

Data Protection Policy: Projects (General)

Last updated: October 2025

1) Purpose & scope

This policy describes how **Curious Roots Consulting (CRC)** manages personal data in **evaluation/research projects**, including interviews, audio recordings, transcripts, analysis and case-study publication. It applies to employees, associates and approved sub-processors.

2) Roles & responsibilities

Project roles are set by contract. CRC may act as **Controller, Joint Controller or Processor**. Where CRC is **Processor**, the client is Controller and CRC acts only on documented instructions. CRC appoints a **Data Lead** for each project. Associates/sub-processors sign confidentiality and data processing terms.

3) Lawful bases & special-category data

- Lawful bases are defined per project (typically **Art. 6(1)(e) public task** or **Art. 6(1)(f) legitimate interests**).
- If **special-category data** may arise (e.g., health/bereavement context), CRC relies on **Art. 9(2)(a) explicit consent** (layered consent form) or another applicable condition agreed with the client. We minimise collection and prefer **anonymisation** in published outputs.

4) Data minimisation & pseudonymisation

- Collect only data necessary to meet project aims.
- Brief participants to avoid full names/precise locations.
- Assign **unique IDs**; store the **re-identification key separately**, encrypted, accessible only to the Data Lead.
- Published outputs are anonymised by default; **named publication** requires explicit written consent and **quote approval**.

5) Capture & transfer

- **Interviews:** End-to-End Encrypted meetings; **local recording only** (no cloud). Uncompressed **.wav** saved to encrypted disk.
- **File transfer:** No raw files by email; use **encrypted portals/SFTP** or client-approved secure workspace.
- **AI tools:** If used for drafting, tools run **locally/offline**; no uploads to consumer AI platforms.

6) Storage & access

- **Location:** UK/EU business cloud with **MFA**, role-based access and versioning; device full-disk encryption.
- **Network hygiene:** WPA3 (or strong WPA2-AES) with unique passphrase; router firmware up-to-date; guest/segmented network for non-work devices.
- **Access:** least-privilege; access logs retained; screen lock at 5 minutes.

7) Sub-processors & international transfers

- Sub-processors (e.g., transcription) must be **UK/EU-based**, operate under a **Data Processing Agreement**, and **not** use data for model training.
- Processing/storage occurs in the **UK/EU only**, unless otherwise agreed with appropriate safeguards (e.g., IDTA/SCCs).

8) Consent, publication options & withdrawal cut-off

- **Layered consent** covers participation, anonymised use, publication options (named/anonymised/composite), quote approval, image consent, and a **withdrawal cut-off** (the latest date by which participants can withdraw and request deletion).
- **Deceased individuals:** default anonymised; naming only with written permission from an appropriate representative.
- **After the cut-off**, data may already be embedded in analysis/outputs; we will remove/pseudonymise identifiers going forward and stop using new material.

9) Retention & deletion

- **Raw audio:** deleted after transcript verification/sign-off unless the Controller instructs otherwise.
- **Transcripts/analysis:** retained **12 months** post-project.
- **Consent & re-ID key:** retained **24 months**.
- **Vendor copies:** deletion **≤30 days** after acceptance, with written confirmation.
- Retention may be varied by contract; secure deletion is logged.

10) Data subject rights

CRC supports Controllers to meet rights requests (access, rectification, erasure, restriction, objection, portability). Requests via **clare@curiousrootsconsulting.com** re acknowledged promptly and resolved within **one month** (or as agreed with the Controller).

11) Security controls (summary)

MFA; full-disk encryption; least-privilege access; AV/EDR with daily quick & weekly full scans; critical patching within **7 days**; TLS 1.2+; secure portals/SFTP; geo-redundant UK/EU backups with 30-day version history; removable media disabled or hardware-encrypted only.

12) Incident response

CRC maintains a **Data Breach Response Plan**. If CRC is Processor, the Controller is notified **within 24 hours** of becoming aware of a breach and supported with ICO/individual notifications. All incidents are logged and followed by a **post-incident review**.

13) Training & review

All project staff/associates receive onboarding on this policy and periodic refreshers. This policy is reviewed **annually** or after material changes to processing or law.

Contact (data matters): Clare Meakin, Lead Consultant, Curious Roots Consulting, clare@curiousrootsconsulting.com