

P3 Audit Limited

Resolut™ Privacy Policy

Version 1.0

Legal Entity: P3 Audit Limited

Product Platform: Resolut™

Status: Approved 31 July 2026.

Important Notice

This Privacy Policy is intended to provide a framework for explaining how P3 Audit Limited processes personal information through the Resolut platform and associated services.

This Privacy Policy does not replace:

- customer-specific privacy notices;
 - contractual data processing agreements;
 - data-sharing agreements;
 - jurisdiction-specific legal obligations; or
 - regulatory guidance applicable to particular organisations.
-

1. Introduction

P3 Audit Limited ("**P3 Audit**", "**we**", "**us**", or "**our**") respects your privacy and is committed to protecting personal information.

This Privacy Policy explains how P3 Audit collects, uses, stores, shares and protects personal information when individuals and organisations access or use:

- the Resolut™ platform;
- Resolut websites;
- Resolut applications;
- Resolut portals;
- Resolut APIs;
- related services; and
- future products or services made available under the Resolut brand.

Resolut is a compliance, trust and resilience platform designed to help individuals and organisations demonstrate responsible data stewardship through controlled information sharing, verification and trusted relationships.

2. Who We Are

For the purposes of applicable privacy and data protection legislation, including the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018, the organisation responsible for processing personal information depends upon the circumstances in which Resolut is used.

The legal entity providing Resolut is:

P3 Audit Limited

Registered Office: 71-75 Shelton Street, London, WC2H 9JQ

Company Registration Number: 10838544

United Kingdom

Privacy Contact: privacy@p3audit.com

3. Why Resolut Exists

P3 Audit was founded in 2017 with a specific focus on helping organisations demonstrate responsible handling of personal information and comply with evolving privacy obligations.

The original focus was supporting organisations operating complex workforce and supply-chain environments, including:

- payroll providers;
- business process outsourcing organisations;
- employers;
- service providers; and
- organisations processing personal information across international boundaries.

Through this work, P3 Audit identified a fundamental challenge:

Traditional compliance models often require organisations to collect, duplicate and store increasing volumes of personal information and supporting evidence across multiple systems.

This creates additional:

- privacy risk;

- security exposure;
- administrative burden;
- compliance complexity; and
- uncertainty regarding ownership and control of information.

Resolut was created to support a different approach.

The platform is based on the principle that:

Individuals should have greater transparency and control over how their personal information participates in professional, commercial and organisational relationships.

Resolut enables organisations and individuals to establish trusted relationships while reducing unnecessary duplication and uncontrolled distribution of personal information.

4. Our Privacy Philosophy

Resolut has been designed around the principles of:

4.1 Privacy by Design and Default

Privacy protection is embedded into the design philosophy of the platform.

Resolut seeks to support:

- responsible information sharing;
- appropriate access control;
- data minimisation;
- transparency;
- accountability; and
- security.

4.2 Data Subject Empowerment

Individuals are not merely records within organisational systems.

Personal information relates to real people who should understand:

- how their information is used;
- who may access it;
- why access exists;

- what relationships exist; and
- how permissions may change.

Resolut supports greater transparency between individuals and organisations while recognising the legal responsibilities of organisations acting as data controllers and processors.

4.3 Reducing Unnecessary Data Duplication

Traditional compliance approaches frequently rely on multiple organisations collecting identical information.

Resolut is designed to reduce unnecessary duplication by supporting:

- controlled information sharing;
 - verification;
 - relationship-based compliance;
 - permission management; and
 - evidence of trusted interactions.
-

4.4 Responsible Data Stewardship

P3 Audit believes that effective privacy management requires organisations to demonstrate responsible stewardship of information.

Resolut supports organisations by enabling them to maintain clearer visibility of:

- compliance obligations;
 - information relationships;
 - permissions;
 - verification status;
 - accountability records; and
 - governance activities.
-

5. Scope of This Privacy Policy

This Privacy Policy applies to individuals and organisations using or interacting with Resolut, including:

- individual users;

- professional subscribers;
- organisational users;
- administrators;
- employees;
- contractors;
- suppliers;
- customers;
- auditors;
- certification bodies;
- regulatory participants;
- authorised representatives; and
- other approved users.

This Privacy Policy applies when you:

- create a Resolut account;
- access or use the platform;
- subscribe to services;
- communicate with P3 Audit;
- request support;
- participate in demonstrations or trials;
- interact with our websites;
- receive communications from us; or
- otherwise engage with P3 Audit.

6. Definitions

For the purposes of this Privacy Policy:

6.1 Personal Data

"Personal Data" means information relating to an identified or identifiable individual.

This includes equivalent concepts such as:

- personal information;

- personally identifiable information ("PII"); or
 - other protected personal information defined under applicable privacy laws.
-

6.2 Customer Data

"Customer Data" means information submitted, uploaded, created or managed by a Customer through Resolut.

Customer Data may include personal information belonging to employees, contractors, suppliers, customers or other individuals connected to the Customer's activities.

6.3 Trust Data

"Trust Data" means information generated through the operation of Resolut to support verification, accountability and trusted relationships.

Trust Data may include:

- verification records;
- acknowledgement records;
- permissions;
- approval history;
- relationship information;
- compliance status;
- timestamps;
- audit trails; and
- evidence of interactions.

Where Trust Data contains Personal Data, it remains subject to applicable privacy obligations.

6.4 Platform Data

"Platform Data" means information generated through operation, security and improvement of Resolut.

Examples include:

- technical logs;
- system performance information;

- security information;
 - usage analytics;
 - operational records.
-

7. Privacy Roles and Responsibilities

Depending on how Resolut is used, P3 Audit may act as either a Data Controller or Data Processor.

7.1 P3 Audit as Data Controller

P3 Audit acts as a Data Controller where we determine the purpose and means of processing information.

Examples include:

- managing user accounts;
 - providing customer support;
 - processing subscriptions;
 - maintaining platform security;
 - improving Services;
 - managing our business relationship;
 - communicating service updates; and
 - complying with legal obligations.
-

7.2 P3 Audit as Data Processor

P3 Audit may act as a Data Processor where a Customer uses Resolut to manage its own compliance, workforce, supplier or relationship information.

In those circumstances:

- the Customer determines the purpose of processing;
 - the Customer remains responsible as Data Controller;
 - P3 Audit processes information according to Customer instructions;
 - applicable processing agreements may apply.
-

7.3 Customer Responsibilities

Customers using Resolut remain responsible for ensuring that:

- Personal Data is collected lawfully;
- appropriate privacy notices are provided;
- permissions are obtained where required;
- information shared through Resolut is accurate;
- processing complies with applicable laws.

PART 2

Personal Data Collection and Processing

8. Sources of Personal Data

P3 Audit may collect Personal Data from the following sources.

8.1 Directly From Individuals

We may collect information when you:

- create an account;
 - complete registration details;
 - update your profile;
 - subscribe to services;
 - request information;
 - contact support;
 - provide feedback;
 - participate in demonstrations;
 - communicate with us.
-

8.2 From Organisations

Where you access Resolut through an organisation, we may receive information from:

- your employer;
- contracting organisation;
- customer;
- supplier;
- auditor;
- certification body;
- authorised administrator.

Examples may include:

- name;
 - role;
 - professional information;
 - organisation affiliation;
 - permissions;
 - compliance responsibilities.
-

8.3 From Other Resolut Participants

Resolut supports trusted relationships between participants.

Personal Data may therefore be provided by another authorised participant where:

- a relationship exists;
 - appropriate permissions are established;
 - sharing supports a legitimate purpose;
 - applicable privacy requirements are satisfied.
-

8.4 Automatically Collected Information

When you use Resolut, we may collect technical information including:

- IP address;
- device information;
- browser information;
- operating system;
- access timestamps;
- security logs;
- usage information;
- diagnostic information.

This information supports:

- platform security;
- reliability;
- troubleshooting;

- service improvement.
-

9. Categories of Personal Data Processed

Depending on how Resolut is configured and used, categories of Personal Data may include:

9.1 Identity Information

Including:

- name;
 - username;
 - account identifier;
 - profile information;
 - professional role.
-

9.2 Contact Information

Including:

- email address;
 - telephone number;
 - business address;
 - communication preferences.
-

9.3 Account Information

Including:

- subscription information;
 - authentication information;
 - user preferences;
 - access permissions.
-

9.4 Professional Information

Depending on Customer requirements, this may include:

- qualifications;
 - certifications;
 - registrations;
 - training records;
 - employment-related information;
 - compliance-related information.
-

9.5 Verification and Trust Information

Resolut may process information relating to trusted relationships, including:

- verification status;
 - acknowledgement records;
 - approval history;
 - permissions;
 - relationship information;
 - compliance records;
 - audit activity;
 - timestamps.
-

10. Lawful Basis for Processing Personal Data

P3 Audit processes Personal Data only where an appropriate lawful basis exists under applicable privacy legislation.

10.1 Contractual Necessity

We may process Personal Data where necessary to:

- provide Services;
- manage accounts;
- authenticate users;
- provide support;
- fulfil contractual obligations.

10.2 Legitimate Interests

We may process Personal Data where necessary for legitimate business interests, including:

- maintaining platform security;
- improving Services;
- preventing misuse;
- managing customer relationships;
- developing functionality.

10.3 Legal Obligations

We may process Personal Data where required to:

- comply with laws;
- respond to lawful requests;
- maintain required records;
- satisfy regulatory obligations.

10.4 Consent

Where required by law, we may rely on consent.

Individuals may withdraw consent where applicable.

Withdrawal does not affect lawful processing completed before withdrawal.

11. Special Category Personal Data

Certain information receives enhanced protection under privacy laws.

Examples may include:

- health information;
- biometric information;
- identity verification information;
- regulated professional information;
- other protected categories.

Resolut does not require Special Category Personal Data unless necessary for a Customer-specific use case.

Where such information is processed:

- appropriate safeguards should apply;
- the Customer remains responsible for lawful processing;
- processing will be limited to the intended purpose.

12. How We Use Personal Data

P3 Audit may use Personal Data to:

- provide and manage Services;
- authenticate users;
- support compliance workflows;
- enable authorised sharing;
- maintain security;
- investigate incidents;
- improve platform functionality;
- communicate important information;
- meet legal obligations.

13. Artificial Intelligence and Automated Processing

Resolut may include AI-enabled functionality to assist users with:

- information analysis;
- compliance workflows;
- risk identification;
- search;
- recommendations;
- workflow automation.

AI functionality is intended to support human decision-making.

P3 Audit does not intend AI functionality to replace appropriate professional judgement.

Customers remain responsible for reviewing and validating AI-generated outputs.

P3 Audit will not intentionally use Customer Confidential Information or identifiable Personal Data to train publicly available AI models without appropriate permission or lawful basis.

PART 3

Privacy by Design, Data Governance and International Compliance

14. Privacy by Design and by Default

P3 Audit has designed Resolut around the principle that privacy protection should be embedded into systems, processes and relationships from the outset.

Privacy should not be treated solely as a compliance requirement or an administrative activity after information has been collected.

Resolut has been developed to support organisations in adopting a more responsible approach to managing personal information by enabling:

- greater transparency;
- controlled information sharing;
- appropriate access management;
- reduced unnecessary duplication of personal information;
- improved accountability;
- evidence of trusted relationships; and
- continuous governance.

P3 Audit seeks to apply the principles of privacy by design and by default throughout the development, operation and improvement of Resolut.

15. Data Protection Principles

P3 Audit is committed to processing Personal Data in accordance with internationally recognised privacy principles, including those established under the UK GDPR and EU GDPR.

These principles include:

15.1 Lawfulness, Fairness and Transparency

Personal Data will be processed:

- lawfully;
- fairly;

- transparently; and
- in a manner that individuals can reasonably understand.

P3 Audit aims to provide clear information regarding how Personal Data is used and the rights available to individuals.

15.2 Purpose Limitation

Personal Data will only be processed for specific, legitimate and clearly identified purposes.

P3 Audit will not intentionally process Personal Data for purposes incompatible with those communicated to individuals or Customers unless permitted by applicable law.

15.3 Data Minimisation

P3 Audit supports the principle that organisations should collect and process only the Personal Data necessary for a defined purpose.

Resolut has been designed to reduce unnecessary duplication of personal information by supporting:

- controlled access;
 - verification;
 - trusted relationships; and
 - appropriate sharing mechanisms.
-

15.4 Accuracy

P3 Audit recognises the importance of maintaining accurate information.

Customers and users are responsible for ensuring that information submitted into Resolut is accurate, complete and appropriately maintained.

Where inaccurate information is identified, appropriate steps should be taken to correct or update the information.

15.5 Storage Limitation

Personal Data should not be retained longer than necessary for:

- the purpose for which it was collected;
- contractual requirements;

- legal obligations;
- security requirements; or
- legitimate business purposes.

Retention periods may vary depending upon:

- the nature of the information;
 - Customer requirements;
 - regulatory obligations;
 - applicable jurisdiction.
-

15.6 Integrity and Confidentiality

P3 Audit applies appropriate technical and organisational measures designed to protect Personal Data against:

- unauthorised access;
 - accidental loss;
 - misuse;
 - alteration;
 - disclosure; or
 - destruction.
-

15.7 Accountability

P3 Audit recognises that privacy compliance requires organisations to demonstrate responsibility, not merely state compliance.

Resolut supports accountability by enabling organisations to maintain visibility of:

- responsibilities;
- relationships;
- permissions;
- acknowledgements;
- verification activities;
- compliance status; and
- governance records.

16. Data Subject Rights and Individual Control

P3 Audit recognises that individuals have rights regarding their Personal Data under applicable privacy legislation.

These rights may include:

- access to Personal Data;
- correction of inaccurate information;
- deletion of information where applicable;
- restriction of processing;
- objection to certain processing activities;
- data portability;
- withdrawal of consent where processing relies on consent.

Details regarding exercising these rights are provided in Part 4 of this Privacy Policy.

17. Customer Data, Trust Data and Platform Data

Resolut operates across complex relationships involving individuals, organisations and connected supply-chain participants.

To support clarity of responsibility, information processed through Resolut may be categorised as follows:

17.1 Customer Data

Customer Data is information submitted, uploaded or managed by a Customer through Resolut.

Customer Data may include:

- employee information;
- contractor information;
- supplier information;
- customer information;
- compliance information;
- supporting records.

The Customer remains responsible for determining:

- why the information is processed;
 - the lawful basis for processing;
 - appropriate notices;
 - permissions;
 - retention requirements.
-

17.2 Trust Data

Trust Data is information generated through Resolut to support trusted relationships, verification and accountability.

Examples may include:

- verification records;
- acknowledgement records;
- approval history;
- relationship status;
- permission records;
- compliance status;
- audit trails;
- timestamps.

Trust Data exists to provide evidence of interactions and relationships within the Resolut ecosystem.

Where Trust Data contains Personal Data, applicable privacy obligations continue to apply.

17.3 Platform Data

Platform Data is information generated through the operation, security and improvement of Resolut.

Examples may include:

- technical logs;
- performance information;
- system monitoring data;
- security events;

- usage statistics;
- operational records.

Platform Data is used to:

- operate the Services;
 - maintain security;
 - troubleshoot issues;
 - improve performance;
 - develop functionality.
-

18. Data Sharing Through Resolut

Resolut enables authorised participants to share information within trusted relationships.

Depending on Customer configuration, information may be shared between:

- employers;
- employees;
- contingent workers;
- suppliers;
- customers;
- auditors;
- certification bodies;
- professional organisations;
- regulatory participants; and
- authorised third parties.

Resolut is designed to support controlled sharing rather than uncontrolled distribution of information.

Customers remain responsible for ensuring that:

- information sharing is lawful;
- appropriate notices are provided;
- individuals understand relevant processing activities;
- permissions are correctly configured;

- recipients are authorised;
 - information is accurate.
-

19. Controller and Processor Responsibilities

The role of P3 Audit and each Customer depends upon the specific circumstances of processing.

19.1 Data Controller

A Data Controller determines:

- why Personal Data is processed; and
- how processing activities are carried out.

A Customer may act as a Data Controller where it determines the purpose of processing information relating to:

- employees;
 - contractors;
 - suppliers;
 - customers;
 - other individuals.
-

19.2 Data Processor

A Data Processor processes Personal Data on behalf of a Data Controller according to documented instructions.

P3 Audit may act as a Data Processor where:

- a Customer determines the purpose of processing;
 - Resolut processes information on behalf of that Customer; and
 - applicable contractual arrangements apply.
-

19.3 Independent Controllers and Data Sharing

In certain circumstances, multiple organisations may act as independent Data Controllers.

Examples may include:

- supply-chain participants;
- professional service providers;
- certification bodies;
- regulated organisations.

Each organisation remains responsible for determining its own privacy obligations.

20. Supply Chain and Third-Party Relationships

Modern organisations increasingly rely on interconnected ecosystems involving:

- suppliers;
- subcontractors;
- workforce providers;
- technology providers;
- professional partners.

Resolut supports organisations seeking greater visibility and accountability across these relationships.

However, P3 Audit does not assume responsibility for the privacy practices of independent third parties.

Customers remain responsible for ensuring that:

- appropriate contractual arrangements exist;
 - third parties are authorised;
 - processing activities are lawful;
 - privacy obligations are understood.
-

21. International Privacy Framework

P3 Audit operates a global privacy framework designed to support compliance with applicable privacy and data protection laws.

Privacy requirements differ between jurisdictions.

P3 Audit recognises that applicable obligations may depend upon factors including:

- location of individuals;
- location of organisations;

- nature of services provided;
- type of information processed;
- regulatory requirements.

Applicable privacy frameworks may include:

- UK General Data Protection Regulation (UK GDPR);
- European Union General Data Protection Regulation (EU GDPR);
- California Consumer Privacy Act and California Privacy Rights Act (CCPA/CPRA);
- South Africa Protection of Personal Information Act (POPIA);
- other applicable national and regional privacy laws.

Where applicable local laws provide additional rights or obligations, those requirements will apply.

22. International Data Transfers

Where Personal Data is transferred internationally, P3 Audit will consider applicable legal requirements relating to international transfers.

Depending on circumstances, appropriate safeguards may include:

- adequacy decisions;
- approved contractual mechanisms;
- standard contractual clauses;
- international transfer agreements;
- contractual protections;
- technical and organisational safeguards.

P3 Audit aims to ensure that international processing arrangements provide appropriate protection for Personal Data.

23. Data Sovereignty and Residency

P3 Audit recognises that many jurisdictions have introduced requirements relating to data sovereignty and data residency.

These requirements may address:

- where information is stored;
- where information may be accessed;

- restrictions on international transfers;
- government access requirements;
- security obligations.

Customers with specific regulatory, contractual or geographic requirements should discuss their requirements with P3 Audit.

Data residency options may depend upon:

- technical feasibility;
- hosting arrangements;
- subscription model;
- regulatory requirements;
- Customer needs.

24. Third-Party Service Providers and Sub-Processors

P3 Audit may engage trusted third-party service providers to support delivery of Resolut.

These providers may include:

- cloud hosting providers;
- infrastructure providers;
- security providers;
- communication providers;
- analytics providers;
- payment providers;
- customer support providers.

P3 Audit seeks to ensure that third-party providers implement appropriate safeguards appropriate to the services provided.

Where required, contractual protections will be established.

25. Security and Data Protection Measures

P3 Audit maintains technical and organisational measures designed to protect information processed through Resolut.

Measures may include:

- authentication controls;
- access management;
- encryption;
- monitoring;
- vulnerability management;
- backup processes;
- incident response procedures;
- security reviews;
- personnel awareness.

Security measures are reviewed periodically and improved as risks, technology and regulatory expectations evolve.

PART 4

Individual Rights, Data Retention and Information Management

26. Our Commitment to Individual Rights

P3 Audit recognises that privacy legislation exists to protect the rights and freedoms of individuals.

Resolut has been designed to support transparency, accountability and responsible stewardship of Personal Data while enabling organisations to demonstrate compliance with their legal and contractual obligations.

Where P3 Audit acts as a Data Controller, individuals may exercise the rights available to them under applicable privacy legislation.

Where P3 Audit acts solely as a Data Processor on behalf of a Customer, requests relating to Customer Data will normally be referred to the relevant Customer, who remains responsible for determining how such requests should be handled.

P3 Audit will provide reasonable assistance to Customers in responding to lawful requests where required by applicable law or contractual agreement.

27. Right of Access

Subject to applicable law, individuals may request confirmation as to whether P3 Audit processes their Personal Data.

Where applicable, individuals may also request access to information including:

- the categories of Personal Data being processed;
- the purposes for which the information is processed;
- the categories of recipients to whom the information has been disclosed;
- the anticipated retention period, where known;
- the rights available to the individual;
- the source of the information, where it was not obtained directly from the individual; and
- information regarding any applicable automated decision-making.

Requests for access may be subject to identity verification and other lawful requirements.

28. Right to Rectification

Individuals may request that inaccurate or incomplete Personal Data be corrected.

Where P3 Audit acts as a Data Controller, reasonable steps will be taken to update inaccurate information.

Where the information forms part of Customer Data, the relevant Customer may be responsible for making the correction.

P3 Audit may assist Customers in implementing such corrections where appropriate.

29. Right to Erasure ("Right to be Forgotten")

Individuals may request the deletion of Personal Data where permitted under applicable law.

Requests may be considered where:

- the information is no longer required for the purpose for which it was collected;
- consent has been withdrawn and no other lawful basis applies;
- the individual successfully objects to processing;
- processing has been unlawful; or
- deletion is required to comply with a legal obligation.

This right is not absolute.

P3 Audit may retain Personal Data where continued processing is required for reasons including:

- compliance with legal obligations;
- the establishment, exercise or defence of legal claims;
- fraud prevention;
- security investigations;
- contractual obligations;
- public interest requirements; or
- other lawful grounds.

Where P3 Audit acts solely as a Data Processor, requests for deletion will normally be referred to the relevant Customer.

30. Right to Restrict Processing

Individuals may request that processing of their Personal Data be restricted in circumstances permitted by applicable law.

Where processing is restricted, P3 Audit may continue to retain the information but will only process it where permitted by law.

Restrictions may apply while:

- the accuracy of information is verified;
- objections are considered;
- legal claims are assessed; or
- lawful processing requirements are determined.

31. Right to Object

Individuals may object to certain forms of processing where permitted by applicable law.

This may include processing based upon legitimate interests or direct marketing activities.

Where an objection is received, P3 Audit will consider the request in accordance with applicable legal requirements.

Processing may continue where compelling legitimate grounds exist or where required by law.

32. Right to Data Portability

Where applicable, individuals may request a copy of Personal Data that they have provided in a structured, commonly used and machine-readable format.

Where technically feasible and legally permissible, individuals may also request that the information be transmitted to another organisation.

This right applies only in circumstances recognised by applicable law.

33. Withdrawal of Consent

Where processing relies upon consent, individuals may withdraw that consent at any time.

Withdrawal of consent does not affect:

- the lawfulness of processing undertaken before consent was withdrawn;
- processing based upon another lawful basis;
- information retained to comply with legal obligations.

Where consent is withdrawn, P3 Audit will take reasonable steps to implement the request where applicable.

34. Automated Decision-Making and Artificial Intelligence

Resolut may incorporate automated tools and AI-assisted functionality to support:

- information analysis;
- compliance workflows;
- risk identification;
- document processing;
- search and knowledge retrieval;
- workflow recommendations.

These capabilities are designed to support human decision-making rather than replace it.

P3 Audit does not intentionally use automated processing to make decisions that produce legal or similarly significant effects on individuals without appropriate safeguards where required by applicable law.

Where applicable legislation provides rights relating to automated decision-making, P3 Audit will seek to respect those rights.

Customers remain responsible for decisions made using information generated through Resolut and should ensure that appropriate human oversight is maintained.

35. Exercising Privacy Rights

Individuals wishing to exercise privacy rights may submit a request using the contact details provided within this Privacy Policy.

Requests should include sufficient information to enable P3 Audit to:

- identify the individual;
- understand the nature of the request;
- verify identity where appropriate; and

- respond efficiently.

P3 Audit may request additional information where reasonably necessary to confirm identity or clarify the request.

Identity verification measures are intended to protect Personal Data from unauthorised disclosure.

36. Response Times

P3 Audit aims to respond to privacy requests within the timeframes required by applicable law.

Where requests are particularly complex or involve multiple systems or Customers, additional time may be required.

Where permitted by law, individuals will be informed if additional time is required together with the reasons for the extension.

37. Customer Responsibilities

Where P3 Audit acts as a Data Processor, Customers remain responsible for responding to requests relating to Customer Data.

Customers should ensure that they have:

- appropriate privacy notices;
- lawful processing arrangements;
- internal procedures;
- responsible personnel;
- suitable governance processes

to enable individuals to exercise their privacy rights.

P3 Audit may provide reasonable assistance to Customers in accordance with contractual agreements and applicable law.

38. Data Retention

P3 Audit retains Personal Data only for as long as reasonably necessary to:

- provide the Services;
- fulfil contractual obligations;
- maintain security;

- comply with legal obligations;
- resolve disputes;
- establish, exercise or defend legal claims;
- maintain legitimate business records.

Retention periods may vary depending upon:

- the type of information;
- the nature of the Customer relationship;
- applicable legal requirements;
- contractual obligations;
- regulatory expectations.

Where information is no longer required, P3 Audit will seek to securely delete, anonymise or otherwise dispose of the information in accordance with applicable legal requirements and operational practices.

39. Account Closure and Data Deletion

Where a Customer account is closed or Services are terminated, P3 Audit will manage Customer Data in accordance with:

- contractual agreements;
- applicable retention requirements;
- legal obligations;
- operational requirements;
- Customer instructions where appropriate.

Certain information may continue to be retained where reasonably necessary for:

- financial record keeping;
- security investigations;
- fraud prevention;
- dispute resolution;
- legal compliance;
- protection of legitimate business interests.

Deletion may not be immediate where backup, disaster recovery or legal preservation processes apply.

40. Accuracy and Ongoing Responsibility

Maintaining accurate information is a shared responsibility.

Individuals are encouraged to notify their organisation or P3 Audit, as appropriate, where Personal Data changes or inaccuracies are identified.

Customers are responsible for maintaining the accuracy of Customer Data that they upload, manage or process through Resolut.

P3 Audit will take reasonable steps to support correction of information where appropriate and within the scope of its responsibilities.

PART 5

Security, Governance, Regulatory Engagement and General Provisions

41. Information Security

P3 Audit recognises that protecting Personal Data requires a combination of technical, organisational and operational safeguards.

Resolut has been developed with security as a core design principle and seeks to support the confidentiality, integrity, availability and resilience of information processed through the platform.

Security controls are reviewed periodically and enhanced in response to evolving technology, emerging threats and changes in regulatory expectations.

42. Technical and Organisational Measures

P3 Audit maintains appropriate technical and organisational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or unauthorised access.

Depending upon the nature of the Services provided, these measures may include:

- identity and access management;
- role-based permissions;
- authentication controls;
- encryption of data in transit and, where appropriate, at rest;
- network and infrastructure security;
- vulnerability assessment and remediation;
- security monitoring and logging;
- secure software development practices;
- backup and disaster recovery procedures;
- business continuity planning;
- personnel training and awareness; and
- periodic review of security controls.

The specific measures implemented may evolve over time as the platform develops and security practices mature.

43. Security Incident Management

P3 Audit maintains procedures for identifying, assessing, managing and responding to actual or suspected security incidents affecting Resolut.

Where a security incident is identified, P3 Audit will seek to:

- investigate the incident promptly;
- assess potential impact;
- contain and remediate the issue;
- preserve relevant evidence where appropriate;
- reduce the likelihood of recurrence; and
- communicate with affected Customers where appropriate.

44. Personal Data Breach Notification

Where P3 Audit becomes aware of a Personal Data Breach affecting information for which it acts as a Data Controller, it will assess the incident in accordance with applicable privacy legislation.

Where notification is legally required, P3 Audit will seek to notify:

- the appropriate supervisory authority;
- affected individuals; and
- relevant Customers,

within the applicable legal timeframes.

Where P3 Audit acts as a Data Processor, it will notify the relevant Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Data, enabling the Customer to fulfil its own legal obligations.

Not every security incident constitutes a reportable Personal Data Breach.

45. Business Continuity and Operational Resilience

P3 Audit recognises that protecting information also requires maintaining the availability and resilience of the Services.

Reasonable measures are maintained to support:

- continuity of critical operations;

- recovery from disruptive events;
- restoration of services where practical;
- protection of Customer information during operational incidents.

Business continuity arrangements are reviewed periodically and may evolve as the Services develop.

46. Confidentiality

Employees, contractors and authorised representatives of P3 Audit who may have access to Personal Data are expected to maintain appropriate standards of confidentiality.

Access to Personal Data is limited to individuals who require such access for legitimate business purposes and who are subject to appropriate confidentiality obligations.

47. Children's Privacy

Resolut is intended for use by organisations, professionals and authorised users in a business or professional capacity.

The Services are not intentionally directed to children or intended for use by individuals below the age at which they may lawfully enter into binding agreements under applicable law.

P3 Audit does not knowingly collect Personal Data directly from children through Resolut unless expressly authorised and supported by an appropriate lawful basis.

Where P3 Audit becomes aware that Personal Data has been collected contrary to applicable law, appropriate steps will be taken to address the matter.

48. Regulatory Cooperation

P3 Audit is committed to cooperating with supervisory authorities and other competent regulatory bodies where required by applicable law.

Where appropriate, P3 Audit will seek to respond openly and constructively to lawful regulatory enquiries relating to its privacy obligations.

Nothing in this Privacy Policy limits any legal rights or obligations that may apply under applicable legislation.

49. Complaints

Individuals who believe that P3 Audit has not handled their Personal Data appropriately are encouraged to contact P3 Audit in the first instance so that concerns may be investigated and, where appropriate, resolved.

P3 Audit aims to respond to complaints fairly, transparently and within reasonable timeframes.

Where an individual remains dissatisfied, they may have the right to lodge a complaint with the relevant supervisory authority or other competent regulatory body in accordance with applicable law.

Nothing in this Privacy Policy affects any statutory rights available to individuals.

50. Changes to this Privacy Policy

P3 Audit may update this Privacy Policy from time to time to reflect:

- changes in legislation;
- regulatory guidance;
- technological developments;
- changes to the Services;
- operational improvements; or
- changes to business practices.

Where material changes are made, P3 Audit will take reasonable steps to notify Customers or users where appropriate.

The most recent version of this Privacy Policy will be made available through Resolut or the P3 Audit website.

The version number and effective date will identify the current published version.

51. Contacting P3 Audit

Questions regarding this Privacy Policy or the handling of Personal Data may be directed to P3 Audit using the contact details published on our website.

P3 Audit Limited

Registered Office: 71-75 Shelton Street, London, WC2H 9JQ, United Kingdom

Company Registration Number: 10838544

General Enquiries:

info@p3audit.com

Privacy Enquiries:

privacy@p3audit.com

Website:

www.p3audit.com or www.resolut.pro

Where required by applicable law, requests relating to privacy rights should be submitted using the published privacy contact details.

52. Governing Law

This Privacy Policy shall be governed by and interpreted in accordance with the laws applicable to P3 Audit Limited, except where mandatory privacy legislation in another jurisdiction applies.

Nothing in this Privacy Policy limits any rights granted to individuals under mandatory applicable privacy or data protection legislation.

53. Relationship with Other Documents

This Privacy Policy should be read together with other applicable Resolut governance documents, including:

- Terms of Service;
- Cookie Policy;
- Data Processing Addendum (where applicable);
- Acceptable Use Policy;
- Security Statement;
- Applicable Customer agreements; and
- any jurisdiction-specific privacy notices published by P3 Audit.

Where a conflict exists between this Privacy Policy and a separately executed contractual agreement, the contractual agreement shall prevail to the extent of that conflict unless prohibited by applicable law.

54. Our Privacy Commitment

Privacy is fundamental to trust.

P3 Audit was established on the belief that organisations should be able to demonstrate responsible stewardship of personal information without creating unnecessary complexity, duplication or risk.

Resolut has been developed to support a model in which individuals, organisations and their partners can establish trusted relationships while respecting privacy, maintaining accountability and reducing unnecessary exposure of Personal Data.

We believe privacy is not simply a regulatory obligation. It is an essential element of trustworthy relationships between people, organisations and the wider communities they serve.

As privacy legislation and technology continue to evolve, P3 Audit remains committed to improving Resolut and our governance practices in support of responsible, transparent and ethical information management.

Document Control

Document Title: Resolut™ Privacy Policy

Legal Entity: P3 Audit Limited

Version: 1.0

Status: Approved 31 July 2026

Owner: P3 Audit Limited

Review Frequency: At least annually, or sooner where required by legal, regulatory or operational changes.

Approved By: *Chris Els CEO P3 Audit Limited*
