

Data Protection & UK GDPR Statement

LAST UPDATED: 8 JULY 2026

Revenant Systems' approach to data protection: privacy by design, data minimisation and compliance with UK GDPR, the Data Protection Act 2018 and PECR.

1. Our Commitment

At Revenant Systems, we believe privacy and security are fundamental parts of building good software.

As a small UK software company, we take a practical and proportionate approach to data protection.

We aim to design our products, services and internal processes with privacy, security and transparency in mind.

2. Our Approach to Data Protection

We follow the principles of UK data protection legislation, including:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations (PECR), where applicable

We aim to ensure that personal information is:

- Processed lawfully, fairly and transparently
- Collected only for legitimate purposes
- Limited to what is necessary
- Kept accurate where required
- Retained only for appropriate periods
- Protected against unauthorised access or misuse

3. Privacy by Design

Privacy is considered throughout our software development process.

Where practical, we aim to:

- Minimise the amount of personal information collected

- Avoid unnecessary user tracking
- Avoid collecting information that is not required
- Provide transparency about how information is used
- Build products with privacy considerations from the start

4. Data Minimisation

We believe software should not collect information simply because it can.

Where possible, we aim to:

- Reduce unnecessary data collection
- Avoid mandatory accounts where they are not required
- Limit reliance on unnecessary third-party services
- Keep user data within the user's control where appropriate

5. Security Practices

We use reasonable technical and organisational measures designed to protect information.

Our approach includes:

- Secure software development practices
- Appropriate access controls
- Secure authentication methods
- Keeping systems and dependencies updated
- Using reputable service providers
- Reviewing security practices as our services evolve

The specific controls used may vary depending on the service, technology and requirements involved.

6. Third-Party Services

Where we use third-party services to operate our business or deliver services, we consider their suitability, reliability and security practices.

Third-party providers may include:

- Cloud hosting providers
- Software platforms
- Communication services
- Development tools

Where required, appropriate agreements and safeguards are used.

7. Handling Security Incidents

We take potential security incidents seriously.

If we become aware of a suspected personal data breach, we will:

- Assess the nature and impact of the incident
- Take reasonable steps to contain and address the issue
- Notify relevant parties where required by law

8. Individual Rights

Individuals have rights under UK GDPR, including:

- Accessing their personal information
- Requesting corrections
- Requesting deletion where applicable
- Restricting processing
- Objecting to certain processing activities

Requests can be made by contacting Revenant Systems.

9. Continuous Improvement

As Revenant Systems grows, we will continue to review and improve our privacy and security practices.

We believe good software should respect users, protect information and operate transparently.

QUESTIONS

If you have any questions about the Data Protection & UK GDPR Statement, contact Revenant Systems Ltd at hello@revenantsystems.co.uk or visit <https://revenantsystems.co.uk>.