DATA PROTECTION AND UK GDPR POLICY

Localscript — transcription and anonymisation services

Last updated: 20 August 2026
Review date: 20 August 2027

1. WHAT THIS POLICY IS

This is the framework document for how Localscript Ltd complies with the UK GDPR and the Data Protection Act 2018. It is the document to hand to a research ethics committee, a data protection officer or a procurement team who asks whether I have a data protection policy.

It is deliberately short, because most of the substance lives in the documents it points to:

Document	**What it governs**
Data Processing Agreement	The terms on which I process a client's recordings. Signed before any audio moves
Terms and Conditions	The commercial contract for the Services
Privacy Policy	What I do with data for which I am the controller — your contact and billing details
Information Security Policy	Technical and organisational measures
Retention and Deletion Policy	Retention periods and how erasure is carried out
Business Continuity Policy	What happens if I cannot operate
Complaints Policy	How to complain and what happens next

Where this policy and a signed Data Processing Agreement differ, **the Agreement prevails**. Where this policy and one of the other documents differ on a point of detail, the more specific document governs.

Owner: Montagu Franks, Director. There is no governance officer, no committee and no delegation, because there is one person.

Scope: every device, account and process used to deliver the Services, and every category of personal data I handle, wherever it is held.

2. THE TWO CAPACITIES

Almost every mistake in this area comes from blurring these, so they are set out first.

As a processor. For recordings, transcripts, anonymisation logs and re-identification keys, the client is the controller and I am the processor. I act only on the client's documented instructions and do not determine the purposes of processing. This is clause 3.6 of the Data Processing Agreement. Research participants' personal data is always in this category.

As a controller. For my own business records — client and enquirer contact details, correspondence, quotations, invoices and accounting data — I am the controller. That processing sits outside the Data Processing Agreement and is governed by the Privacy Policy.

The practical consequence: **I have no purposes of my own for participant data.** Recordings and transcripts are never used to train, fine-tune, evaluate or improve any machine learning model, nor for research, benchmarking, marketing or portfolio purposes. That is clause 3.2(o) of the Data Processing Agreement — a contractual prohibition, not a preference.

3. THE PRINCIPLES I WORK TO

The UK GDPR sets six principles at Article 5(1). Personal data must be:

1. processed lawfully, fairly and transparently;
2. collected for specified, explicit and legitimate purposes, and not processed further in a way incompatible with those purposes;
3. adequate, relevant and limited to what is necessary;
4. accurate and, where necessary, kept up to date;
5. kept in a form permitting identification no longer than is necessary;
6. processed securely, including against unauthorised or unlawful processing and accidental loss or destruction.

Article 5(2) adds a seventh obligation, accountability: I must be able to **demonstrate** compliance, not merely assert it. Section 8 below is how that demonstration is maintained.

(Some published policies still list eight principles and cite the Data Protection Act 1998, or restrict transfers by reference to the European Economic Area. Both are pre-Brexit framing and neither reflects the law that applies to a UK business today.)

4. LAWFUL BASIS

For participant data, the lawful basis is not mine to establish. The client, as controller, warrants at clause 4.2 of the Data Processing Agreement that it holds an Article 6 basis for the processing it instructs; where special category data is or may be present in a recording, an Article 9 condition — for academic research, commonly Article 9(2)(j) together with Schedule 1 Part 1 of the Data Protection Act 2018; and all necessary consents and ethics approvals, including having told participants that transcription may be carried out by an external provider.

I will not begin work where I have reason to believe that warranty is untrue, and I will tell a client without undue delay where an instruction appears to me to infringe data protection law, and may suspend performance of it. That is clause 3.2(q).

For my own controller-side processing, the bases are set out in Privacy Policy section 3: legitimate interests for enquiries and for direct approaches to research professionals; steps taken before entering a contract for bookings; performance of a contract for client engagement; and legal obligation for accounting and tax records.

Where I rely on legitimate interests for **cold outreach**, the balancing assessment is recorded, the source of the contact details is disclosed as Article 14 requires, and every message carries an unconditional right to stop. A suppression list of email addresses is maintained indefinitely for the sole purpose of not contacting people who have asked not to be contacted. This is Privacy Policy section 3.4.

5. ANONYMISATION AND PSEUDONYMISATION

The service is sold as anonymisation, because that is the term researchers and ethics committees use. The legally accurate term for what I deliver is **pseudonymisation**.

Identifying details are replaced consistently across a project, and a re-identification key linking pseudonyms to originals is produced and delivered to the client. Because that key exists, the transcript remains personal data under UK GDPR and the full protections of this policy and the Data Processing Agreement apply to it. It is not anonymous data outside the scope of the legislation, and I do not represent it as such.

Whether the client's own copy becomes anonymous data after they destroy the key is a question for the client as controller.

6. SECURITY, LOCATION AND THIRD PARTIES

Recordings and transcripts are processed on **one machine, at the registered premises in the United Kingdom**, and are not transmitted to any external service, application programming

interface or cloud provider at any stage. Speech recognition, speaker segmentation and identifying-detail detection all run on models installed and executed locally.

This is a contractual commitment at clause 3.2(g) and Annex C of every Data Processing Agreement I sign, not a configuration that could be quietly changed.

It follows that:

- **There are no sub-processors.** Clause 3.2(m). General authorisation is neither sought nor accepted.
- **There are no transfers outside the United Kingdom**, so there is nothing to disclose or safeguard under Chapter V of the UK GDPR. Annex C records this.
- **There are no third-party copies to chase** when deletion is due.

The transfer route by which recordings reach me is chosen by the client, because it is the only point in the chain where a third party could touch the data and that decision belongs to the accountable controller. Recordings are never sent as email attachments or through consumer file-sharing services.

Full technical and organisational measures are set out in Annex D of the Data Processing Agreement and in the Information Security Policy, which is provided to clients on request.

What I do not hold. I do not hold ISO 27001, Cyber Essentials or Cyber Essentials Plus certification, and these controls are not externally audited. Information Security Policy section 15 states this in full. Where a client's procurement process requires a certification I do not hold, I say so at the point of enquiry rather than after a contract is signed.

7. RETENTION AND ERASURE

Recordings, transcripts, anonymisation logs and re-identification keys are securely deleted **within 30 days of delivery, including from backups**, or earlier on written request at no charge. Erasure of encrypted media is by cryptographic erase, the method described in NIST SP 800-88 and in National Cyber Security Centre guidance, which is the reliable method for solid-state storage.

A **Certificate of Erasure** is provided free on written request. A short internal deletion record supports it, so the confirmation is verifiable rather than asserted.

Business records I hold as controller are kept to the schedule in Privacy Policy section 7 and Retention and Deletion Policy section 5 — mostly six years where a statutory or limitation period applies. None of those categories contains participant data.

Because deletion is bound to 30 days, correction of a transcript against the audio is only possible inside that window. What has been erased cannot be corrected or produced.

8. ACCOUNTABILITY RECORDS

I maintain:

- **Records of processing activities** under Article 30, in both capacities. The exemption for organisations under 250 staff does not apply, because the processing is regular rather than occasional and may include special category data. The processor-side record is made available to clients on request under clause 3.2(l).
- **A deletion record** for each engagement — what was deleted, when, and confirmation that backups were included.
- **An incident log**, covering security incidents whether or not they proved reportable.
- **Legitimate interests assessments** for controller-side processing relying on that basis.
- **Restore and rebuild test records**, per Information Security Policy section 9 and Business Continuity Policy section 9.
- **An account inventory** of every service holding business or client information.

These are produced to clients on request as part of their own assurance obligations under Article 28(3)(h). Inspection rights are at clause 3.2(d).

9. DATA SUBJECT RIGHTS

Individuals have rights of access, rectification, erasure, restriction, portability and objection, and rights concerning automated decision-making.

Where I am the processor, I do not respond to participant requests directly, and clause 3.2(h) forbids it unless the controller authorises me to. Verifying a participant's identity and understanding their relationship to the research are the controller's job, not mine. Any request or complaint I receive is forwarded to the client, with copies, **within 48 hours**, and I then assist them in responding, including by locating and retrieving the relevant records.

Where I am the controller, requests are handled directly, free of charge, and answered within one month — usually within a few days. Email monty@localscript.co.uk.

No automated decision-making. The output of the pipeline is a document, reviewed in full against the audio by me, and returned to the researcher who commissioned it. No decision producing legal or similarly significant effects for any individual is made by automated means, and automated output is never delivered unreviewed.

10. PERSONAL DATA BREACHES

A breach is any event where personal data may have been lost, disclosed, altered, corrupted or accessed without authorisation — including a lost device, a suspected account compromise, or a transcript sent to the wrong recipient.

Client data: notification within 24 hours of my becoming aware, to the address in that client's Data Processing Agreement, stating so far as known the nature of the breach, the categories and approximate number of data subjects and records affected, the likely consequences, and the measures taken. This is clause 3.2(e), and it is a firmer commitment than the statutory "without undue delay" standard.

Notification is not conditional on the incident being my fault or on my being certain of its scope. Where scope is still unclear at 24 hours, I notify with what is known and follow up. The client is the controller and decides whether to notify the Information Commissioner's Office and the data subjects; I provide whatever they need to make and act on that decision.

My own controller-side data: where a breach is likely to result in a risk to individuals, I report to the Information Commissioner's Office within 72 hours, and notify affected individuals where the risk is high.

Every incident is recorded, including those assessed as not reportable, together with the reasoning for that assessment. The response procedure is at Information Security Policy section 12.

11. ASSISTING CLIENTS

Under clause 3.2(j) I assist clients with their obligations under Articles 32 to 36. In practice that means:

- **Data protection impact assessments.** A written description of how processing is carried out is available for clients to incorporate into their own DPIA, rather than leaving a researcher to reconstruct it from the Agreement.
- **Ethics and institutional review.** This policy, the Data Processing Agreement, the Information Security Policy and the Retention and Deletion Policy are provided in whatever form a review process requires.
- **Prior consultation** with the Information Commissioner's Office, where a client requires it.
- **Audit and inspection**, on 14 days' notice, remotely where practicable, per clause 3.2(d).

12. DATA PROTECTION OFFICER

I have assessed whether Article 37 requires me to appoint a Data Protection Officer and concluded that it does not. Localscript is not a public authority; its core activities do not consist of regular and systematic monitoring on a large scale; and while special category data may be present in recordings, the processing is not large scale within the meaning of Information Commissioner's Office guidance, judged on the number of data subjects, the volume and range of data, the duration and the geographical extent.

This assessment is reviewed annually and revisited if volumes grow materially. A sole director cannot meaningfully appoint himself as an independent officer, so if the threshold is ever crossed, an external DPO will be appointed rather than the role notionally assigned to me.

13. CONTINUITY

Data protection obligations do not lapse during a disruption. No transfers outside the UK, no sub-processors, no access by anyone other than the named individual, and the 30-day deletion schedule all apply in full during an incident.

Where I become unable to perform the Services through illness, incapacity or death, the client is notified and chooses between return and secure destruction of their material, and **no other person is given access to it in order to complete the work** without the client's prior written authorisation. This is clause 3.4 of the Data Processing Agreement, and the standing written instructions that give effect to it are described in Business Continuity Policy section 6.

14. COMPETENCE

There are no staff to train, so keeping current is a named task rather than something that happens by itself. I follow Information Commissioner's Office guidance and newsletters and National Cyber Security Centre advisories, review this policy annually against published guidance, and obtain external advice where a question exceeds my competence rather than guessing at the answer.

15. COMPLAINTS

If I have got something wrong, tell me first — monty@localscript.co.uk — and I will respond within **2 working days**. Complaints are handled under the Localscript Complaints Policy.

You also have the right to complain to the Information Commissioner's Office at any time, whether or not you have raised it with me:

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF 0303 123 1113 · ico.org.uk/make-a-complaint

Where a complaint concerns a **research participant's** data rather than your own, I am the processor and not the controller. I will say so, and pass the complaint to the client who commissioned the transcription within 48 hours, as clause 3.2(h) requires.

16. REVIEW

Reviewed annually, and additionally whenever the law changes, the Information Commissioner's Office issues relevant guidance, the processing changes materially, an incident occurs, or a client identifies a gap.

Version	**Date**	**Amendments**
1.0	20 August 2026	First issue

Localscript Ltd is registered in England and Wales, company no. 17388152 · registered office 13 The Terrace, Barnes, London, SW13 0NP · registered with the Information Commissioner's Office, reference ZC217301 · monty@localscript.co.uk