ResolvX

Privacy Programme

Privacy Policy · ROPA · Data Subject Request Process

POL-006 · v1.0 · 2026 · Internal — Restricted

Document Information

Policy ID	POL-006
Version	1.0
Status	Active
Classification	Internal — Restricted
Owner	GRC Lead / Legal
Approver	CISO
Review Cycle	Annual
Next Review	Q1 2027
Frameworks	ISO 27001:2022 A5.34 · GDPR Art.5,6,13–22,28,30,32–34 · SOC 2 P1–P8 · NIST CSF ID.AM-07

ResolvX — Privacy Programme: Policy, ROPA & DSR Process

Part A — Privacy Policy

A.1 Purpose

This document establishes ResolvX's privacy programme, the governance framework, principles, and operational processes by which ResolvX manages personal data responsibly, lawfully, and transparently. It covers ResolvX's role as both a **data controller** (for employee and prospect data) and a **data processor** (for client data entrusted to ResolvX to operate dispute resolution workflows on behalf of regulated financial institutions).

Privacy is not a compliance checkbox. For ResolvX's enterprise clients, banks, payment processors, and financial institutions, confidence in ResolvX's data handling is a commercial prerequisite. This programme exists to earn and maintain that confidence.

A.2 Scope

This policy applies to all personal data processed by ResolvX, including:

- Employee data: HR records, payroll, performance, health information (if any).
- Client data (processed as data processor): Personal data of dispute parties (consumers) provided by clients under data processing agreements such as names, account details, transaction histories, contact information.
- Prospect and marketing data (controller): Contact details of sales prospects and website visitors.
- Vendor contact data: Personal details of vendor contacts processed in the course of commercial relationships.

This policy applies to all ResolvX personnel, and all systems used to process personal data.

A.3 Privacy Principles

ResolvX's processing of personal data is governed by the six GDPR principles (Article 5), applied as operational standards:

Principle	GDPR Article	ResolvX Application
Lawfulness, fairness, transparency	Art. 5(1)(a)	Every processing activity has a documented lawful basis; privacy notices published
Purpose limitation	Art. 5(1)(b)	Data collected for specified purposes; no secondary use without separate legal basis
Data minimisation	Art. 5(1)(c)	Only data necessary for the processing purpose is collected or retained
Accuracy	Art. 5(1)(d)	Processes in place to ensure data is accurate and kept up to date

Storage limitation	Art. 5(1)(e)	Retention schedule enforced; data deleted promptly at end of retention period
Integrity and confidentiality	Art. 5(1)(f)	Technical and organisational measures (TOMs) implemented per the ISMS

A.4 Lawful Bases for Processing

ResolvX processes personal data only where a valid lawful basis exists. The applicable bases by processing activity are documented in the ROPA (Part B). The primary lawful bases are:

Lawful Basis	GDPR Article	Primary Use at ResolvX
Contract	Art. 6(1)(b)	Processing employee data to fulfil employment contracts; processing client-provided consumer data to deliver contracted services
Legitimate interests	Art. 6(1)(f)	Marketing to business prospects; fraud and security monitoring; service improvement analytics
Legal obligation	Art. 6(1)(c)	Tax, employment law, regulatory compliance requirements
Consent	Art. 6(1)(a)	Where no other basis applies and individual consent is freely given, specific, informed, and unambiguous

Where special category data (Art. 9) is processed, an additional condition from Article 9(2) is required. ResolvX does not intentionally process special category data; any inadvertent receipt must be flagged to the GRC Lead and Legal immediately.

A.5 Data Subject Rights

ResolvX respects and facilitates the exercise of data subject rights under GDPR Articles 15–22. These rights and ResolvX's obligations are:

Right	GDPR Article	ResolvX Obligation	Response Deadline
Right of access (SAR)	Art. 15	Provide a copy of personal data held and processing information	1 month (extendable to 3 months for complex requests)
Right to rectification	Art. 16	Correct inaccurate or incomplete data	1 month
Right to erasure ("right to be forgotten")	Art. 17	Delete data where no overriding retention obligation exists	1 month
Right to restriction	Art. 18	Restrict processing pending resolution of accuracy or objection	Promptly

Right to data portability	Art. 20	Provide data in a structured, machine-readable format	1 month
Right to object	Art. 21	Cease processing for direct marketing immediately; assess other objections	Promptly (marketing: immediate)
Rights related to automated decision-making	Art. 22	Not to be subject to solely automated decisions producing legal effects without human review	N/A unless applicable

Data Subject Requests are handled per the DSR Process (Part C of this document). All DSRs are logged and tracked to resolution.

A.6 Cross-Border Data Transfers

Personal data originating in the European Economic Area (EEA) must not be transferred to third countries without adequate safeguards. ResolvX ensures:

- All AWS data processing occurs within EU regions (eu-west-1 or equivalent) for EU personal data.
- Standard Contractual Clauses (SCCs - 2021 EU Commission version) are executed with all vendors receiving EEA personal data located outside the EEA.
- The sub-processor register (maintained by Legal) documents all cross-border transfers and their legal mechanism.
- Transfer Impact Assessments (TIAs) are conducted where SCCs are relied upon for transfers to high-risk jurisdictions.

A.7 Privacy by Design and Default

ResolvX implements privacy by design in all new product development, system changes, and business processes involving personal data:

- Privacy considerations are raised at project initiation not after implementation.
- Data Privacy Impact Assessments (DPIAs) are conducted for processing activities likely to result in high risk to individuals (as defined in GDPR Art. 35 and EDPB guidelines).
- Default system configurations collect the minimum personal data required.
- The GRC Lead and Legal must be consulted before launching new processing activities or materially changing existing ones.
- Data minimisation is considered at the architecture stage, data that is not collected cannot be breached.

A.8 Technical and Organisational Measures (TOMs)

ResolvX implements the following TOMs to protect personal data, as required by GDPR Article 32:

Category	Measure
Encryption	AES-256 at rest; TLS 1.3 in transit across all systems handling personal data
Access control	Role-based; least privilege; MFA; quarterly access reviews (per POL-003)
Pseudonymisation	Applied where feasible for analytics and testing environments
Resilience	AWS multi-AZ deployment; automated backups; DR plan with tested RTO/RPO
Restoration	Backup restoration tested quarterly; integrity checks automated
Review process	Annual security assessment and penetration test; continuous vulnerability scanning

TOMs are documented and evidenced in the ISMS controls framework. They are reviewed annually and after any significant incident or system change.

A.9 Data Breach Management

A personal data breach is any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Detection and assessment: All suspected breaches must be reported to the GRC Lead immediately upon discovery.

Notification obligations:

Breach Type	Obligation	Timeline
Breach likely to result in risk to individuals	Notify supervisory authority (relevant DPA)	Within 72 hours of becoming aware
Breach likely to result in high risk to individuals	Notify affected data subjects directly	Without undue delay
Breach with no risk to individuals	Document internally; no notification required	N/A

ResolvX's **primary supervisory authority** is the Irish Data Protection Commission (DPC) (as lead SA for EU operations). Other SAs may have jurisdiction depending on data subject location.

When ResolvX is acting as a **data processor**, it must notify the relevant controller without undue delay upon becoming aware of a breach, contractual timelines apply (typically 24–72 hours).

All breaches and near misses are logged in the Breach Register maintained by the GRC Lead. Breach logs are retained for a minimum of 5 years.

A.10 Roles and Responsibilities

Role	Privacy Responsibility
GRC Lead	Owns the privacy programme; maintains ROPA; manages DSR process; conducts DPIAs; manages breach register; oversees sub-processor register
Legal	DPA review and negotiation; SCC and transfer mechanism oversight; regulatory notifications and correspondence; sub-processor register co-maintenance
IT Admin / Head of Cloud Ops	Implements technical TOMs; supports data subject requests requiring system-level extraction or deletion
All Personnel	Report suspected breaches and DSRs promptly; handle personal data per this policy; complete annual privacy awareness training

ResolvX does not currently meet the threshold for mandatory appointment of a Data Protection Officer (DPO) under GDPR Art. 37. However, the GRC Lead performs the functional role of DPO-equivalent and is the primary point of contact for privacy matters.

Part B — Record of Processing Activities (ROPA)

This ROPA is maintained in accordance with GDPR Article 30. As data controller and data processor, ResolvX maintains separate registers.

B.1 ResolvX as Data Controller

#	Processing Activity	Purpose	Lawful Basis	Data Categories	Data Subjects	Retention	Third Party Recipients	Int'l Transfer?
C-01	Employee HR management	Employment administration, payroll, performance management	Contract (Art. 6(1)(b)); Legal obligation (Art. 6(1)(c))	Name, contact, employment history, payroll, performance records, emergency contacts	Employees	Duration + 7 years	HRIS provider, payroll processor, pension provider	Depends on vendor location; SCCs where applicable
C-02	Recruitment	Candidate assessment and selection	Legitimate interests (Art. 6(1)(f)); Pre-contract (Art. 6(1)(b))	Name, CV, contact, interview notes	Applicants	6 months post-decision (unsuccessful); duration of employment + 7 years (successful)	ATS provider	SCCs where applicable
C-03	Sales and marketing (B2B)	Pipeline management; marketing communications	Legitimate interests (Art. 6(1)(f))	Business name, job title, business email, phone	Business contacts / prospects	Active pipeline + 2 years	CRM provider	SCCs where applicable
C-04	Website analytics	Improving website experience and content	Consent (Art. 6(1)(a)) where cookies used	IP address, browser data, page visits	Website visitors	13 months	Analytics provider	SCCs where applicable
C-05	Vendor contact management	Supplier relationship management	Legitimate interests (Art. 6(1)(f))	Name, job title, business email, phone	Vendor contacts	Duration of contract + 2 years	None	N/A
C-06	Security monitoring and logging	Information security; fraud prevention; incident response	Legitimate interests (Art. 6(1)(f)); Legal obligation (Art. 6(1)(c))	System access logs, authentication events, IP addresses	All personnel, system users	12 months	SIEM provider (if applicable)	SCCs where applicable

B.2 ResolvX as Data Processor

#	Processing Activity	Purpose	Controller	Lawful Basis (Controller's)	Data Categories	Data Subjects	Retention	Sub-processors	Int'l Transfer?
P-01	Dispute case management	Processing financial dispute cases on behalf of financial institution clients	Financial institution clients (named per DPA)	Contract / legal obligation (varies by controller)	Dispute party name, contact, account number, transaction records, correspondence	Consumers (dispute parties)	Per client DPA; typically 7 years from case close	AWS (infrastructure), Okta (access control)	AWS EU regions; SCCs in place
P-02	Client reporting	Generating dispute outcome reports and analytics for clients	Financial institution clients	Contract / legitimate interests	Aggregated case data; limited individual-level data	Consumers (dispute parties)	Per client DPA	AWS	AWS EU regions
P-03	Client onboarding data	Processing client entity and contact data during onboarding	ResolvX (controller)	Contract	Client company contacts	Client staff	Duration of contract + 2 years	CRM, email	SCCs where applicable

The sub-processor register is maintained separately by Legal and updated within 30 days of any change.

Part C — Data Subject Request (DSR) Process

C.1 Overview

A Data Subject Request (DSR) is any request by an individual exercising their rights under GDPR Articles 15–22 (or equivalent rights under CCPA, UK GDPR, or other applicable law). ResolvX is committed to responding to all DSRs within the statutory deadline.

C.2 DSR Intake

DSRs may be received through:

- Direct email to the GRC Lead or Legal
- Client portal (for consumer dispute parties submitting requests via the client)
- Post (physical mail to registered address)
- Any member of staff verbally or in writing (must be forwarded to GRC Lead immediately)

All DSRs must be forwarded to the GRC Lead within 24 hours of receipt, regardless of channel.

C.3 Identity Verification

Before processing a DSR, the identity of the requester must be verified to prevent fraudulent or mistaken disclosure. Verification is proportionate to the sensitivity of the data:

- For employee DSRs: confirm via HR records and internal identity verification
- For consumer dispute party DSRs: verify against case data (name + account reference or case number)
- For other individuals: request one piece of identifying information consistent with the data held; do not demand excessive documentation

Verification must be completed without undue delay. Requesting verification does not extend the response deadline if the requester provides the requested information promptly.

C.4 DSR Handling by Request Type

Access Requests (Subject Access Requests — SARs):

- GRC Lead searches all systems for data held about the individual (HR systems, case management, CRM, email, access logs)
- Data is compiled and reviewed for any legitimate redaction grounds (e.g., third-party data, legal privilege, law enforcement holds)
- Response provided in a clear, accessible format typically PDF or secure email
- Response includes: categories of data, purposes of processing, recipients or categories of recipients, retention periods, information on data subject rights

Erasure Requests:

- GRC Lead reviews whether any retention obligation or overriding legitimate interest applies
- Where no basis for retention exists, coordinate with IT Admin and Head of Cloud Ops to delete data from all systems including backups (on scheduled backup purge cycle)
- Confirm deletion in writing; document in DSR log
- Where retention basis applies, notify requester with explanation and their right to lodge a complaint with the supervisory authority

Rectification Requests:

- Review the inaccuracy claimed
- Correct data in all systems where held
- Notify sub-processors or third parties who received the inaccurate data
- Confirm rectification in writing

Portability Requests:

- Extract data in structured, commonly used, machine-readable format (JSON or CSV preferred)
- Provide securely (encrypted email or secure file transfer)
- Where technically feasible and requested, transfer directly to named third party

C.5 Processor DSRs

When ResolvX receives a DSR relating to data processed on behalf of a client (ResolvX as data processor), ResolvX must:

- Notify the relevant client (data controller) immediately, within 48 hours
- Not respond directly to the data subject without client authorisation, unless required by law
- Assist the client in fulfilling the request, including by extracting, correcting, or deleting data from ResolvX's systems as directed by the controller

C.6 DSR Log

The GRC Lead maintains a DSR Log recording:

- Date received
- Type of request
- Requester identity (anonymised in public-facing records)
- Verification status
- ResolvX role (controller or processor)
- Status and response date
- Outcome

The DSR Log is reviewed quarterly and retained for 5 years as evidence of compliance.

C.7 Complaints and Escalation

If a data subject is dissatisfied with ResolvX's response to a DSR, they have the right to:

- Escalate to the GRC Lead for internal review
- Lodge a complaint with the relevant supervisory authority (Irish DPC for EU; ICO for UK; relevant state AG for CCPA)
- Seek judicial remedy

All complaints received are logged and investigated. Material complaints are reported to the CISO.

Document Control

Field	Detail
Policy ID	POL-006
Version	1.0
Status	Active
Classification	Internal — Restricted
Owner	GRC Lead — Derick G. Dmello
Co-owner	Legal
Approver	CISO
Review Cycle	Annual, or upon material change to processing activities or regulatory landscape
Next Review	Q1 2027
Framework References	ISO/IEC 27001:2022 A5.34 · GDPR Art. 5, 6, 13–22, 24, 25, 28, 30, 32–34 · CCPA Cal. Civ. Code §1798 · SOC 2 TSC P1–P8 · NIST CSF 2.0 ID.AM-07, GV.PO
Related Policies	POL-001 (IS Policy), POL-004 (Data Classification), POL-005 (Vendor Management)

ResolvX GRC Program — Internal Use Only — v1.0 — 2026

This document contains the Privacy Policy, Record of Processing Activities (ROPA), and Data Subject Request (DSR) Process for ResolvX.

Authorisation

Role	Name	Date
CEO		
CISO		
GRC Lead	Derick G. Dmello	