



Intravo Data Residency and International Transfer Standard

SECURITY • PRIVACY • TRUST

Version 1.0

Status: Published

Distribution: Public

Portal version: 1.0

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

Effective: September 24, 2026

Public

Purpose and decision

Intravo Corp operates services in the United States and European Union. This standard establishes a verifiable regional-processing rule: EU-origin customer content and personal data remain within approved EU processing and storage paths. Some US-origin data may be processed in the EU when contracts and law allow it. EU-origin data does not enter US production, storage, backup, observability, analytics, support, or AI paths unless a documented exception is approved before the transfer.

This standard is intentionally stricter than the GDPR minimum. A DPA, Standard Contractual Clauses, adequacy mechanism, BAA, certification, or encryption may support a lawful transfer, but none replaces an Intravo or customer residency commitment.

Scope

This standard applies to customer content, personal data, confidential information, system metadata that can identify a person or customer, and derived data across:

- Web, application, API, database, file, object, cache, queue, search, and AI services.
- Backups, snapshots, replicas, disaster recovery, exports, support bundles, and test data.
- Logs, traces, metrics, session replay, crash data, security telemetry, and audit records.
- Vendors, subprocessors, content delivery networks, managed services, and support access.
- Production, staging, development, analytics, and incident-response workflows.

Definitions

EU-origin data means data submitted by, collected from, or generated about a person, customer, event, meeting, device, or workload assigned to the EU regional path. The routing decision is based on the contracted customer region or workload tenant, not merely the current IP address of an end user.

EU region means infrastructure physically and contractually restricted to locations in the European Union or another specifically approved European jurisdiction. United Kingdom processing is separately evaluated and is not automatically treated as EU processing.

Transfer includes copying, replication, remote access, support access, disclosure, backup, observability export, or making data available to a person or system outside the approved region.

Customer content includes uploaded material, meeting audio, transcripts, notes, files, attendee information, support content, application records, and derived outputs.

Regional routing rules

1. Every production tenant, customer, event, meeting, or workload that can contain customer data must have an authoritative region assignment.
2. EU assignments route to EU application, database, storage, cache, queue, search, AI, backup, recovery, and observability services.
3. EU-origin data may not fail over to a US region. When EU capacity is unavailable, the service must fail closed, degrade safely, or use an approved EU recovery region.
4. US assignments may use approved US or EU regions when contracts, notices, and applicable law permit it.
5. Region selection may not depend solely on DNS geolocation or a transient client IP. Customer configuration or tenant metadata controls the decision.
6. Test and development environments may not use production personal data unless specifically approved, minimized, protected, regionally compliant, and deleted after the test.

Storage backup and deletion

EU-origin data, replicas, snapshots, and backups are stored only in approved EU locations. Backup catalogs and encryption-key metadata must not expose customer content outside the region.

Backups are encrypted, access-controlled, monitored, and tested. Recovery testing must prove that EU backups restore into an approved EU environment without first passing through US infrastructure.

Retention and deletion apply to active data, backups, replicas, caches, queues, search indexes, derived AI outputs, exports, and observability records. Systems must assign an expiration at creation or through another failure-resistant lifecycle mechanism. Deletion must not depend only on a successful terminal callback.

Logging monitoring and observability

IP addresses, user identifiers, email addresses, meeting identifiers, request paths, traces, session data, and security events may be personal or customer-linked data. EU workload telemetry therefore follows the EU path unless it is irreversibly anonymized before export.

EU workload logs, traces, and identifiable metrics must not be sent to a US-hosted observability site. Intravo must use one of these approved patterns:

- An EU-hosted observability organization for EU telemetry, with separate API keys, agents, forwarders, archives, access controls, monitors, and retention.
- An EU-hosted logging service that meets the same monitoring and evidence requirements.
- Local minimization or irreversible anonymization that removes personal and customer-identifying data before any US export, supported by documented testing and approval.

Operational dashboards may aggregate nonidentifying health indicators across regions. Cross-organization visibility must not copy underlying EU personal data to the US organization.

Edge and serverless processing

EU hostnames handling EU-origin data require contractual and technical regional controls for TLS termination, inspection, serverless execution, logs, analytics, storage, and downstream services.

Regional ingress or execution controls do not automatically regionalize every trigger, outgoing subrequest, storage service, queue, scheduled job, AI service, analytics system, or other bound service. Each component requires product-specific confirmation and testing.

EU-origin prompts, transcripts, files, embeddings, or model outputs may be sent to an AI service only when Intravo has written confirmation that inference, storage, logging, support, and subprocessors remain within the approved EU path. If that confirmation is unavailable, the application must block the EU AI path or use an approved EU-hosted model.

Administrative and support access

Routine access to EU-origin customer data is limited to personnel and systems approved for the EU environment. Access from the United States is treated as an international transfer risk, even when the data remains stored in an EU data center.

Administrative tooling must use least privilege, MFA, compliant managed devices, time-bound elevation where feasible, and full audit logging. Support workflows should expose minimized or pseudonymized information. Emergency access must be approved, time-limited, logged, reviewed, and disclosed when required by contract or law.

Vendors and subprocessors

Before an EU workload uses a vendor, Intravo verifies:

- Contractual processing scope and Article 28 terms where applicable.
- Hosting, backup, support, log, analytics, and subprocessor locations.
- Whether remote access from a non-EU jurisdiction is possible.
- Deletion, return, breach notification, audit, and subprocessor-change terms.
- Applicable transfer mechanism and transfer-impact assessment if a transfer is contemplated.
- Independent assurance and the product-specific scope of that assurance.

A vendor's general SOC 2 report, DPA, BAA, ISO certificate, or marketing statement is not proof that a specific product or feature satisfies this standard.

International transfer exceptions

The default is no EU-to-US transfer. A proposed exception must be approved before processing and must include:

- Business necessity and why an EU-only alternative is not reasonably available.
- Data categories, data subjects, volume, frequency, recipients, locations, and retention.
- Controller or processor role and customer authorization.
- Applicable GDPR Chapter V mechanism, such as an adequacy decision or Standard Contractual Clauses.
- A transfer-impact assessment and effective supplementary safeguards.
- Encryption, pseudonymization, minimization, access restrictions, logging, and deletion controls.
- An owner, expiration date, review date, and exit plan.

If Intravo cannot demonstrate essentially equivalent protection or meet a contractual residency commitment, the transfer does not proceed.

Architecture and change control

Regional data-flow diagrams are required for systems processing customer data. Diagrams identify ingress, services, stores, backups, observability, administration, vendors, AI, and deletion paths.

Infrastructure as code, deployment configuration, and automated tests should enforce approved regions and prevent accidental cross-region replication. Material changes to a region, vendor, storage service, telemetry destination, backup, support model, or AI service require security and privacy review before release.

Evidence and testing

The following evidence is retained for each in-scope service:

- Region assignment and routing configuration.
- Current data-flow diagram and subprocessor list.
- Cloud account, database, storage, backup, key, CDN, and observability region exports.
- Tests showing an EU tenant reaches only the approved EU endpoints and stores.
- Tests showing an EU outage does not fail over to the US.
- Backup restore and deletion evidence.
- Administrative-access logs and quarterly access reviews.
- Vendor contracts, DPAs, transfer mechanisms, transfer-impact assessments, and residency confirmations.
- Exceptions, approvals, expiration, and remediation.

Testing occurs before production, at least annually, and after material changes. Exceptions and failed tests enter the risk and remediation registers.

References

- GDPR official text, including Articles 5, 25, 28, 30, 32, 35, and Chapter V:
<https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- European Data Protection Board guidance on international transfers:
https://www.edpb.europa.eu/topics/international-transfers-and-international-cooperation_en

Approval record

Role	Name	Decision	Date
Company Owner and Information Security Coordinator	Adam Luz	Approved for publication	September 24, 2026
Legal and privacy review where required	Case-specific reviewer	Required before a qualifying transfer exception	Per exception

Revision history

Version	Date	Description
1.0	September 24, 2026	Established EU-only processing and storage requirements, controlled US-to-EU processing, international-transfer governance, and regional observability requirements