



Intravo Privacy and Data Protection Statement

SECURITY • PRIVACY • TRUST

Version: 1.0

Status: Published

Distribution: Public

Classification: Public

Policy owner: Adam Luz, Company Owner and Information Security Coordinator

Effective: September 24, 2026

Review cycle: At least annually and after a material legal, contractual, business, technology, vendor, risk, or security change

Public

Purpose

Explain how Intravo Corp governs personal data when acting as a controller or processor and how individuals and customers can exercise applicable privacy rights.

Scope

This statement covers personal data processed through Intravo websites, products, services, support, business operations, and contracted service providers. Customer-controlled data remains subject to the applicable customer agreement and data processing terms.

Policy requirements

- Intravo processes personal data for specified, lawful purposes and limits collection to data reasonably necessary for those purposes.
- Intravo documents applicable legal bases, honors contractual instructions when acting as a processor, and does not sell personal data.
- Personal data is protected through access controls, encryption, secure configuration, monitoring, incident response, and retention limits proportionate to risk.
- Retention is based on business, legal, security, and contractual requirements. Data is securely deleted or de-identified when no longer required, subject to lawful preservation obligations and backup lifecycles.
- International transfers require an approved legal mechanism and the regional restrictions in Intravo's Data Residency and International Transfer Standard.
- Subprocessors are subject to risk review and written privacy and security obligations. Intravo remains responsible for managing its processor obligations.

Roles and responsibilities

- **Company Owner and Information Security Coordinator:** Approves this document, assigns control owners, resolves material risk decisions, and ensures appropriate resources and oversight.
- **System, service, process, and data owners:** Implement applicable requirements, maintain records, test controls, and remediate deficiencies.
- **Managers:** Grant work and access only to trained, authorized personnel and escalate exceptions, incidents, and overdue actions.
- **All personnel:** Follow this document, protect information and systems, complete required training, and report suspected failures promptly.
- **Vendors and contractors:** Meet applicable contractual requirements and provide requested assurance evidence.

Operating procedure

1. Privacy questions and rights requests may be submitted to privacy@intravo.com. Intravo verifies identity and authority before disclosing, correcting, exporting, restricting, objecting to, or deleting personal data.
2. When Intravo is a processor, requests concerning customer-controlled data are referred to or coordinated with the relevant customer unless law permits a direct response.
3. Intravo assesses privacy incidents promptly and supports required customer or regulator notifications within applicable deadlines.

Monitoring and evidence

Control owners retain evidence in approved systems according to the Document Retention Policy. Evidence includes:

- Request intake and identity-verification record.
- Response and fulfillment record.
- Record of processing activities.
- Data protection impact assessments.
- Vendor and transfer assessments.

Material deficiencies, missing evidence, repeated failures, and overdue corrective actions are recorded in the risk or remediation register and reported to the Company Owner.

Exceptions and enforcement

Exceptions require a documented business need, exact scope, risk assessment, compensating controls, owner, approver, expiration date, and review schedule. An exception does not waive legal, contractual, or customer obligations. Violations may result in access restriction, corrective action, contract remedies, or discipline up to termination of employment or engagement.

Related standards

- EU General Data Protection Regulation 2016/679
- EDPB guidance
- Applicable US privacy laws and customer contracts

Document control

The controlled copy and revision history in the Intravo compliance portal are authoritative. Printed or downloaded copies are uncontrolled after export. This document does not, by itself, represent a SOC 2 attestation, regulatory certification, or legal opinion.

Version 1.0 — Effective September 24, 2026. Comprehensive 2026 review, current brand, current control framework, and publication-ready organization.