

# Data Protection / UK GDPR Policy Summary

Public policy summary

## Classification

Public document

## Effective date

18 June 2026

## Owner

OLYVENRA LTD Management

## Review cycle

Annual or earlier if required

## Purpose

Explains public commitments for responsible handling of personal data, lawful processing and UK GDPR aligned controls.

This public summary supports first-stage assurance and communicates the standards expected before OLYVENRA enters or supports a business relationship.

## Policy position

This document sets OLYVENRA's public position for the named policy area. It is designed for external assurance and early-stage counterparty review, not as a substitute for a signed agreement or full internal procedure.

Explains public commitments for responsible handling of personal data, lawful processing and UK GDPR aligned controls.

## Scope

The policy applies to OLYVENRA personnel, representatives, suppliers, partners, introducers and other counterparties involved in enquiries, sourcing work, business development or document exchange.

## Core Commitments

- Maintain a clear and proportionate control environment for data protection / uk gdpr policy summary.
- Act lawfully, ethically and transparently in every commercial interaction.
- Apply counterparty review where identity, legitimacy, sanctions, product risk or reputation risk requires additional assurance.
- Keep accurate records of relevant decisions, approvals, documents and communications.
- Escalate concerns where a matter may create legal, compliance, security, human rights or reputational risk.
- Apply the policy before accepting a sensitive enquiry, introducing a counterparty or exchanging controlled documents.

## Data Protection / UK GDPR Policy Summary

Public document | Page 2

- Check identity, legitimacy, sanctions exposure, product sensitivity and reputational risk where the context requires it.

### Practical application

---

- Apply the policy before accepting a sensitive enquiry, introducing a counterparty or exchanging controlled documents.
- Check identity, legitimacy, sanctions exposure, product sensitivity and reputational risk where the context requires it.
- Keep communication factual, professional and traceable.
- Escalate unclear, high-risk or regulated matters to management before proceeding.

### Records and evidence

---

- Maintain proportionate records of requests, decisions, approvals, documents shared and key communications.
- Retain public document versions so clients and partners can confirm which summary was active at the time of review.
- Use controlled templates only for qualified matters and approved counterparties.

### Stakeholder Expectations

---

- Clients, suppliers and partners should provide accurate information, disclose relevant risks and avoid misleading statements.
- Any suspected breach or concern may be reported to [info@olyvenra.com](mailto:info@olyvenra.com) for review.

### Controlled material

---

- Commercial terms, fee schedules, commission wording and non-circumvention provisions are not published.
- Business continuity, IT disaster recovery and detailed internal procedures are shared only where required for assurance and approved by management.

### Review and Contact

---

This document is a public summary. It does not replace a contract, legal advice or any controlled internal procedure. OLYVENRA may update this document as its operating environment changes.