

ENERYZ

AI Operating System for Energy Assets

DATA PROCESSING AGREEMENT

Global Data Protection and Cross-Border Transfer Terms

This Data Processing Agreement (“DPA”) forms part of, and is incorporated by reference into, the Facility Services Agreement, or other written agreement, between the Customer and Enerzyz Pte. Ltd. under which the Services are provided (the “Principal Agreement”).

Document reference

ENZ-LEGAL-DPA-001 · Version 3.4 · Global Edition

Issued October 2026 · Effective as set out in Section 18.1

Supersedes Version 3.3 (August 2026)

© 2026 Enerzyz Pte. Ltd. and its Affiliates. All rights reserved.

Revision history

Version	Date	Summary
3.0	June 2026	Initial Global Edition.
3.1	July 2026	ISO/IEC 27001:2022 certification position updated.
3.2	July 2026	Hosting footprint updated.
3.3	August 2026	Role alignment, breach timing and transfer wording corrected.
3.4	October 2026	Incorporates into the Facility Services Agreement and defines the Principal Agreement. Restores the model-training election wording and clarifies site-level learning. States the group ISO/IEC 27001:2022 position and verification route. Adds Singapore transfer terms, export and deletion on exit, and specific technical measures. Aligns the network path with the Enerzyz connection models. Annex III aligned to the live sub-processor register.

Contents

Background and Construction
1. Definitions and Interpretation
2. Scope, Roles and Allocation of Responsibility
3. Customer Responsibilities and Warranties
4. Processing by Enerzyz
5. Customer Data, Service Improvement and Platform Intelligence
6. Confidentiality
7. Lawful Bases for Enerzyz Processing
8. Security of Processing
9. Sub-processors
10. International Data Transfers
11. Data Subject Rights
12. Personal Data Breach Notification
13. Data Protection Impact Assessments and Prior Consultation
14. Audits and Demonstration of Compliance
15. Return, Retention and Deletion of Personal Data
16. Liability
17. Region-Specific Terms
18. General Provisions
Annex I — Details of Processing
Annex II — Technical and Organisational Measures
Annex III — Sub-processors
Annex IV — Standard Contractual Clauses and Transfer Mechanisms
Annex V — Hospitality Data Boundary
Execution

Background and Construction

A. Services. Enerzyz operates an AI-native system for energy assets (the “Enerzyz Platform” or the “Services”) comprising edge hardware where applicable, cloud services, physics-informed digital twins, machine-learning models and autonomous optimisation software that acquire, normalise and analyse equipment telemetry to reduce energy waste and provide engineering and sustainability outputs.

B. Purpose. In delivering the Services, Enerzyz Processes data that may include limited Personal Data. This DPA sets out the data-protection terms applying to that Processing.

C. Architecture. Telemetry originates from the Customer operational-technology environment and is conveyed to the Enerzyz back end for engineering intelligence, optimisation actions and reporting. The hosting, network and transfer facts for each Customer are those stated in the Customer order, this DPA and the current Enerzyz security documentation.

D. Operational data ownership. As between the parties, the Customer owns its operational data, including Telemetry. Enerzyz Processes that data as Processor to provide the Services. Enerzyz acts as an independent Controller only for the limited internal purposes stated in Section 2.3. Enerzyz does not assert ownership of Customer operational data.

Order of precedence. Once effective, this DPA prevails over the Principal Agreement only in relation to Personal Data Processing. Region-Specific Terms and incorporated transfer mechanisms prevail where legally required.

1. Definitions and Interpretation

Term	Meaning
Affiliate	an entity that controls, is controlled by or is under common control with a party.
Aggregated Data	data derived from Customer Data, Service Data or Telemetry that has been aggregated and de-identified so that it cannot reasonably identify the Customer, an individual site or a Data Subject.
Applicable Data Protection Law	all privacy, data-protection and security laws applying to the Processing under this DPA.
Controller	the person that determines the purposes and means of Processing Personal Data.
Customer Account Data	Personal Data used to administer, authenticate and audit Authorised Users and their access.
Customer Data	data the Customer or its Authorised Users provide to the Services, or that the Services collect from the Customer environment, under the Principal Agreement.
Data Subject	an identified or identifiable natural person to whom Personal Data relates.
Derived Data	models, parameters, features, inferences, anomaly signatures, baselines, benchmarks, indices, insights and analytics generated through Processing, excluding Customer Data in its original form.
Personal Data	information relating to an identified or identifiable natural person, including equivalent terms under Applicable Data Protection Law.
Personal Data Breach	a security breach leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Personal Data.
Principal Agreement	the Facility Services Agreement, or other written agreement, between the Customer and the Enerzyz contracting entity under which the Services are provided.

Term	Meaning
Processing	any operation performed on Personal Data, including collection, recording, storage, use, disclosure, transmission, erasure and destruction.
Processor	an entity that Processes Personal Data on behalf of a Controller.
Service Data	data relating to provision, security, performance, configuration, billing and operation of the Services, including diagnostic, log, audit and usage metadata.
Service Insights	the analytics, predictions, optimisation recommendations, energy and emissions reporting and other outputs the Services make available to the Customer.
Standard Contractual Clauses or SCCs	the standard contractual clauses approved by European Commission Implementing Decision (EU) 2021/914, and any equivalent or successor clauses adopted under another Applicable Data Protection Law.
Sub-processor	a third party engaged by a Processor to Process Personal Data for the Controller.
Telemetry	real-time and historical operational data acquired from equipment and the facility environment, including temperatures, pressures, electrical currents, flow, vibration, runtime, resource levels, aggregate occupancy signals, weather, tariffs and equipment state.

1.1 Interpretation. Capitalised terms not defined here have the meaning in the Principal Agreement. References to law include subordinate and successor provisions. “Including” means including without limitation.

2. Scope, Roles and Allocation of Responsibility

2.1 Scope. This DPA applies to Personal Data Processed by Enerzyz and its authorised Sub-processors in providing the Services under the Principal Agreement.

2.2 Customer as Controller and Enerzyz as Processor. For Customer Data, including Telemetry, operational data and Customer Account Data, the Customer is Controller and Enerzyz is Processor. Enerzyz Processes Customer Data only on documented instructions and as needed to provide, support and secure the Services.

2.3 Limited independent controllership. Enerzyz is an independent Controller only for the minimum Personal Data necessary for platform security, platform operations, service monitoring, billing, legal compliance and de-identified internal analytics.

2.4 No independent operational use. Enerzyz does not determine independent purposes for identifiable Customer operational Telemetry and does not use it to provide services to a third party.

2.5 Independent Controllers. Where each party determines its own purposes and means for the same dataset, each acts as an independent Controller and remains responsible for its own compliance.

2.6 Processing details. The subject matter, duration, purposes, data categories, Data Subjects and operations are set out in Annex I.

3. Customer Responsibilities and Warranties

3.1 Lawful collection. The Customer warrants that it has provided required notices, established lawful bases and obtained required consents for Customer Data supplied to Enerzyz, including occupancy or presence data that may relate to individuals.

3.2 Accuracy and instructions. The Customer is responsible for the accuracy, quality and legality of Customer Data and for ensuring its instructions comply with law.

3.3 Prohibited data. The Customer shall not configure the Services to receive special categories of Personal Data, patient or clinical data, payment-card data, government identifiers, children's data, passwords, private keys, certificates, network credentials or other secrets unless the parties expressly agree a lawful and secured workflow in writing.

3.4 Regulated environments. The Customer remains responsible for sector-specific obligations. Enerzyz shall provide reasonable technical documentation and assistance within its role.

3.5 Building and guest data boundary. The Services use energy and equipment signals and may use aggregate zone-level occupancy counts. They must not ingest guest names, named room assignments, check-in or check-out records, reservation, folio, loyalty, payment or other guest-record data. Where a connected system exposes those fields, Enerzyz shall exclude them at the integration boundary.

4. Processing by Enerzyz

4.1 Processor obligations. Enerzyz shall Process Customer Data only on documented instructions; bind authorised personnel to confidentiality; implement Annex II; control Sub-processors under Section 9; assist with rights, security, breach, impact-assessment and audit obligations; delete or return data under Section 15; and notify the Customer if an instruction infringes law.

4.2 Documented instructions. The Principal Agreement, this DPA, the agreed technical scope and the Customer configuration constitute the documented instructions. Additional instructions require written agreement and may incur charges.

4.3 Limited internal purposes. Enerzyz may Process the minimum data necessary for its limited Controller purposes under Section 2.3. It shall not use identifiable Customer Data to develop products for, benchmark or provide services to a third party.

5. Customer Data, Service Improvement and Platform Intelligence

5.1 Customer ownership. The Customer retains all rights in Customer Data, including Telemetry and operational and energy data. Enerzyz receives only the limited Processing rights necessary to provide and secure the Services.

5.2 Service improvement. Enerzyz shall not use identifiable Customer Data to train or fine-tune models for other customers. Service improvement may use Service Data and data that has been de-identified and aggregated so it cannot reasonably identify the Customer, any site or any Data Subject.

5.3 Enterprise election. An enterprise Customer may elect in writing to exclude its data from model-improvement activities, including de-identified datasets. The election does not affect the Customer's continued receipt of the Services or their quality. The models that operate the Customer's own sites continue to learn from that site's data as part of providing the Services; that site-level learning is not model improvement for the purposes of this Section. Enerzyz shall confirm implementation of the election.

5.4 Platform Intelligence. Enerzyz owns the Services, algorithms, models, methods and de-identified Aggregated Data ("Platform Intelligence"). Platform Intelligence does not include Customer Data in identifiable form. The Customer may use the Service Insights made available during the term.

5.5 Binding protections. Enerzyz shall not re-identify Derived or Aggregated Data, disclose a customer-specific operating or energy profile, create externally shared customer-specific competitive benchmarking, or attribute a benchmark to a Customer or site without prior written consent.

5.6 De-identification. Enerzyz shall maintain de-identification, shall not attempt re-identification and shall bind recipients to the same restriction.

5.7 Survival. This Section survives termination. De-identified Platform Intelligence may be retained only where it cannot identify the Customer, a site or a Data Subject and is not subject to a valid exclusion election.

6. Confidentiality

6.1 Confidentiality. Enerzyz shall treat Personal Data as confidential and ensure authorised personnel are bound by confidentiality obligations that survive their engagement.

6.2 Least privilege. Access shall be role-based, attributable, logged and limited to a documented purpose. Privileged access shall be time-bounded and revoked when the purpose ends.

7. Lawful Bases for Enerzyz Processing

7.1 Processor role. The Customer establishes the lawful basis for Processing performed on its behalf. For Enerzyz limited Controller purposes, Enerzyz shall identify an applicable lawful basis, including legitimate interests, contract, legal obligation or consent where required.

7.2 Restricted uses. Enerzyz shall not sell Personal Data or share it for cross-context behavioural advertising and shall not make solely automated decisions producing legal or similarly significant effects on Data Subjects. Equipment optimisation remains subject to Customer override.

8. Security of Processing

8.1 Security programme. Enerzyz shall maintain appropriate technical and organisational measures proportionate to risk, as described in Annex II, and shall not materially diminish the overall protection during the term.

8.2 Security claims. Any certification, network-path, hosting, identity, access, encryption or operational-security statement supplied to a Customer must be accurate, current and supported by evidence. Enerzyz Pte. Ltd. operates under the Enerzyz group information security management system, certified to ISO/IEC 27001:2022 (certificate GH60XXIX62026103, held by Enerzyz Inc.), verifiable on IAF CertSearch (iafcertsearch.org). A copy of the certificate and its scope are available on request. No Enerzyz Edge device opens an inbound listening port or requires an inbound firewall rule, and platform traffic is outbound TLS on TCP 443, with TLS 1.2 as the minimum and TLS 1.3 preferred. Building-control protocol traffic remains on the controls network. Where an Edge Pro holds addresses on both the controls network and the site LAN, forwarding, routing and address translation between them are disabled, and only outbound platform traffic crosses the site LAN. The connection model and network path for each site are stated in the Customer order. Authorised users access the Enerzyz Console through outbound HTTPS from an approved corporate device or network.

8.3 Certification maintenance. Enerzyz shall use commercially reasonable efforts to maintain ISO/IEC 27001:2022 certification, or certification to its successor standard, throughout the term of the Principal Agreement, and shall notify the Customer without undue delay if the certification is withdrawn, suspended or materially reduced in scope.

8.4 Testing. Enerzyz shall regularly test and evaluate relevant security controls and remediate material findings.

8.5 Assurance evidence. This DPA is published on the Enerzyz website. Enerzyz shall provide the Security White Paper, and a copy of its ISO/IEC 27001:2022 certificate and scope, on request. The Statement of Applicability, the penetration-test executive summary and further security documentation shall be provided under a non-disclosure agreement.

9. Sub-processors

9.1 Authorisation. The Customer gives general authorisation for Enerzyz to engage the Sub-processors listed in the current register referred to in Annex III, subject to this Section.

9.2 Flow-down. Enerzyz shall impose written obligations no less protective than this DPA and remains responsible for the performance of its Sub-processors.

9.3 Notice and objection. Enerzyz shall provide at least 30 days' prior notice of an intended addition or replacement through the maintained register and its notification mechanism. The Customer may object on reasonable data-protection grounds. The parties shall seek mitigation for up to 30 days. If unresolved, the Customer may terminate the affected Services without penalty.

10. International Data Transfers

10.1 Hosting facts. The Customer order and the current sub-processor register identify the cloud provider, legal entity, hosting region and permitted remote-access locations. Unless a specific residency configuration is agreed in the Customer order, the Enerzyz production environment runs active-active across AWS Asia Pacific (Singapore), AWS US East (Northern Virginia) and Google Cloud (Singapore), and Customer Data may be Processed in Singapore and the United States. Additional hosting regions are available on request, subject to commercial agreement.

10.2 Transfer mechanisms. Cross-border transfers shall use a lawful mechanism, including adequacy, approved standard clauses, certification, binding corporate rules or another recognised safeguard, together with supplementary measures where required.

10.3 SCC incorporation. Where EU SCCs apply, Module Two applies to Processor activities and Module One only to Enerzyz limited Controller activities. Annex IV completes the selected options. The parties shall conduct transfer impact assessments where required.

10.4 Onward transfers. Enerzyz shall ensure onward transfers by Sub-processors remain subject to appropriate safeguards.

11. Data Subject Rights

11.1 Processor assistance. Enerzyz shall provide reasonable assistance enabling the Customer to respond to Data Subject requests for Customer Data.

11.2 Controller requests. Where Enerzyz is Controller, it shall handle requests directly. Where a request relates to Customer-controlled data, Enerzyz shall redirect it and notify the Customer unless prohibited by law.

12. Personal Data Breach Notification

12.1 Notification. Enerzyz shall notify the Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data and in sufficient time for the Customer to meet its own legal obligations.

12.2 Commercial commitment. Enerzyz shall provide an initial notice within 72 hours after becoming aware of the breach, even if investigation continues, and provide updates as facts become available.

12.3 Contents and cooperation. The notice shall describe known facts, affected categories and approximate volumes, likely consequences and mitigation. Enerzyz shall document breaches and cooperate with the Customer and competent authorities. Notification is not an admission of liability.

13. Data Protection Impact Assessments and Prior Consultation

13.1 Assistance. Taking account of the nature of Processing and available information, Enerzyz shall reasonably assist the Customer with required impact assessments and prior consultation.

14. Audits and Demonstration of Compliance

14.1 Documentation. Enerzyz shall provide information reasonably necessary to demonstrate compliance, principally through its ISO/IEC 27001:2022 certification, audit materials, architecture and security documentation, and questionnaire responses, subject to confidentiality.

14.2 Audit. If those materials are insufficient, the Customer or a non-competitor independent auditor may audit relevant controls no more than once in 12 months on reasonable notice, during business hours and without compromising other customers or operations. Additional audits may occur following a material breach or regulator request.

15. Return, Retention and Deletion of Personal Data

15.1 Enerzyz Customer Data. On expiry or termination, the Customer may request an export of its Customer Data in a machine-readable format within 30 days. Enerzyz shall delete Customer Data from production systems within the period in the Principal Agreement or, if none, within 90 days of expiry or termination, except where law requires retention. Backup copies expire within 90 days while remaining protected and not actively Processed.

15.2 Edge devices. On decommissioning, Enerzyz shall erase Customer Data in local buffers and revoke device certificates. Retrieval, return or on-site sanitisation shall be agreed with the Customer. A sanitisation certificate shall be provided on reasonable request.

15.3 Permitted retention. Enerzyz may retain only fully anonymised aggregated statistics, generic de-identified model learnings, Platform Intelligence that cannot identify a Customer or site, and legally required records for the required period. A valid model-training exclusion election shall be respected.

16. Liability

16.1 Contractual limits. Liability under this DPA is subject to the limitations and exclusions in the Principal Agreement, applied in aggregate with liability under that agreement.

16.2 Mandatory liability. Nothing limits liability where limitation is prohibited by Applicable Data Protection Law, including enforceable Data Subject rights under transfer clauses.

17. Region-Specific Terms

17.1 European Economic Area. The GDPR applies. Enerzyz acts as Processor for Customer Data and independent Controller only for Section 2.3 purposes. EEA transfers use the EU SCCs and required supplementary measures.

17.2 United Kingdom. The UK GDPR and Data Protection Act 2018 apply. Transfers use the UK International Data Transfer Addendum or another lawful mechanism.

17.3 Switzerland. The Swiss Federal Act on Data Protection applies. EU SCCs are adapted for Swiss law and the competent Swiss authority.

17.4 United States. Where Enerzyz is a service provider or processor, it Processes Personal Data only for specified Services, does not sell or share it, and does not retain, use, disclose or combine it except as permitted by law.

17.5 Canada. Enerzyz shall maintain comparable protection, assist with breach and confidentiality obligations and support transfer impact assessments required under PIPEDA or applicable provincial law.

17.6 Brazil. LGPD Controller and Processor roles apply. Enerzyz shall support rights, reporting and lawful international transfer requirements.

17.7 China. PIPL entrusted-party requirements apply. Cross-border transfers require the applicable CAC assessment, standard contract, certification or another lawful route, together with required notices and consents.

17.8 Japan. APPI entrustment and cross-border requirements apply, including appropriate supervision and equivalent protection.

17.9 Singapore. The PDPA applies. Enerzyz shall comply with data-intermediary protection and retention duties and assist with breach notification. Critical Information Infrastructure obligations remain with the relevant party. For transfers of Personal Data out of Singapore, Enerzyz relies on the obligations in this DPA, including the clauses incorporated under Annex IV, as legally enforceable obligations for the purposes of the Transfer Limitation Obligation.

17.10 India. The DPDP Act and rules apply as brought into force. Enerzyz Processes on Data Fiduciary instructions, maintains safeguards and assists with breach obligations.

17.11 Australia. The Privacy Act and Australian Privacy Principles apply, including reasonable security, Notifiable Data Breaches and APP 8 cross-border requirements.

17.12 South Africa. POPIA operator requirements apply, including authorised Processing, confidentiality and compromise notification.

17.13 South Korea. PIPA entrusted-processing, supervision and cross-border disclosure and consent requirements apply.

17.14 Thailand. The PDPA applies. Enerzyz Processes on Controller instructions, maintains PDPC-aligned safeguards and supports breach notification and lawful transfers.

17.15 Malaysia. The PDPA and its amendments apply, including processor security, breach and transfer obligations and DPO requirements where applicable.

17.16 Gulf and Middle East. Applicable Saudi, UAE, DIFC, ADGM and other regional laws apply. Processing and transfers require the documented scope and recognised safeguards.

18. General Provisions

18.1 Term. This DPA takes effect when signed or incorporated by exact title and version into an executed Principal Agreement and continues while Enerzyz Processes Personal Data. Surviving provisions continue as stated.

18.2 Governing law. The governing law of the Principal Agreement applies unless mandatory law or an incorporated transfer mechanism requires otherwise.

18.3 Severability. An invalid provision shall be replaced with a valid provision that most closely achieves its purpose; remaining provisions continue.

18.4 Variation. Enerzyz may update this DPA for changes in law or the Services only where protection is not materially diminished. Material changes require reasonable prior notice and an opportunity to review. The Customer may terminate affected Services without penalty if a material adverse change cannot be resolved.

18.5 Entire data processing agreement. Once effective, this DPA, its Annexes and the Principal Agreement constitute the agreement on Enerzyz Processing of Customer Personal Data and supersede any prior data-processing terms.

18.6 Acceptance. This DPA is binding only when executed by authorised signatories or incorporated by exact title and version into an executed Principal Agreement. Mere website access or use before contract does not make this DPA binding. Electronic signatures and counterparts are valid.

Annex I — Details of Processing

Item	Description
Controller / exporter	The Customer for Customer Data.
Processor / importer	Enerzyz Pte. Ltd.
Subject matter	Energy platform operation, telemetry acquisition and analysis, optimisation, reporting and related account administration.
Duration	Term of the Principal Agreement plus the documented return, retention and deletion periods.
Purpose	Operation, security, optimisation, technical support, sustainability reporting and permitted de-identified service improvement.
Data Subjects	Authorised Users, facility and engineering contacts, client representatives, and other individuals whose business contact or access metadata is Processed. Guests and building occupants are not intentionally singled out.
Personal Data	Business names, roles, email addresses and phone numbers; user and authentication identifiers; IP, device, session, access and audit metadata; and aggregate occupancy signals.
Excluded data	Guest records, named room assignments, loyalty, payment, folio, reservation and check-in data; patient or clinical data; special categories; children's data; government identifiers; passwords, keys, certificates and network secrets.
Frequency	Continuous for Telemetry and periodic or on-demand for account, Console and support data.
Retention	Enerzyz data under Section 15.

Annex II — Technical and Organisational Measures

Domain	Measures
Governance	Documented security programme, risk assessment, threat modelling, incident management and assigned ownership.
Certification	Energyz Pte. Ltd. operates under the Energyz group information security management system, certified to ISO/IEC 27001:2022 (certificate GH60XXIX62026103, held by Energyz Inc.), verifiable on IAF CertSearch; certificate copy and scope supplied on request.
Architecture	Segregated customer environments and documented network boundaries. Four connection models (Unified API, Edge Mini, Edge Pro, Edge Max); no inbound listening port or inbound firewall rule on any Edge device; building-control traffic confined to the controls network; on the Edge Pro, forwarding and address translation between interfaces disabled, with a separate routing table per interface; Console access by outbound HTTPS. Connection model and network path stated per site.
Encryption	TLS 1.2 minimum and TLS 1.3 preferred in transit, with mutual TLS and per-device X.509 certificates between Edge and cloud; AES-256 at rest; keys generated and held in HSM-backed key management; device-bound, non-exportable private keys where the hardware supports it.
Identity and access	Role-based access, MFA or federated identity where supported, least privilege and joiner-mover-leaver controls.
Privileged support	No default Energyz engineering access to Customer Telemetry. Just-in-time elevation requires a named support ticket and dual approval (engineering lead and security lead), is limited to a maximum of 8 hours per grant, and is fully logged.
Logging	Tamper-evident, hash-chained audit records for configuration changes, commands, certificate events and privileged actions; SIEM export; monitoring and alerting. Platform audit logs retained for a minimum of 12 months, configurable up to 7 years.
Vulnerability management	Secure development, dependency and vulnerability review, severity-based remediation and patch cadence. CVSS-based triage; critical (9.0 and above) vulnerabilities remediated within 7 days in the cloud and 14 days in Edge firmware, with same-day notification to Customer administrators.
Resilience	Backups, tested recovery, monitored availability and controlled local buffering on Edge devices.
Personnel	Confidentiality, background checks where lawful, least privilege and security awareness.
Sub-processors	Due diligence, written flow-down, maintained register and change notification.
Deletion	Documented deletion and backup-expiry procedures; backup copies expire within 90 days.

Annex III — Sub-processors

The principal Sub-processors are listed below. The current, controlling list, with legal entities, services, hosting locations and transfer mechanisms, is the Energyz sub-processor register at energyz.com/sub-processors, from which the Customer may subscribe to change notifications under Section 9.3.

Provider	Service	Location	Transfer mechanism	Status
Amazon Web Services, Inc.	Enerzyz cloud infrastructure, storage and transactional email delivery	AWS Asia Pacific (Singapore) and AWS US East (Northern Virginia), or the region in the executed order	SCCs (Annex IV) or other lawful mechanism	Current
Google LLC	Cloud and managed data services for the production platform and Customer Data	Google Cloud (Singapore)	SCCs (Annex IV) or other lawful mechanism	Current
Enerzyz Affiliates (Enerzyz Inc.)	Engineering, support and operations	Singapore and the United States	Intra-group safeguards	Current
Twilio Inc.	Cellular connectivity for Edge Max	Per network coverage	SCCs (Annex IV) or other lawful mechanism	Current
Dropbox, Inc. (DocSend)	Contract and electronic-signature workflow	United States	SCCs (Annex IV) or other lawful mechanism	Current

Annex IV — Standard Contractual Clauses and Transfer Mechanisms

Clause or option	Completion
Modules	Module Two for Customer Data Processed by Enerzyz as Processor. Module One only for Section 2.3 Controller purposes.
Clause 7	Optional docking applies by written agreement.
Clause 9	Option 2 general written authorisation with Section 9 notice.
Clause 11	Optional independent dispute-resolution body not selected.
Clause 17	Law of the data exporter EU member state, or Ireland if the exporter is outside the EEA, unless otherwise specified.
Clause 18	Courts corresponding to Clause 17.
UK Addendum	Applies to UK transfers and is completed by reference to this DPA and the EU SCCs.
SCC Annexes	Completed by Annexes I, II and III of this DPA.
Transfer impact assessment	Required where applicable, with documented supplementary measures.

Annex V — Hospitality Data Boundary

For hotel and hospitality deployments, Enerzyz shall collect only asset and energy-relevant equipment Telemetry and aggregate occupancy signals needed for optimisation. It shall not collect, store, transmit or profile the following through the Enerzyz Platform:

- PMS or GRMS guest-record data
- guest names or contact details
- loyalty or membership data
- payment-card, folio or billing data
- reservations and check-in or check-out records
- individual guest tracking or behavioural profiles

Where a connected system exposes guest-identifying fields, Enerzyz shall consume only the energy-relevant signal and exclude the identifying fields at the integration boundary. A material breach of this Annex is a material breach of this DPA.

Execution

This DPA becomes binding when signed below or incorporated by exact title and version into an executed Principal Agreement.

For and on behalf of ENERZYZ PTE. LTD. (UEN 202620931G)

Signature: _____

Name: _____

Title: _____

Date: _____

For and on behalf of the CUSTOMER

Signature: _____

Name: _____

Title: _____

Date: _____