Services: telemetry originates from the Customer's operational-technology environment, is conveyed over an outbound-only, mutually-authenticated channel to a multi-cloud back end, and is used by Enerzyz to deliver engineering intelligence, optimisation actions and sustainability reporting to the Customer.

D. **Customer ownership of operational data.** As between the parties, the Customer owns its operational data, including Telemetry, and Enerzyz Processes such data as the Customer's Processor for the sole purpose of providing the Services. Enerzyz acts as an independent Controller only for the limited, internally-facing purposes of platform security, platform operations, service monitoring and the generation of de-identified and aggregated analytics, as set out in Section 2. Enerzyz does not assert ownership of, or independent control over, the Customer's operational data.

Order of precedence. In the event of any conflict between this DPA and the Principal Agreement with respect to the Processing of Personal Data, this DPA prevails. In the event of any conflict between this DPA and the Region-Specific Terms in Section 17, the Region-Specific Terms prevail for the relevant jurisdiction. The Standard Contractual Clauses and other transfer mechanisms incorporated under Section 11 prevail over this DPA to the extent of any conflict in respect of the safeguarded transfer.

1. Definitions and Interpretation

Capitalised terms used but not defined in this DPA have the meaning given in the Principal Agreement. The following definitions apply:

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with a party, where "control" means ownership of more than fifty percent (50%) of the voting interests.

"Aggregated Data" means data and statistics that are derived or generated from the Processing of Customer Data, Service Data or Telemetry and that have been aggregated and/or de-identified such that they do not identify, and could not reasonably be used to identify, the Customer or any Data Subject.

"Applicable Data Protection Law" means all laws, regulations and binding regulatory guidance relating to the protection, privacy or security of Personal Data that apply to the Processing under this DPA, including without limitation the regimes identified in Section 17, in each case as amended, replaced or superseded from time to time.

"Controller" means the natural or legal person that, alone or jointly with others, determines the purposes and means of the Processing of Personal Data, and includes an equivalent concept under Applicable Data Protection Law (such as "business" under U.S. State Privacy Laws or "personal information handler" under the PIPL).

“Customer Data” means data, including Telemetry and Customer Account Data, that the Customer or its Authorised Users provide to, or that is collected by the Services from the Customer’s environment, in each case under the Principal Agreement.

“Customer Account Data” means Personal Data relating to the Customer’s Authorised Users that is used to administer accounts, authenticate identities through the Customer’s identity provider, manage role-based access and maintain audit records.

“Data Subject” means an identified or identifiable natural person to whom Personal Data relates.

“Derived Data” means any data, models, model weights, parameters, embeddings, features, inferences, anomaly signatures, baselines, benchmarks, indices, insights, analytics and other outputs that Enerzyz creates, learns or generates through the Processing of Telemetry, Customer Data or Service Data, including the trained state of the Enerzyz machine-learning and physics-informed models. Derived Data does not include Customer Data in its original, unprocessed form.

“Personal Data” means any information relating to an identified or identifiable natural person that is Processed under this DPA, and includes “personal information” and equivalent terms under Applicable Data Protection Law.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data Processed under this DPA.

“Processing” (and “Process”, “Processes”, “Processed”) means any operation performed on Personal Data, whether or not by automated means, including collection, recording, organisation, storage, adaptation, retrieval, use, disclosure, transmission, erasure or destruction.

“Processor” means an entity that Processes Personal Data on behalf of a Controller, and includes a “service provider” under U.S. State Privacy Laws and an “entrusted party” under the PIPL.

“Service Data” means data generated by, or relating to, the provision, security, performance, configuration, billing and operation of the Services, including device, system, diagnostic, log, audit, usage and telemetry-handling metadata.

“Service Insights” means the analytics, predictions, optimisation recommendations, energy and emissions reporting, benchmarks and other intelligence produced by the Enerzyz Platform.

“Sub-processor” means any third party engaged by Enerzyz or an Enerzyz Affiliate to Process Personal Data in connection with the Services.

“Standard Contractual Clauses” or “SCCs” means, as applicable, the standard contractual clauses approved by the European Commission by Implementing Decision (EU) 2021/914 of 4 June 2021, and any equivalent or successor clauses adopted under another Applicable Data Protection Law.

“Telemetry” means the real-time and historical operational data acquired from the Customer’s equipment and environment, including temperatures, pressures, electrical currents, vibration, runtime hours, fuel and resource levels, occupancy signals, weather and tariff data, and equipment state changes.

“U.S. State Privacy Laws” means the California Consumer Privacy Act as amended by the California Privacy Rights Act, together with comparable comprehensive state privacy statutes in the United States, in each case as amended or supplemented.

Interpretation. References to statutes include subordinate legislation and successor provisions. Headings are for convenience only. “Including” means “including without limitation”. The terms “Controller”, “Processor”, “special categories of data” and “supervisory authority” are construed in accordance with the Applicable Data Protection Law of the relevant jurisdiction.

2. Scope, Roles and Allocation of Responsibility

2.1 This DPA applies to the Processing of Personal Data by Enerzyz and its Affiliates in the course of providing the Services to the Customer, and reflects the operational reality that the Enerzyz Platform is engineered to ingest equipment Telemetry rather than personal information.

2.2 **Customer as Controller; Enerzyz as Processor.** In respect of all Customer Data — including Telemetry, operational data and Customer Account Data — the Customer is the Controller and Enerzyz acts as the Customer's Processor. Enerzyz Processes Customer Data only on the Customer's documented instructions and only to the extent necessary to provide, support and secure the Services, and does not determine the purposes of such Processing. The Customer owns its Customer Data, and nothing in this DPA transfers ownership of Customer Data to Enerzyz.

2.3 **Limited independent controllership.** Enerzyz acts as an independent Controller only for the following limited, internally-facing purposes, and only in respect of the data strictly necessary for them:

- **Platform security** — detecting, investigating and preventing security incidents, fraud, abuse and threats to the integrity of the Platform;
- **Platform operations** — operating, maintaining, troubleshooting and ensuring the availability and performance of the Services;
- **Service monitoring** — monitoring usage for capacity, reliability, billing and abuse-prevention purposes; and
- **Internal analytics** — generating de-identified and aggregated analytics that do not identify the Customer, any site or any Data Subject, as further governed by Section 5.

2.4 **No independent use of operational data.** For the avoidance of doubt, Enerzyz does not act as a Controller of, and does not determine its own purposes for, the Customer's operational Telemetry. Enerzyz's limited controllership under Section 2.3 does not entitle Enerzyz to use Customer Data in identifiable form for any purpose beyond providing the Services and the limited purposes listed above.

2.5 Where each party determines its own purposes and means in respect of the same dataset, each party acts as an independent Controller and not as a joint controller. Nothing in this DPA requires either party to Process Personal Data in a manner that infringes Applicable Data Protection Law, and each party is responsible for its own compliance with Applicable Data Protection Law in respect of the Processing for which it is responsible.

2.6 The subject matter, duration, nature and purpose of the Processing, the categories of Personal Data and Data Subjects, and the Processing operations, are set out in Annex I (Details of Processing).

3. Customer Responsibilities and Warranties

3.1 The Customer warrants that it has provided all notices, obtained all consents, and established all lawful bases required under Applicable Data Protection Law for the collection of Telemetry and other Customer Data from its environment and for the disclosure of such data to Enerzyz for the purposes contemplated by this DPA, including any occupancy-sensing or presence-detection data that may relate to identifiable individuals.

3.2 The Customer is responsible for the accuracy, quality and legality of Customer Data and the means by which it acquired such data, and for ensuring that its instructions to Enerzyz comply with Applicable Data Protection Law.

3.3 The Customer shall not configure the Services to ingest special categories of Personal Data, government identifiers, payment-card data, or data relating to children, and acknowledges that the Services are not

designed to Process such data. The Services are not intended to Process patient health records or clinical data, and the Customer shall not route such data to the Services.

3.4 Where the Customer deploys the Services in a regulated environment (including healthcare, hospitality, data-centre or critical-infrastructure facilities), the Customer remains responsible for its sector-specific regulatory obligations, and Enerzyz shall provide reasonable assistance and documentation to support the Customer's compliance.

3.5 Building-system and guest-data boundary. The Services integrate with building management systems (BMS), guest-room management systems (GRMS) and energy assets for the sole purpose of energy and equipment optimisation. Enerzyz ingests only aggregate, zone-level occupancy and presence counts as energy-management telemetry (for example, the number of occupied zones or rooms on a floor used to drive HVAC set-points). Enerzyz does not ingest, store or transmit guest names, room numbers tied to a named individual, check-in or check-out records, reservation or folio data, loyalty identifiers, or any Property Management System (PMS) or GRMS guest-record data, and the Services are not configured to do so. Where a BMS or GRMS exposes such fields, Enerzyz consumes only the energy-relevant signal and excludes guest-identifying attributes at the point of integration.

4. Processing by Enerzyz

4.1 Processor obligations. In respect of Customer Data Processed on the Customer's behalf, Enerzyz shall: (a) Process such data only on the Customer's documented instructions, including with regard to international transfers, unless required to do otherwise by a law to which Enerzyz is subject, in which case Enerzyz shall, where legally permitted, inform the Customer of that legal requirement before Processing; (b) ensure that persons authorised to Process such data are bound by confidentiality obligations; (c) implement the measures set out in Section 8 and Annex II; (d) respect the conditions for engaging Sub-processors in Section 9; (e) assist the Customer, by appropriate measures and taking into account the nature of the Processing, in fulfilling its obligations under Sections 11 to 14; (f) make available information necessary to demonstrate compliance and allow for audits under Section 14; (g) on termination, return or delete such data in accordance with Section 15; and (h) immediately inform the Customer if, in its opinion, an instruction infringes Applicable Data Protection Law.

4.2 Documented instructions. The Customer's complete and final instructions for the Processing of Customer Data are set out in this DPA, the Principal Agreement, and the Customer's configuration of the Services. Enerzyz uses Customer Data only to provide and support the Services and does not use it for its own independent purposes. Additional instructions outside the scope of the Services require prior written agreement and may incur additional charges.

4.3 Limited internal purposes. To the extent permitted by Applicable Data Protection Law, Enerzyz Processes the minimum data necessary for the limited controllership purposes in Section 2.3 — namely platform security, platform operations, service monitoring and the generation of de-identified and aggregated analytics — and for compliance with law. Such Processing does not extend to using Customer Data in identifiable form to develop products for, or to provide services to, any third party. The lawful bases for this limited Processing are set out in Section 7.

5. Customer Data, Service Improvement and Platform Intelligence

5.1 Customer ownership. As between the parties, the Customer owns and retains all right, title and interest in and to the Customer Data, including Telemetry and the operational and energy data of its sites and assets. Enerzyz obtains no ownership of, and only the limited rights to Process, Customer Data necessary to provide the Services and to perform the limited internal functions in Section 2.3.

5.2 Service improvement uses de-identified data only. Enerzyz does not use the Customer's identifiable operational data, Telemetry or Customer Account Data to train or fine-tune its machine-learning or physics-informed models for the benefit of other customers. Where Enerzyz improves the Services and underlying models, it does so using Service Data and de-identified, aggregated data that has been processed so that it does not identify, and cannot reasonably be used to identify, the Customer, any site or any Data Subject. The Customer's identifiable Customer Data is used only to deliver the Services to that Customer.

5.3 Enterprise model-training election (opt-out). In addition, and without prejudice to Section 5.2, an enterprise Customer may elect, by written notice to Enerzyz or through the Platform controls, to exclude its data from contributing to model-improvement activities entirely, including from de-identified and aggregated training datasets. Such an election does not affect the Customer's continued receipt of, or the quality of, the Services. Enerzyz will give effect to the election within a reasonable period and will confirm it in writing.

5.4 Platform Intelligence and IP. As between the parties, Enerzyz and its Affiliates own and retain all right, title and interest in and to the Services and the Platform, including all models, model weights, parameters, methods, algorithms, software, know-how and de-identified Aggregated Data developed or embodied in the Services (collectively, "Platform Intelligence"), together with all intellectual property rights therein. Platform Intelligence comprises only generalised, de-identified learnings and does not include Customer Data. The Customer receives the right to access and use the Service Insights made available to it through the Services during the term of the Principal Agreement.

5.5 Binding customer-protection commitments. Enerzyz commits, as binding undertakings, that:

- Derived Data and Aggregated Data will never be reverse-engineered, re-identified or otherwise processed in a manner that identifies, or could reasonably be used to identify, the Customer, any individual property or site, or any Data Subject;
- no customer-specific operating profile, energy profile, asset-performance profile or other customer-identifiable analytic will be disclosed to any third party;
- Derived Data will not be used to create customer-specific competitive benchmarking, and no benchmark, index or comparative analytic shared externally will single out, or permit the inference of, any individual customer or property; and
- any externally-shared benchmark, index or market insight will be presented only at a multi-property, portfolio or market-segment level, applying recognised aggregation and minimum-cohort thresholds, and will never be attributed to a named or identifiable customer without that customer's prior written consent.

5.6 De-identification standard. Once data has been de-identified or aggregated such that it no longer relates to an identifiable natural person and does not identify the Customer or any site, it ceases to be Customer Data or Personal Data for the purposes of this DPA. Enerzyz maintains such de-identification, does not attempt to re-identify the data, and contractually binds any recipient to the same restriction.

5.7 Survival. This Section 5 survives termination or expiry. The return or deletion of Customer Data under Section 15 does not require Enerzyz to delete generalised, de-identified Platform Intelligence that does not identify the Customer or any Data Subject, as further specified in the deletion schedule in Section 15.

6. Confidentiality

6.1 Enerzyz shall treat Personal Data as confidential and shall ensure that all personnel authorised to Process Personal Data are subject to a duty of confidentiality, whether by contract or statute, that survives the termination of their engagement.

6.2 Enerzyz operates a least-privilege access model. By default, Enerzyz engineering personnel cannot view Customer Telemetry without an active, time-bounded support case authorised by dual approval, and all such access is logged and attributable in accordance with Annex II.

7. Lawful Bases for Enerzyz Processing

7.1 Where Enerzyz Processes Customer Data as the Customer's Processor, the Customer is responsible for establishing the lawful basis for that Processing and warrants that it has done so under Section 3. Where Enerzyz Processes Personal Data as a limited independent Controller for the purposes in Section 2.3 (platform security, operations, monitoring and de-identified analytics), it relies, as applicable under the relevant Applicable Data Protection Law, on one or more of the following lawful bases:

- **Legitimate interests —** the legitimate interests of Enerzyz and third parties in operating, securing, optimising and improving the Services and the Platform, where such interests are not overridden by the interests or fundamental rights of Data Subjects;
- **Performance of a contract —** where Processing is necessary to provide the Services requested by the Customer;
- **Legal obligation —** where Processing is necessary for compliance with a legal obligation to which Enerzyz is subject; and
- **Consent —** where required by Applicable Data Protection Law and obtained in accordance with Section 3.

7.2 Enerzyz shall not sell Personal Data and shall not share Personal Data for cross-context behavioural advertising within the meaning of U.S. State Privacy Laws. Enerzyz does not engage in solely-automated decision-making producing legal or similarly significant effects on Data Subjects through the Services; autonomous optimisation actions operate on equipment, with human override authority retained by the Customer at all times.

8. Security of Processing

8.1 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 to Data Subjects, Enerzyz shall implement and maintain appropriate technical and organisational measures designed to ensure a level of security appropriate to the risk, as described in Annex II.

8.2 Enerzyz's information-security programme is aligned to ISO/IEC 27001:2022, IEC 62443 for industrial-automation security, the NIST Cybersecurity Framework 2.0, and the SOC 2 Trust Services Criteria. Enerzyz maintains an outbound-only, mutually-authenticated integration architecture that places no inbound attack surface on the Customer's network and does not traverse the Customer's corporate IT environment.

8.3 Enerzyz regularly tests, assesses and evaluates the effectiveness of its measures, and shall not materially diminish the overall level of protection during the term.

8.4 Certification status. Enerzyz's information-security programme is designed and operated in full alignment with ISO/IEC 27001:2022, IEC 62443, the NIST Cybersecurity Framework 2.0, and the SOC 2 Trust Services Criteria. Enerzyz's ISO/IEC 27001:2022 certification is in progress and is being pursued through an accredited certification body. Enerzyz maintains a SOC 2 controls programme and will make its SOC 2 report available to the Customer upon request, subject to a confidentiality undertaking (NDA). Enerzyz will, on the Customer's reasonable request, provide its current certification and attestation status and supporting evidence of its controls to support the Customer's vendor-assurance process.

8.5 **Transparency pending certification.** Until its certifications are complete, and on an ongoing basis thereafter, Enerzyz maintains and makes available to the Customer a Security and Data Protection White Paper together with reference architecture diagrams, data-flow descriptions, control summaries, encryption standards and access-management controls, so that the Customer's security and procurement teams can complete their assessment with documentary evidence rather than reliance on certification alone. These materials are designed to materially reduce the volume of bespoke security questionnaires.

9. Sub-processors

9.1 The Customer provides general authorisation for Enerzyz to engage Sub-processors, including Enerzyz Affiliates and the infrastructure providers identified in Annex III, to Process Personal Data in connection with the Services.

9.2 Enerzyz shall impose on each Sub-processor, by written contract, data-protection obligations no less protective than those set out in this DPA, and remains responsible for each Sub-processor's performance of its obligations.

9.3 **Notice and objection.** Enerzyz shall maintain an up-to-date list of Sub-processors and shall notify the Customer of any intended addition or replacement of a Sub-processor at least thirty (30) days before that Sub-processor begins Processing Personal Data, through the web-linked register and a subscribable notification mechanism. Within that 30-day period, the Customer may object on reasonable data-protection grounds by written notice setting out its grounds. The parties shall then work together in good faith for a resolution period of up to thirty (30) days to address the objection, including by Enerzyz proposing reasonable mitigations or an alternative. If the objection cannot be resolved within that period, the Customer may, as its sole remedy, suspend or terminate the affected Services without penalty. Enerzyz will not engage the objected-to Sub-processor for the Customer's Personal Data while a timely objection is being resolved.

10. International Data Transfers

10.1 Enerzyz operates a multi-cloud back end and selects the hosting region in accordance with the Customer's data-residency requirements where such options are made available through the Services. Personal Data may be Processed in, or accessed from, jurisdictions other than the Customer's own.

10.2 **Transfer mechanisms.** Where Enerzyz transfers Personal Data across borders, it shall do so only where a valid transfer mechanism is in place under the relevant Applicable Data Protection Law, including: an adequacy decision; the Standard Contractual Clauses; the United Kingdom International Data Transfer Addendum or Addendum to the EU SCCs; the Swiss addendum recognised by the Swiss Federal Data Protection and Information Commissioner; certification under the EU–U.S. Data Privacy Framework, the UK Extension and the Swiss–U.S. Data Privacy Framework (where and for so long as available); the PIPL standard contract and security-assessment route; or binding corporate rules or other lawful safeguards.

10.3 **Incorporation of the SCCs.** Where the EU SCCs apply, they are incorporated into this DPA by reference and completed as set out in Annex IV. Module Two (controller-to-processor) applies to Customer Data Processed by Enerzyz as the Customer's Processor, and Module One (controller-to-controller) applies only to Personal Data Processed by Enerzyz as a limited independent Controller under Section 2.3, in each case with the docking, options and annexes specified in Annex IV. The parties shall, where required, conduct a transfer impact assessment and implement supplementary measures.

10.4 **Onward transfers.** Enerzyz shall ensure that onward transfers to Sub-processors are subject to appropriate safeguards consistent with this Section 10.

11. Data Subject Rights

11.1 Taking into account the nature of the Processing, Enerzyz shall provide reasonable assistance to the Customer, by appropriate technical and organisational measures and insofar as possible, to enable the Customer to respond to requests from Data Subjects exercising their rights under Applicable Data Protection Law in respect of Customer Account Data.

11.2 Where Enerzyz Processes Personal Data as a Controller, Enerzyz shall handle Data Subject requests directly and shall maintain a privacy contact and request channel for that purpose. If Enerzyz receives a request relating to data for which the Customer is the Controller, Enerzyz shall, unless legally prohibited, promptly redirect the Data Subject to the Customer and notify the Customer.

12. Personal Data Breach Notification

12.1 Enerzyz shall notify the Customer without undue delay, and in any event within the timeframe required by Applicable Data Protection Law, after becoming aware of a Personal Data Breach affecting Personal Data Processed under this DPA, and where the Customer is the Controller, in sufficient time to enable the Customer to meet its own notification obligations.

12.2 **Commercial notification commitment.** In addition to the statutory standard in Section 12.1, and to provide the Customer with operational certainty, Enerzyz shall notify the Customer of a confirmed Personal Data Breach affecting the Customer's Personal Data without undue delay and in any event within seventy-two (72) hours of Enerzyz confirming the breach. Where the relevant facts are still under investigation, Enerzyz shall provide an initial notification within that window and supplement it with further information as it becomes available.

12.3 Such notification shall describe, to the extent known, the nature of the breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, and the measures taken or proposed to address the breach and mitigate its effects. Enerzyz shall document Personal Data Breaches and cooperate with the Customer and competent authorities. A notification is not an acknowledgement of fault or liability.

13. Data Protection Impact Assessments and Prior Consultation

13.1 Taking into account the nature of the Processing and the information available to it, Enerzyz shall provide reasonable assistance to the Customer with data-protection impact assessments and prior consultations with supervisory authorities, where required by Applicable Data Protection Law in respect of the Customer's use of the Services.

14. Audits and Demonstration of Compliance

14.1 Enerzyz shall make available to the Customer information reasonably necessary to demonstrate compliance with this DPA, primarily through its third-party certifications, audit reports and security documentation. In particular, Enerzyz shall, upon the Customer's request and subject to a confidentiality undertaking (NDA), provide its SOC 2 report and evidence of its ISO/IEC 27001 certification status, together with responses to the Customer's reasonable security and privacy questionnaires.

14.2 Where such materials are insufficient to demonstrate compliance, and subject to confidentiality undertakings, the Customer (or an independent auditor mandated by the Customer that is not a competitor of Enerzyz) may conduct an audit no more than once in any twelve-month period, on reasonable prior written

notice, during business hours, in a manner that does not disrupt Enerzyz's operations or the security and confidentiality of other customers' data. The parties shall bear their own costs, save that the Customer shall reimburse Enerzyz's reasonable costs for audits exceeding ordinary scope.

15. Return and Deletion of Personal Data

15.1 On expiry or termination of the Principal Agreement, Enerzyz shall, at the Customer's election, return or delete Customer Data, including Customer Account Data, within the period specified in the Principal Agreement or, absent such specification, within ninety (90) days, save to the extent retention is required by law.

15.2 As provided in Section 5.7, the return or deletion of Customer Data does not extend to generalised, de-identified Platform Intelligence that does not identify the Customer or any Data Subject. Enerzyz may also retain Personal Data in routine backups for a limited period in accordance with its retention schedule, during which such data remains subject to this DPA and is not actively Processed.

15.3 **Edge devices.** Enerzyz Edge Max devices deployed at the Customer's facility buffer telemetry locally only on a transient basis to bridge periods of cloud unreachability; they are not designed as a long-term store of Customer Data. On termination, or on decommissioning or replacement of an Edge device, Enerzyz shall securely erase Customer Data held in the device's local buffer using its secure-decommissioning procedure (including cryptographic erasure of device keys, which renders any residual encrypted data unrecoverable), and shall revoke the device's operational certificate. The parties shall agree the logistics of physical retrieval, return or on-site sanitisation of Enerzyz-owned hardware; where the Customer retains physical possession pending collection, the Customer shall take reasonable steps to safeguard the device. Enerzyz shall provide a certificate of data sanitisation on the Customer's reasonable request.

15.4 **Deletion schedule.** For clarity, on expiry or termination of the Principal Agreement the following applies:

Permanently deleted	Retained (only in non-identifying form)
Raw Telemetry and operational data Customer records and content Customer Account Data and user identities Site, asset and configuration data Edge-device local buffers (securely erased)	**Fully anonymised, aggregated statistics** Generic, de-identified AI model learnings Platform Intelligence that cannot identify the Customer, any site or any Data Subject Records Enerzyz must retain by law (for the required period only)

Nothing retained under the right-hand column identifies, or can reasonably be used to identify, the Customer, any individual property or site, or any Data Subject. Where a Customer has made the Section 5.3 model-training election, its data is also excluded from the retained de-identified learnings.

16. Liability

16.1 Each party's liability arising out of or related to this DPA, whether in contract, tort or otherwise, is subject to the limitations and exclusions of liability set out in the Principal Agreement, and any reference in the Principal Agreement to the liability of a party means the aggregate liability of that party and its Affiliates under the Principal Agreement and this DPA together.

16.2 Nothing in this DPA limits liability to the extent such limitation is not permitted by Applicable Data Protection Law, including liability to Data Subjects under the SCCs.

17. Region-Specific Terms

This Section 17 supplements the DPA for the jurisdictions identified below and applies only to the extent the relevant Applicable Data Protection Law governs the Processing. In case of conflict with the body of this DPA, this Section 17 prevails for the relevant jurisdiction.

17.1 European Economic Area (EU GDPR)

This DPA gives effect to Articles 28, 32–36 and Chapter V of Regulation (EU) 2016/679 ("GDPR"). References to "supervisory authority", "special categories of data" and "Data Subject rights" have the meaning given in the GDPR. Enerzyz acts as the Customer's Processor under Article 28 in respect of Customer Data, and as an independent Controller only for the limited internal purposes set out in Section 2.3. Cross-border transfers from the EEA are governed by the EU SCCs as incorporated in Annex IV.

17.2 United Kingdom (UK GDPR)

This DPA applies to Processing subject to the UK GDPR and the Data Protection Act 2018. Transfers from the United Kingdom are governed by the UK International Data Transfer Addendum to the EU SCCs (the "UK Addendum") issued by the Information Commissioner, as completed in Annex IV. References to the EU SCCs are read as modified by the UK Addendum, and references to supervisory authorities, governing law and forum are read as referring to the United Kingdom.

17.3 Switzerland (revFADP)

For Processing subject to the Swiss Federal Act on Data Protection, the EU SCCs apply with the Swiss adaptations: the Swiss Federal Data Protection and Information Commissioner is the competent authority, the term "member state" does not bar Data Subjects resident in Switzerland from enforcing rights in their place of habitual residence, and references to the GDPR are read as references to the revFADP, which also protects the data of legal entities until such protection is removed.

17.4 United States (State Privacy Laws)

Where Enerzyz Processes Personal Data as a service provider or processor on the Customer's behalf under the U.S. State Privacy Laws (including the CCPA as amended by the CPRA, and comparable laws in Virginia, Colorado, Connecticut, Utah, Texas and other states), Enerzyz shall: Process such Personal Data only for the limited and specified purposes of providing the Services; not sell or share such Personal Data; not retain, use or disclose it outside the direct business relationship or for purposes other than those specified; and not combine it with Personal Data from other sources except as permitted by law. Enerzyz certifies that it understands and will comply with these restrictions. Enerzyz's generation and use of Aggregated Data and Derived Data is conducted in a manner consistent with the "deidentified" and "aggregate consumer information" exclusions of those laws.

17.5 Canada (PIPEDA and Quebec Law 25)

For Processing subject to the Personal Information Protection and Electronic Documents Act and provincial statutes including Quebec's Act respecting the protection of personal information in the private sector ("Law 25"), Enerzyz shall maintain protections comparable to those required of the Customer, assist with breach-record and confidentiality-incident obligations, and support transfer-related privacy impact assessments where the Customer is required to conduct them.

17.6 Brazil (LGPD)

For Processing subject to Lei Geral de Proteção de Dados (Law No. 13.709/2018), the roles of "controlador" and "operador" map to Controller and Processor respectively. Enerzyz shall support the data-subject rights

and reporting obligations under the LGPD and cooperate with the Autoridade Nacional de Proteção de Dados (ANPD). International transfers rely on the ANPD-approved standard contractual clauses or other lawful mechanisms.

17.7 China (PIPL)

For Processing subject to the Personal Information Protection Law, where Enerzyz acts as an entrusted party it Processes personal information only within the agreed scope and purpose. Cross-border transfers of personal information out of the People's Republic of China are conducted only through a lawful route — the CAC security assessment, the China standard contract for the outbound transfer of personal information, or certification — and subject to the separate consent and notice requirements of the PIPL where applicable. Enerzyz supports the Customer's personal-information protection impact assessment obligations.

17.8 Japan (APPI)

For Processing subject to the Act on the Protection of Personal Information, Enerzyz handles personal data within the scope of the entrustment and implements necessary and appropriate supervision of any party it further entrusts. Cross-border provision of personal data relies on the establishment of equivalent protection by appropriate measures, with the information disclosures required under the APPI, or on the data subject's consent.

17.9 Singapore (PDPA)

For Processing subject to the Personal Data Protection Act 2012, Enerzyz, as a data intermediary in respect of Customer Account Data, complies with the protection and retention-limitation obligations and assists the Customer with the data-breach notification obligation to the Personal Data Protection Commission. The parties acknowledge Enerzyz's alignment with the Cybersecurity Act 2018 where the Customer operates Critical Information Infrastructure.

17.10 India (DPDP Act 2023 and DPDP Rules 2025)

For Processing subject to the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025 (notified and being brought into force in phases), where Enerzyz acts as a Data Processor it Processes personal data only on the Customer's (Data Fiduciary's) instructions and under a valid contract, implements reasonable security safeguards, and assists with the Customer's breach-intimation obligations to the Data Protection Board of India. The parties acknowledge that occupancy-sensing or presence-detection data is Processed only where a lawful basis exists.

17.11 Australia (Privacy Act / APPs)

For Processing subject to the Privacy Act 1988 and the Australian Privacy Principles, Enerzyz shall take reasonable steps to protect personal information, support the Customer's obligations under the Notifiable Data Breaches scheme, and ensure that cross-border disclosures are made on a basis consistent with APP 8.

17.12 South Africa (POPIA)

For Processing subject to the Protection of Personal Information Act, 2013, Enerzyz, as an operator, Processes personal information only with the knowledge or authorisation of the responsible party and treats it as confidential, notifies the responsible party of any compromise, and supports notification to the Information Regulator.

17.13 South Korea (PIPA)

For Processing subject to the Personal Information Protection Act, Enerzyz, where entrusted with personal information handling, Processes it within the entrusted scope, is supervised by the Customer, and supports the disclosure and consent requirements applicable to the cross-border transfer of personal information.

17.14 Thailand (PDPA)

For Processing subject to the Personal Data Protection Act B.E. 2562 (2019), where Enerzyz acts as a data processor it Processes personal data only on the Customer's (data controller's) instructions, implements appropriate security measures consistent with the standards of the Personal Data Protection Committee (PDPC), and notifies the Customer of any personal-data breach so as to support the Customer's breach-notification obligation to the PDPC (generally within 72 hours where required). Cross-border transfers rely on adequate-protection findings, the Customer's consent, or appropriate safeguards recognised under the PDPA.

17.15 Malaysia (PDPA)

For Processing subject to the Personal Data Protection Act 2010 and its amendments, Enerzyz, as a data processor, Processes personal data on the Customer's instructions, gives effect to the Security Principle and the data-processor obligations introduced by the 2024 amendments (including the appointment of a data protection officer where applicable and support for data-breach notification to the Personal Data Protection Commissioner), and effects cross-border transfers in accordance with the conditions of the PDPA.

17.16 Gulf and Middle East (Saudi PDPL, UAE and others)

For Processing subject to the Kingdom of Saudi Arabia Personal Data Protection Law and its Implementing Regulations, the United Arab Emirates Federal Decree-Law No. 45 of 2021 (and the data-protection regimes of the DIFC and ADGM financial free zones), and comparable laws in Qatar, Bahrain, Oman and Kuwait, Enerzyz Processes personal data within the documented scope, implements appropriate safeguards, and effects cross-border transfers through the standard contractual clauses, adequacy or other lawful mechanisms recognised by the competent authority (including the Saudi Data and Artificial Intelligence Authority).

18. General Provisions

18.1 **Term.** This DPA takes effect on the effective date of the Principal Agreement and continues for so long as Enerzyz Processes Personal Data under the Principal Agreement, after which the surviving provisions (including Sections 5, 15 and 16) continue to apply.

18.2 **Governing law.** This DPA is governed by the governing law of the Principal Agreement, save where Applicable Data Protection Law or an incorporated transfer mechanism requires otherwise for the protection of Data Subjects.

18.3 **Severability.** If any provision of this DPA is held invalid or unenforceable, the remaining provisions continue in full force, and the parties shall replace the affected provision with a valid one that achieves its purpose as closely as possible.

18.4 **Variation.** Enerzyz may update this DPA from time to time to reflect changes in Applicable Data Protection Law or the Services, provided that no such update materially diminishes the protection of Personal Data or the Customer's rights under this DPA. Any material change affecting the Customer's rights will not take effect until Enerzyz has given the Customer reasonable prior notice and the Customer has had a reasonable opportunity to review the change. If a material change would have a material adverse effect on

the Customer and the parties cannot agree, the Customer may terminate the affected Services without penalty. Changes required to comply with law take effect as required by that law.

18.5 Entire agreement. This DPA, together with its Annexes and the Principal Agreement, constitutes the entire agreement between the parties regarding the Processing of Personal Data and supersedes any prior data-processing terms.

18.6 Acceptance and execution. This DPA may be accepted and made binding in either of two ways: (a) for self-service and online subscriptions, by the Customer's acceptance of the Principal Agreement or by accessing or using the Services, in which case this DPA is incorporated by reference without a separate signature; or (b) for enterprise engagements, by the parties' execution of the signature block in the Execution section, which the parties agree governs where completed. A DPA executed by authorised signatories prevails over online acceptance for the same engagement. Electronic signatures and counterparts are valid and binding.

Annex I — Details of Processing

Item	Description
Data exporter / Controller	The Customer (in respect of Customer Account Data) and Enerzyz (in respect of Telemetry, Service Data and Derived Data, as independent Controller).
Data importer / Processor	Enerzyz Pte. Ltd. and its Affiliates.
Subject matter	Provision of the Enerzyz Platform: acquisition, normalisation, analysis and optimisation of energy-asset telemetry, and associated reporting.
Duration	For the term of the Principal Agreement and the retention periods set out in this DPA.
Nature & purpose	Operation, security, optimisation, sustainability reporting, and continual improvement of the Services and Platform Intelligence.
Categories of Data Subjects	The Customer's Authorised Users (administrators, engineers, operators). The Services do not target or single out building occupants or hotel guests; only aggregate, zone-level occupancy counts are used as energy telemetry.
Categories of Personal Data	Customer Account Data: names, business email addresses, user identifiers, role assignments, authentication identifiers, audit-log entries and access metadata. Operational data: aggregate, zone-level occupancy/presence counts used as energy-management telemetry.
Excluded data (out of scope)	Guest names, room numbers tied to a named individual, check-in/check-out records, reservation, folio or loyalty data, and any Property Management System (PMS) or Guest Room Management System (GRMS) guest-record data; special categories of data; clinical or patient data; payment-card data; government identifiers; and children's data. The Services are not configured to Process such data (see Section 3.5).
Special categories	None. The Services are not configured to Process special categories of data, clinical or patient data, or children's data.
Frequency	Continuous (real-time telemetry) and on-demand (console access).
Retention	Customer Account Data: per Section 15. Telemetry: per the Principal Agreement service configuration. Derived/Aggregated Data: retained as Platform Intelligence in non-identifying form.

Hospitality data boundary. For hotel and hospitality deployments, Enerzyz confirms that it integrates with BMS and GRMS infrastructure solely to obtain energy-relevant signals, consuming only aggregate, zone-level occupancy counts to drive optimisation. No guest name, room number, check-in or check-out record, reservation, folio, loyalty identifier or PMS/GRMS guest-record data is ingested, stored or transmitted by the Services.

Annex II — Technical and Organisational Measures

Domain	Measures
Governance	Information-security programme aligned to ISO/IEC 27001:2022, IEC 62443, NIST CSF 2.0 and SOC 2 Trust Services Criteria; documented policies; periodic risk assessment; STRIDE-based threat modelling.
Certifications & attestations	Programme fully aligned to ISO/IEC 27001:2022, IEC 62443, NIST CSF 2.0 and SOC 2 Trust Services Criteria. ISO/IEC 27001:2022 certification in progress via an accredited body. SOC 2 report available to the Customer on request under NDA. Current certification status and evidence provided to support vendor assurance (see Section 8.4).
Architecture	Outbound-only, mutually-authenticated integration; no inbound attack surface on the Customer firewall; OT/IT segregation; the Customer corporate IT network is never traversed; per-tenant data isolation by Project ID.
Encryption	Mutual TLS 1.2/1.3 in transit; end-to-end message signing from edge; encryption at rest; keys generated and managed in HSM-backed KMS; device-bound, non-exportable private keys where supported.
Access control	Customer SSO via SAML 2.0 / OIDC with MFA enforced at the Customer IdP; role-based access control; no Enerzyz-side passwords for human users by default.
Engineering access	Default state: no access to Customer telemetry; just-in-time elevation requires a named ticket and dual approval (engineering + security lead); time-bounded (max 8-hour grants); fully logged; no persistent production shells.
Key & certificate lifecycle	Per-device X.509 certificates issued at manufacture, rotated on first cloud bind and annually thereafter, and immediately on suspected compromise; OCSP revocation.
Logging & monitoring	Tamper-evident audit chain; attribution of privileged actions; SIEM export; security-event handling and alerting.
Vulnerability management	Defined patch cadence; advisory subscription; CVSS-based triage; secure software development practices.
Resilience	Local edge buffering during cloud unreachability with transparent resync; multi-cloud back end; defined uptime targets; backup and recovery.
Personnel	Background checks where lawful; confidentiality undertakings; least-privilege; joiner-mover-leaver process; security awareness training.
Sub-processor management	Contractual flow-down of protections; ongoing oversight; maintained register.

Annex III — Approved Sub-processors

The following sub-processors are engaged by Enerzyz to Process Personal Data in connection with the Services. The current, authoritative version of this register — including legal entity names, services and country-level hosting locations — is maintained by Enerzyz and made available to the Customer, with changes notified in accordance with Section 9.

Sub-processor (legal entity)	Service provided	Hosting / processing location	Transfer mechanism
Amazon Web Services, Inc. (and AWS regional entities)	Cloud infrastructure, hosting and storage of the Enerzyz Cloud back end	Region selected per Customer data-residency requirement (default: AWS Asia Pacific — Singapore)	SCCs / DPF / adequacy as applicable
Google LLC and Google Cloud EMEA Limited	Cloud infrastructure, storage and managed data services	Region selected per Customer data-residency requirement	SCCs / DPF / adequacy as applicable
Enerzyz Affiliates	Provision, support, engineering and customer success	Jurisdictions in which Enerzyz operates (incl. Singapore)	Intra-group SCCs / safeguards
Global M2M connectivity provider (named in the live register)	Cellular (4G) fallback connectivity for edge devices; data encrypted in transit	Per network coverage	SCCs / adequacy as applicable

Maintained register. *The named legal entities, the specific services they perform and their country-level hosting locations are published in Enerzyz's web-linked sub-processor register, which is kept current and from which the Customer may subscribe to change notifications. The entries above identify the principal sub-processors; the live register is the controlling list for the purposes of Section 9.*

Annex IV — Standard Contractual Clauses and Transfer Mechanisms

Clause / option	Completion for this DPA
Modules	Module Two (controller-to-processor) for Customer Data Processed by Enerzyz as Processor; Module One (controller-to-controller) only for the limited Controller purposes under Section 2.3.
Clause 7 (docking)	Optional docking clause applies; additional entities may accede by agreement.
Clause 9 (sub-processors)	Option 2 — general written authorisation, with notice of changes per Section 9 of this DPA.
Clause 11 (redress)	Optional independent dispute-resolution body not selected.
Clause 17 (governing law)	The law of the EU member state of the data exporter, or of Ireland where the exporter is outside the EEA, unless otherwise specified.
Clause 18 (forum)	Courts of the member state identified under Clause 17.
UK Addendum	The ICO International Data Transfer Addendum applies to UK transfers; Tables 1–4 completed by reference to the EU SCCs and this DPA; ending of the Addendum per its Section 19.
Annex I/II/III of the SCCs	Populated by reference to Annex I, II and III of this DPA respectively.
DPF	Where Enerzyz or a Sub-processor is certified under the EU–U.S. Data Privacy Framework (and UK Extension / Swiss–U.S. DPF), that certification may serve as the transfer mechanism for relevant transfers to the United States.

Transfer impact assessment. *The parties acknowledge the evolving legal landscape for transfers to the United States and other third countries and shall conduct and document a transfer impact assessment and implement supplementary measures where required by Applicable Data Protection Law.*

Annex V — Hospitality Data Boundary

This Annex applies to deployments at hotels and hospitality facilities. It records, in one place, the categories of guest-related data that Enerzyz does and does not collect, so that hotel legal, privacy and procurement teams can confirm the data boundary quickly. This Annex supplements, and does not limit, Section 3.5 and Annex I.

Enerzyz confirms that, in hospitality deployments, it does NOT collect, store, transmit or profile any of the following:

- Property Management System (PMS) data;
- Guest names or contact details;
- Loyalty-programme or membership data;
- Payment-card or financial data;
- Room folio, billing or charge data;
- Reservation, check-in or check-out records;
- Guest Room Management System (GRMS) guest-record data; and
- Any guest behavioural profiling or individual guest tracking.

What Enerzyz does collect. Enerzyz collects only energy-relevant equipment Telemetry and aggregate, zone-level occupancy counts (for example, the number of occupied zones on a floor) used solely to drive HVAC and energy optimisation. These signals are not linked to any named individual and are not used to identify or track guests.

Collected (energy telemetry only)	Never collected
Equipment telemetry (temperatures, pressures, currents, vibration, runtime, fuel/resource levels) Aggregate, zone-level occupancy counts for HVAC/energy optimisation Weather and tariff data; equipment state changes	Guest names, PMS / GRMS guest records Loyalty, payment-card, folio and reservation data Check-in/out records; any guest behavioural profiling or individual tracking

This boundary is enforced technically at the point of integration: where a building system exposes guest-identifying fields, Enerzyz consumes only the energy-relevant signal and excludes those fields. A breach of this Annex is a material breach of this DPA.

Execution

By signing the Principal Agreement, or by accessing or using the Services, the parties agree to be bound by this DPA. Where a signature block is required, the parties execute this DPA below.

For and on behalf of ENERZYZ PTE. LTD.

Signature: _____

Name: _____

Title: _____

Date: _____

For and on behalf of the CUSTOMER

Signature: _____

Name: _____

Title: _____

Date: _____