



Data Protection Policy

e: info@redactxpert.ai

w: <https://www.redactxpert.ai>

Powered by Simpson Associates



Contents

1. Introduction..... 3

1.1 Scope..... 3

2. Principles for Data Protection 3

2.1 General Data Access Restrictions..... 3

2.1.1 Considerations for Bypassing Data Access Controls..... 4

2.2 Encryption and Key Management..... 4

2.3 Data Residency..... 4

2.4 Data Isolation 4

2.4.1 Environment Separation..... 4

2.4.2 Network Isolation 4

2.4.3 Tenant Isolation 5

2.4.3.1 Team, Organisation, and Enterprise Tiers 5

2.4.3.2 Individual Tier 5

2.4.3.3 Central Database 6

2.4.3.4 Shared Services..... 6

2.5 AI Data Processing..... 6

3. Deletion and Retention 7

3.1 Secure Deletion..... 7

3.2 Retention..... 7

1. Introduction

This policy defines how Simpson Associates protects personal data and other sensitive information within the RedactXpert application throughout its lifecycle, aligning with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and applicable contractual and sector requirements.

1.1 Scope

This policy applies to:

- All employees, contractors, and third-party processors handling RedactXpert data.
- All systems, applications, services, devices, and storage locations used to process RedactXpert data.
- All data classifications

2. Principles for Data Protection

- **Lawfulness, fairness, and transparency.** Processing must have a lawful basis and be transparent to individuals through appropriate privacy notices.
- **Purpose limitation.** Collect data for specified, explicit, and legitimate purposes; do not repurpose incompatibly.
- **Data minimisation.** Limit collection to what is adequate, relevant, and necessary.
- **Accuracy.** Keep data accurate and up to date; rectify inaccuracies promptly.
- **Storage limitation.** Retain data only as long as necessary for stated purposes and legal obligations.
- **Integrity and confidentiality.** Protect data with appropriate technical and organisational measures (see sections 2.1–2.4).
- **Accountability.** Maintain records of processing (RoPA), DPIAs where required, supplier due diligence, and evidence of control effectiveness.
- **Privacy by design and default.** Embed privacy in system and process design, enabling least privilege access, data minimisation, and secure defaults.

2.1 General Data Access Restrictions

At the data level, all RedactXpert staff (including administrators and support team members) are explicitly prevented from accessing customer file contents or sensitive metadata.

Specifically:

- RedactXpert staff cannot view uploaded files stored in Azure Blob Storage
- RedactXpert staff cannot view file contents, document names, detected PII, or label names stored in SQL databases

These restrictions are enforced through:

- Azure Policy
- SQL Always Encrypted

However, to allow processing/support of customer requests, the Support Team will be able to access end user email addresses and view usage statistics. Relevant team members will be able to access audit logs from activity within the RedactXpert solution (e.g. when a user has uploaded a document) to be able to provide management information to customers, and for general security monitoring.

2.1.1 Considerations for Bypassing Data Access Controls

It is acknowledged that it is theoretically possible for a RedactXpert administrator to bypass the security and data access controls in place, e.g. by disabling/editing the policy that explicitly blocks access. However, this is mitigated by using privileged identity access management (PIM) within Entra ID to be able to make changes to Azure policy, as well as alerts that are generated for risky behaviour, such as when a user principal is granted access to read documents within a tenant storage account.

2.2 Encryption and Key Management

- Sensitive data columns in the database are encrypted with SQL Always Encrypted using a RedactXpert Managed Key, protected by Azure Key Vault
- Documents within the storage accounts are encrypted using a Microsoft-managed key, and with infrastructure encryption
- Encryption keys are not accessible to support or administrative users and are explicitly blocked via Azure Policy
- A minimum of TLS 1.2 is used for communication internally within the solution, and is the minimum requirement for requests to RedactXpert

As a result:

- No support or administrative role has access to plaintext customer file data
- Data remains encrypted at rest, in use, and during support activities

2.3 Data Residency

All data within the RedactXpert solution is stored and processed in the **UK only**. Primarily, this will be in the Azure UK South region. For geo-redundancy purposes UK West may be used as the backup location.

Alternative regions may be considered for Enterprise Tier customers on request.

2.4 Data Isolation

2.4.1 Environment Separation

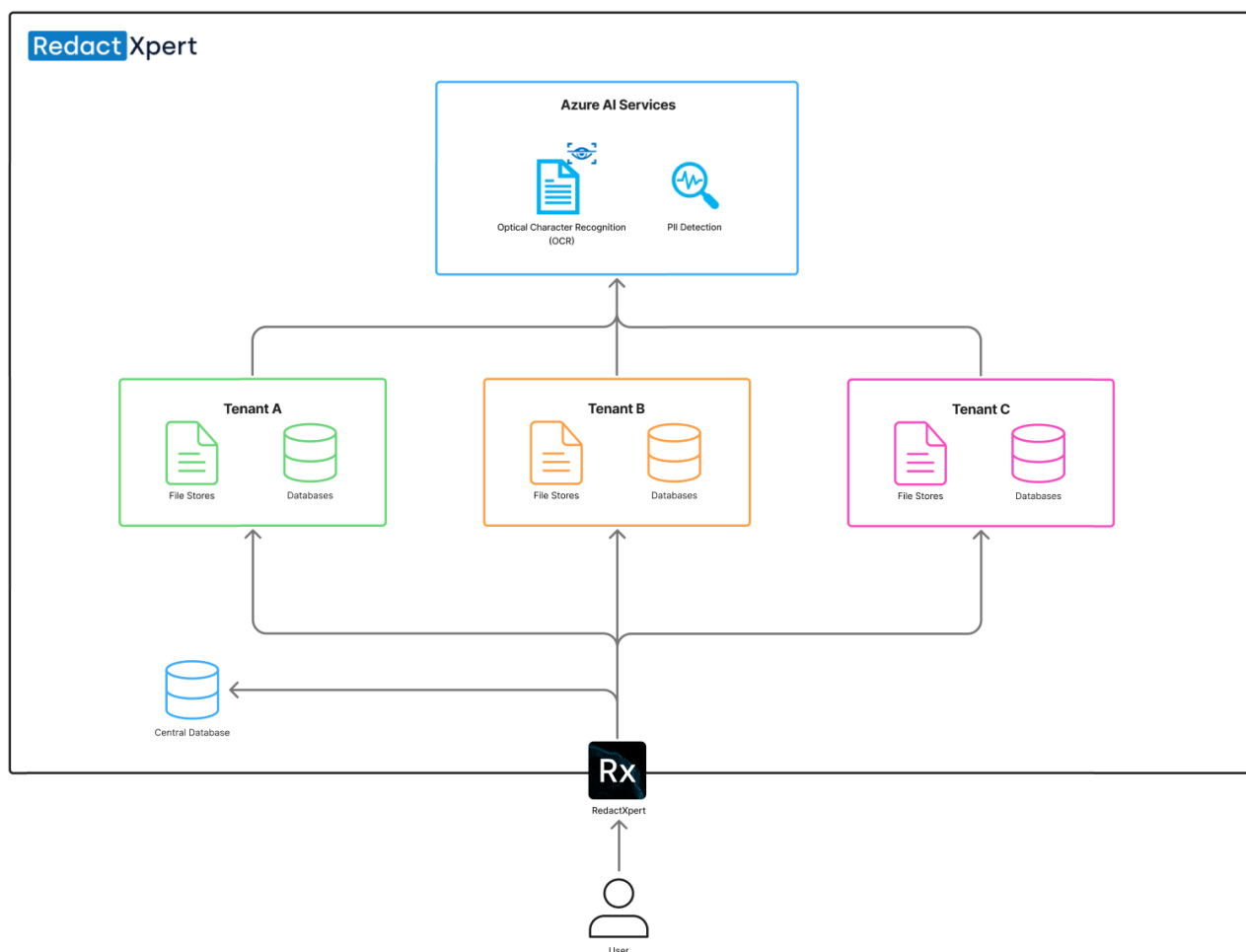
- Production must be isolated from non-production using separate:
 - Subscriptions
 - Resource groups and networking
 - Key Vault instances
- Production data must not be copied into non-production unless:
 - Approved by the Data Owner
 - Data is anonymised/pseudonymised and minimised
 - The purpose is legitimate (e.g., defect investigation) and time-bound

2.4.2 Network Isolation

- Private Networking connectivity **must** be used:
 - Private Endpoints must be used for PaaS services
 - VNets must be segregated, segmented and protected with Network Security Groups
 - All inbound access must be restricted

2.4.3 Tenant Isolation

RedactXpert is a multi-tenanted SaaS platform, with security at the forefront of the solution. The below diagram shows how tenant data stores are isolated from each other:



2.4.3.1 Team, Organisation, and Enterprise Tiers

An organisation that purchases the Team, Organisation, or Enterprise tier, is associated with a dedicated tenant. Each tenant on these tiers is provisioned with the following for increased security:

- Dedicated file and database storage that is separated from all other tenants' data
- A separate virtual network for network segregation from other tenants

Only users within a tenant can access data for that tenant (i.e. a user in Tenant A could not access data in Tenant B).

Additional security controls are applied within each tenant to restrict the data individual users can access. By default, users can only access their own redactions, however they can choose to explicitly share these with other users as needed by assigning users a relevant role.

2.4.3.2 Individual Tier

Users on the Individual tier can only access their own data (and no other users can access that data). This data is stored in a shared file store and database with other users on the Individual tier.

2.4.3.3 Central Database

Some information used by RedactXpert is stored centrally. This information is required to provide the multi-tenant nature of the platform, such as the tenants that are currently configured.

Documents that are uploaded by users (and any information detected in them) is never stored in this central database and only exists within the tenant databases.

2.4.3.4 Shared Services

Regardless of the tier, some security and compute services used by RedactXpert are shared across tenants, such as the web server, application gateways, Web-Application Firewalls, and AI services. Controls such as role-based access control (RBAC) are still in place to ensure that information cannot be accessed across tenants whilst it is being processed by these shared services.

2.5 AI Data Processing

Sensitive data uploaded by customers is sent to Azure AI services to be processed, therefore security is considered throughout this process. Information on how the AI Language model processes the data can be found here:

[Data, privacy, and security for Azure Language in Foundry Tools - Foundry Tools | Microsoft Learn](#)

In particular, the LoggingOptOut parameter determines whether temporary logs are stored on Microsoft's side. Although the default for the PII model is to disable these logs being stored, the RedactXpert solution explicitly sets this parameter to "true" as part of its processing to opt out of logs being stored by Microsoft.

3. Deletion and Retention

3.1 Secure Deletion

- Data must be securely deleted from primary stores, caches, and indexes.
- For cloud storage and databases, deletion must:
 - Remove the record and associated blobs/attachments
 - Ensure soft-delete and versioning settings are configured intentionally (to avoid accidental retention)
- Removal of Enterprise Customers, Tenants and Individual users should follow the corresponding deletion process to ensure data removal is complete and accurate.

3.2 Retention

- All uploaded documents and associated requests are permanently erased after 7 days by default, but each tenant can request their own interval to meet their security requirements.
- The following data may be retained beyond this interval:
 - Anonymised aggregated usage metrics, which contains no sensitive or user data, may be retained for longer.
 - Security Audits for up to 1 year for compliance purposes (even if the tenant, user or enterprise has been deleted).
 - Logging, diagnostics and telemetry are retained for 90 days.
- Documents, their contents and the extracted PII will **never** be retained as a copy of this information is never stored.