Synergia Consult Limited
Transformation Consultancy, Programme Delivery & Learning

GDPR Compliance Policy

Status: MANDATED — statutory / legal requirement
Legal basis: UK GDPR and the Data Protection Act 2018
Effective date: [Effective Date] | Next review: [Next Review Date — recommended annually] | Owner: [Policy Owner / Director]

Purpose

This policy sets out how Synergia Consult Limited complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 across our consultancy, project management and online training academy operations. It sits alongside our public-facing Privacy Policy and our internal Data Protection & Information Security Policy, and governs how we discharge our duties as a data controller and, in some engagements, a data processor on a client's behalf.

Data controller and responsible person

Synergia Consult Limited is the data controller for client, learner, supplier and marketing data collected in the course of our business. Day-to-day responsibility for data protection compliance sits with [the Director], who acts as our data protection lead. We are not required to appoint a statutory Data Protection Officer given the scale and nature of our processing, and will keep this under review as the business grows.

The seven UK GDPR principles

We process personal data in line with the UK GDPR principles: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality (security); and accountability. Our Privacy Policy explains what this means for clients and learners in practice; this policy explains how we evidence and govern it internally.

Lawful basis for processing

- We maintain a record of processing activities (ROPA) identifying what personal data we hold, why, and the lawful basis relied on for each use
- Contract delivery data (client and learner records) is processed under performance of a contract
- Marketing data is processed under consent, which can be withdrawn at any time
- Business development and website analytics rely on legitimate interests, balanced against individual rights
- Safeguarding, accreditation and tax records are processed under legal obligation

Data protection impact assessments (DPIA)

Before starting any new activity likely to result in high risk to individuals — for example, a new client engagement involving special category data, or a significant change to the online academy platform — [the Director] carries out a DPIA to identify and mitigate risk before processing begins.

Handling data subject requests

- Requests to access, correct, erase, restrict or port personal data are logged on receipt and acknowledged promptly
- Identity is verified before any data is released
- We respond within one calendar month, extendable by two further months for complex requests, with the individual informed of any extension and the reason for it
- Requests are directed in the first instance to the contact given in our Privacy Policy

Data protection by design and default

New systems, client engagements and course content are assessed for data protection impact at the design stage, not retrofitted afterwards. We collect only the data needed for the purpose in hand, and default to the most privacy-protective setting available on any platform we use.

Processors and sub-processors

Where a third party processes personal data on our behalf — our learning management system, video-conferencing, email, accounting or payment provider — we hold a written data processing agreement setting out the scope, purpose, security requirements and sub-processing terms, and we carry out due diligence before appointment.

International transfers

Where personal data is transferred outside the UK by us or a processor, we rely on adequacy regulations, the UK International Data Transfer Agreement, or Standard Contractual Clauses with a UK addendum, and assess the destination country's protections before transfer.

Personal data breaches

Any suspected breach is reported immediately to [the Director] and logged, including its cause, effect and remedial action. Where a breach is likely to result in a risk to individuals' rights and freedoms, we notify the Information Commissioner's Office within 72 hours of becoming aware. Where the risk is high, we also notify affected individuals directly and without undue delay.

Training and awareness

All staff and associates handling personal data receive data protection guidance proportionate to their role when they join, and refreshed periodically, covering lawful basis, retention, and how to recognise and report a suspected breach.

Governance and review

This policy, our record of processing activities, and our Privacy Policy are reviewed at least annually, and sooner following any material change to our processing activities, a regulatory update, or a data protection incident.

This policy is issued by Synergia Consult Limited (Company No. 17436025), 128 City Road, London, EC1V 2NX, United Kingdom. Contact: info@synergiaconsult.com | www.synergiaconsult.com.