PUBLIC LEGAL FRAMEWORK

Privacy Policy

Personal data, customer information and individual rights

CONTROLLED DOCUMENT	EDITION DETAILS
Edition	1.0 - Approved for publication
Prepared	22 September 2026
Effective date	28 September 2026
Classification	Public policy
Document owner	Data Protection Officer
Publication approval	Site owner confirmation, 28 September 2026

ORYVEN SOLUTIONS PTE. LTD.

UEN 202643771N
7 Temasek Boulevard, #12-07
Suntec Tower One, Singapore 038987

Public privacy notice. Effective 28 September 2026. This document does not certify compliance.

Edition notice and revision history

Edition 1.0 approved for publication following the site owner's confirmation on 28 September 2026. Earlier working drafts were not approved editions. Publication does not itself establish customer acceptance, an operational control, legal review, or an executed DPO appointment.

Edition / date	Revision record	Approval status
1.0 / 28 Sep 2026	Full rewrite: separate Oryven's own processing from customer-directed processing; specific purposes, AI safeguards, individual rights and DPO contact; consistent document control.	Approved for publication

Approval and release

Required record	Entry
Approval record	Site owner confirmed finalisation in the website editing conversation.
Approval date	28 September 2026
Effective / publication date	28 September 2026
Superseded approved edition	None established in the records reviewed

Ongoing governance

Confirm the DPO appointment and monitored contact channel, actual categories of data and providers, processing locations, cookie inventory, AI use and retention arrangements. Align the notice with what Oryven actually does. Obtain appropriate Singapore legal review.

Version control

Use 1.1, 1.2 and later minor editions for administrative corrections or clarifications. Use 2.0 and later major editions for material changes to rights, obligations, purposes or controls. Record the actual changes, approver and effective date; retain the prior edition and any acceptance or notification evidence. A revision log does not substitute for legally required notice, consent or contractual agreement.

Document-control pages are retained with the signed or published PDF. Website HTML may present the operative notice with its current edition and effective date; retain the matching controlled master internally.

1. Who we are and what this notice covers

Oryven Solutions Pte. Ltd. (UEN 202643771N) ("Oryven", "we", "us" or "our") provides business software for inventory and operational workflow management. This notice explains our handling of personal data in connection with our website, enquiries, commercial relationships, authorised accounts, support and applicable Oryven services. It is intended to be read alongside our Cookie Policy and relevant customer agreements.

"Personal data" means information, whether true or not, about an individual who can be identified from it, or from it together with other information to which we have or are likely to have access. Business information that does not identify individuals is not necessarily personal data, but may still be protected by contractual confidentiality obligations.

Our products, including Oryven Horizon, Oryven Orbit and Oryven Aurora where supplied, are intended for business and professional use by laboratories, hospitals, clinics and distributors. Their intended purpose is inventory and operational administration, not medical diagnosis, treatment or clinical decision-making. They are not intended to hold patient medical records or clinical results. This purpose limitation does not mean that user accounts, support messages or technical records contain no personal data.

2. Our different roles

Oryven's own business activities. We determine the relevant purposes of processing for activities such as responding to enquiries, administering our customer relationships, billing, managing our own personnel and protecting our corporate systems. This notice explains the website, customer and business-contact activities. Separate employment or recruitment notices may provide additional information where relevant.

Customer-directed processing. Where we process personal data on behalf of and for the purposes of a customer under a written agreement, we act as a data intermediary to the extent that Singapore law recognises that role. The customer determines the relevant business purposes and authorised instructions. Our service agreement and applicable data-processing terms govern that processing, alongside our own legal obligations. Descriptions in this notice do not give us unrestricted rights to repurpose customer data.

An organisation may act in different roles for different activities. We do not treat all service information as our own data merely because it is stored on our platform. Conversely, the customer's responsibility does not remove obligations that apply directly to Oryven.

3. Information we handle and why

The categories below apply only where the relevant interaction or feature occurs. We do not require every category from every individual.

Interaction	Information involved	Principal purposes
Enquiry, demonstration or business meeting	Name, organisation, professional role, contact details, correspondence and information you choose to provide	Respond, arrange the requested interaction and prepare a relevant proposal
Customer and supplier administration	Business representatives, contract and invoice details, payment status and transaction references	Establish and manage the relationship, provide service communications, maintain accounts and meet legal requirements
Authorised service access	Account identifiers, permissions, organisational affiliation and authentication/security events	Provide access, implement customer permissions, support users and investigate misuse

Interaction	Information involved	Principal purposes
Support and troubleshooting	Ticket details, relevant communications, diagnostic records and limited data needed to reproduce a reported issue	Resolve the request, maintain reliability and protect the affected service
Website and system operation	IP address, browser or device characteristics, timestamps, access/security logs and applicable cookie identifiers	Deliver requested functions, secure systems, diagnose errors and, subject to applicable choices, measure usage
Customer-directed service use	Operational records and incidental personal data submitted by authorised users	Perform the contracted inventory/workflow service under the customer's lawful instructions

Where an enabled feature requires additional information, its configuration or accompanying notice will explain the relevant purpose before collection where required. We will not use a general reference to improvement as permission to collect unnecessary personal data or introduce an unrelated purpose without the necessary assessment and notice or consent.

4. Sources and information about other people

We obtain information directly from you, through your organisation or its authorised administrators, through use of our systems, and from service providers acting on our behalf. We may receive appropriate business contact information from lawful public or professional sources. Availability in a public source does not remove other applicable obligations.

When you provide information about another individual, provide only what is needed and ensure that you have the necessary authority and that required notices or permissions have been addressed. We may seek clarification, restrict use or reject information that is inappropriate for the service.

Business contact information supplied for business rather than solely personal purposes is treated differently under the PDPA. This does not mean that every record about an employee, every support message or every account-activity log is excluded from data protection requirements.

5. Consent and other permitted processing

We seek consent where required. Depending on the circumstances, Singapore law may permit processing based on deemed consent or a specific statutory exception, subject to its conditions. We assess those conditions rather than treating the existence of a contract or a business interest as an unrestricted permission to process data.

Reading this notice, browsing a page or accepting our contractual Terms and Conditions does not by itself give blanket consent to optional marketing, unrelated processing or all tracking technologies. Necessary service communications and optional marketing choices are distinguished.

We may use relevant information to meet legal obligations, respond to lawful requests, investigate security events, prevent misuse and establish or defend legal rights where permitted. A material new purpose will be assessed and notified, and consent obtained where required, before that processing begins.

6. Customer data and information that should not be submitted

Customers retain their rights in their own data. They should control what users submit, assign suitable access and avoid patient-identifiable information, medical records, clinical results, unnecessary identification

documents and unrelated sensitive information. Do not place third-party passwords, authentication codes or payment-card authentication data in messages or ordinary free-text fields.

An exceptional proposal to handle restricted information requires an expressly agreed scope, a data-protection and security assessment, and appropriate contractual safeguards before processing begins. A customer cannot authorise that change merely by uploading the information.

If inappropriate information is discovered, we will restrict unnecessary access and coordinate appropriate containment, lawful preservation and removal. We do not assume that deleting a record automatically resolves any incident or notification duty.

7. AI-assisted features and analytics

Where an AI-assisted feature is enabled, relevant input and service information may be processed to deliver that feature to the customer, subject to the service agreement and any applicable feature notice. Such processing may involve approved service providers where disclosed or contractually authorised. AI outputs can contain errors and require appropriate human review.

We will not use Customer Data, identifiable user content or customer-confidential materials to train or improve general-purpose models or models serving other customers without separate, explicit agreement addressing the purpose and applicable rights. Processing needed to deliver an authorised AI feature is not the same as permission for model training. A feature-specific training arrangement must be expressly described and approved before it is used.

We may use genuinely anonymised operational statistics for appropriate service analysis, provided that re-identification is not reasonably likely and customer confidentiality is respected. Pseudonymisation, removal of a name or aggregation of a very small group does not automatically make information anonymous.

8. Marketing and preferences

We may send relevant business marketing where permitted and where any required consent has been obtained. You may stop marketing by using the available unsubscribe mechanism or contacting our DPO. We will maintain a limited suppression record where needed to respect your choice and will not use that record to resume marketing.

Opting out of marketing does not stop communications genuinely necessary for an existing contract, account security or a requested transaction. We will not disguise promotional messages as mandatory service communications. Applicable Singapore direct-marketing and other relevant requirements are assessed for the intended communication channel and audience.

9. Cookies and similar technologies

Our Cookie Policy explains cookies, local storage, pixels and similar technologies, including their purposes and available choices. The applicable technology schedule identifies what is actually deployed; a generic category description is not a claim that a particular provider or tracker is in use.

Optional analytics and marketing tracking will be subject to the choices described in the Cookie Policy. Rejecting optional tracking will not be treated as refusal of necessary website functions. Technical security logs are not necessarily cookies and remain subject to appropriate purpose, access and retention controls.

10. Who may receive information

Information may be provided, only as reasonably required and lawfully permitted, to approved hosting and technology providers, email and communications providers, support contractors, payment or accounting

providers, and professional advisers. Providers processing on our behalf must have appropriate contractual obligations concerning permitted processing, confidentiality, security and incident handling.

An integration deliberately enabled by a customer may transmit the information needed for that integration to the selected third party. A provider acting independently may have its own notice and legal responsibilities. We remain responsible for obligations applicable to our own disclosures and to providers acting on our behalf; a third-party label is not a blanket exemption.

We may disclose relevant information to competent authorities where lawfully required or permitted, or in connection with a business transaction such as a merger or sale, with appropriate confidentiality and data-protection safeguards. We do not sell personal data. We do not authorise service providers to exploit customer content for their unrelated advertising or general model training.

11. International processing

Some approved providers or support arrangements may involve processing outside Singapore. A Singapore company address does not mean that all data stays in Singapore. Relevant hosting, support-access and onward-transfer locations must be assessed for the actual service.

Where Singapore's transfer requirements apply, we take the required steps to secure a comparable standard of protection, through appropriate binding safeguards or another permitted mechanism. Additional territorial requirements or customer commitments are addressed where applicable. Details relevant to a customer's implementation are governed by its agreed processing arrangements; we do not promise a particular residency location unless expressly agreed.

12. Security

We apply reasonable administrative, technical and organisational measures appropriate to the information and processing risks. The internal programme addresses access authorisation, tenant boundaries, authentication, secure transmission and storage where appropriate, secure development, vendor oversight, logging, backups and incident response. Controls must be proportionate to the actual system and its risks.

No system can guarantee that an incident will never occur. That limitation does not remove our legal or contractual duties. Customers also need to protect their devices, accounts, administrators and user permissions. We do not claim certification, a specific encryption implementation or a service level unless it has been verified and expressly stated for the relevant service.

13. Retention, return and deletion

We retain identifiable personal data only while it is needed for its notified purpose or another legitimate legal or business purpose. Retention decisions consider the relationship, statutory records, dispute or security needs and applicable contractual return/deletion obligations. We periodically review information that is no longer actively used.

When retention is no longer justified, we securely delete the information or remove the means of associating it with individuals. Customer service data follows the agreed export and deletion arrangements. Restricted backup copies may expire through controlled backup cycles rather than immediately; the applicable cycle must be established and must not be used as a reason for indefinite retention. Any legally required preservation remains access-restricted and purpose-limited.

14. Access, correction and other requests

Subject to applicable exceptions, you may request access to personal data about you in our possession or control and information about its use or disclosure during the preceding year. You may also request correction

of an error or omission. We verify identity proportionately and protect information about others; please do not email unnecessary identity documents or authentication secrets.

We respond as soon as reasonably possible. If an access or correction request cannot be completed within 30 days after receipt, we will inform you in writing within that period of when we can respond, as required. An access fee may be charged only where permitted and after informing you of the estimated fee. We do not charge for a correction request.

For customer-directed data, please contact the relevant organisation first where possible. If you approach us, we will route and assist with the request as appropriate without disregarding any obligation directly applicable to us. A request for personal data does not generally entitle a person to another customer's information, source code or entire proprietary documents; lawful rights and applicable exceptions govern the response.

You may also contact us about deletion, restriction or other rights that may apply under relevant law. This notice does not imply that every right available in another jurisdiction applies to every individual in Singapore.

15. Withdrawing consent and raising concerns

You may withdraw consent on reasonable notice for processing that depends on consent. We will explain likely consequences where applicable and cease the affected processing, including by relevant agents or intermediaries, unless another lawful basis permits or requires it to continue. Withdrawal does not invalidate prior lawful processing or necessarily require removal of records needed for a continuing legal purpose.

Questions, complaints, requests and suspected privacy incidents should be directed to our DPO. You may also approach the Personal Data Protection Commission or another competent authority where appropriate. We will not require you to waive a statutory right as a condition of making a request or complaint.

16. Incidents, external services and intended audience

We assess suspected personal-data breaches and make notifications required by applicable law. When acting as a data intermediary, we notify the relevant customer without undue delay as required and cooperate in its assessment. We do not wait for a complete forensic report before making a notification that is already due.

Independent websites reached through links have their own practices. Our services are designed for business and professional users, not consumer services directed to children. Please notify us if information inconsistent with the intended use has been submitted.

17. Contact and changes

Data Protection Officer
Oryven Solutions Pte. Ltd.
7 Temasek Boulevard, #12-07, Suntec Tower One, Singapore 038987
Email: dpo@oryvensolutions.com
Website: oryvensolutions.com

We may revise this notice as our activities or applicable requirements change. The current approved edition will identify its effective date. We will provide additional notice and obtain any required consent for material changes; publishing a revision does not retrospectively authorise an incompatible use. Mandatory legal rights prevail over conflicting language in this notice.