

Data protection policy

OWNER: AMRIT KHAREL, DIRECTOR, UK OPERATIONS

LAST REVIEWED: SEPTEMBER 2026

NEXT REVIEW: SEPTEMBER 2027

Purpose

This policy sets out how Kyros Software Ltd (Co. 16915277) complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Data controller: Kyros Software Ltd, 82a James Carter Road, Mildenhall, Bury St Edmunds, Suffolk IP28 7DE. Contact: info@kyrosweb.com

Scope

This policy applies to all personal data processed by the company, whether as a data controller or data processor on behalf of clients.

Data protection principles

We process personal data in accordance with the UK GDPR principles:

Lawfulness, fairness and transparency — we have a valid lawful basis for each processing activity and are transparent about how we use data.

Purpose limitation — data is collected for specified, explicit and legitimate purposes.

Data minimisation — we collect only the data we need.

Accuracy — we keep personal data accurate and up to date.

Storage limitation — data is retained only as long as necessary.

Integrity and confidentiality — data is protected by appropriate technical and organisational measures.

Accountability — we can demonstrate compliance with these principles.

Lawful basis

We identify and document the lawful basis for each processing activity before processing begins. Our most common bases are:

Contract — processing necessary to perform a contract with the data subject or client.

Legitimate interests — where we have a genuine business need and it does not override the individual's rights (e.g. business communications, fraud prevention).

Consent — where no other basis applies, and freely given, specific, informed consent is obtained.

Data subject rights

Individuals have the right to:

Be informed about how their data is used

Access their personal data

Rectification of inaccurate data

Erasure (where applicable)

Restrict processing

Data portability

Object to processing

Rights related to automated decision-making

Requests are acknowledged within 5 working days and fulfilled within one calendar month. Contact info@kyrosworld.com.

Data minimisation and retention

We collect only the minimum personal data required for each purpose.

Retention periods are defined for each category of data and documented in our data register.

Data is securely deleted or anonymised when no longer needed.

Data breach notification

In the event of a personal data breach:

The breach is reported internally to the Director immediately upon discovery.

The breach is assessed for risk to individuals.

Where the breach is likely to result in a risk to individuals' rights and freedoms, it is reported to the ICO within 72 hours of becoming aware.

Where the breach is likely to result in a high risk to individuals, affected individuals are notified without undue delay.

All breaches are logged, including those not reported to the ICO, with reasons documented.

Data protection impact assessments

A Data Protection Impact Assessment (DPIA) is carried out before any processing that is likely to result in a high risk to individuals. This includes:

- Large-scale processing of special category data
- Systematic monitoring of public areas
- New technologies where the impact on individuals is not well understood

International transfers

Personal data is not transferred outside the UK unless adequate safeguards are in place, such as:

- Transfer to a country with an adequacy decision
- Standard contractual clauses (international data transfer agreement)
- Binding corporate rules

Our default position is to host data in the UK or EEA.

Processing on behalf of clients

Where we process personal data on behalf of a client (as data processor), we:

- Act only on documented instructions from the controller
- Enter into a data processing agreement before processing begins
- Implement appropriate technical and organisational security measures
- Assist the controller with data subject requests, breach notification and DPIAs
- Delete or return all personal data at the end of the contract

Training

All staff complete data protection awareness training on joining and annually thereafter. Training covers UK GDPR principles, recognising personal data, breach reporting and individual rights.

Review

This policy is reviewed annually or following a data breach, regulatory change or significant change to processing activities. The next review is due September 2027.