DPA 2018 SCHEDULE 1 PART 4

Appropriate Policy Document — Voice Fingerprints

Issued by Datazero Ltd trading as NumberGroup. Forms part of the NumberGroup Agreement.

EFFECTIVE **1 November 2026**	VERSION **1.0**
ISSUER **Datazero Ltd (Co. No. 07390438)**	REGISTERED OFFICE **International House, 36-38 Cornhill, London EC3V 3NG**
CONTACT **help@numbergroup.com · 0800 310 1010**	ONLINE COPY **numbergroup.com/terms**

1. Purpose of this document

The Data Protection Act 2018 (Schedule 1, Part 4) requires a controller that relies on certain Schedule 1 conditions to process special-category data to have an Appropriate Policy Document. This document explains the condition we rely on for voice fingerprints, how we comply with the UK GDPR Article 5 principles, and our retention and deletion policy for this data. Our Data Protection Officer, who owns this document, is Jody Samuel, Director (help@numbergroup.com). It supplements our Privacy Policy .

2. Processing covered

Voice fingerprints. On numbers where a customer has enabled our AI call-intelligence services (transcribed or Call IQ), our systems automatically create a voice fingerprint — a numerical summary of voice characteristics — from the speakers on each call, and compare it with fingerprints from earlier calls. Voice characteristics used to identify a person are biometric data and therefore special-category data under UK GDPR Article 9(1). Datazero Ltd is the controller for this processing.

We use caller fingerprints to:

- recognise repeat callers who **withhold their number**, so that their calls can be grouped together in caller history; and
- help detect repeat nuisance, abusive or fraudulent calls from withheld numbers.

Scope limits:

- Not used for marketing, general profiling or any other purpose.
- Grouping is automatic, but no decision with legal or similarly significant effects is made from it. Any action against a suspected nuisance, abusive or fraudulent caller is reviewed by a person first.
- Processed only on servers and computers Datazero Ltd operates in a datacentre in the Isle of Man.
- Separate, more targeted voice matching against known fraud voices has been built but is **not active**. It will not be switched on until this document has been updated to cover it.

3. Condition relied on and why

Article 9(2)(g) UK GDPR (substantial public interest), with Data Protection Act 2018, Schedule 1, Part 2, paragraph 10 — preventing or detecting unlawful acts. Our Article 6 basis is legitimate interests (Article 6(1)(f)).

- **Necessity.** Callers who make nuisance, abusive or fraudulent calls often withhold or change their number, so the number alone cannot show that calls come from the same person. Recognising the voice is the only practical way to link those calls.
- **Without consent.** Asking a caller for consent to voice matching would let the people the processing is meant to detect avoid it, which would prejudice the purpose.
- **Substantial public interest.** Protecting businesses, their staff and telephone users from nuisance, abusive and fraudulent calls.

4. How we comply with the Article 5 principles

- **Lawfulness, fairness and transparency:** the processing is described in our Privacy Policy (sections 2, 4, 7 and 8), our Call Recording, Transcription and AI explainer, and this document. Our Caller Notice Templates give customers wording to tell callers and staff.
- **Purpose limitation:** fingerprints are used only for the purposes in section 2. Any new use needs a new assessment and an update to this document first.
- **Data minimisation:** we keep the numerical fingerprint, not a separate copy of the voice, and use it only for matching.
- **Accuracy:** a match is treated as a likely link, not proof of identity. A person reviews any match before action is taken against a caller.
- **Storage limitation:** see section 5.
- **Integrity and confidentiality:** processing on our own infrastructure, encryption in transit, access limited to staff who need it, and logging.
- **Accountability:** this document, our data protection impact assessment, our record of processing activities, and ICO registration ZA261621.

5. Retention and deletion

- A caller's fingerprint is deleted 90 days after their last call, and all fingerprints for a customer's numbers are deleted when the customer leaves or switches the service off.
- A fingerprint is deleted when the person objects, unless there are compelling legitimate grounds (for example an open fraud investigation), which we record and explain.
- Fingerprints linked to a confirmed fraud or abuse incident may be kept longer where needed for that incident, legal claims or a lawful disclosure; each case is recorded with its reason.
- Backup copies are overwritten on our normal backup cycle and are not used for matching.
- We keep this document for as long as the processing continues and for at least 6 months after it ends, and give it to the ICO on request.

6. Your rights

You can object to voice fingerprinting, or ask for access to or deletion of your fingerprint, by emailing help@numbergroup.com . Please tell us the approximate date and time of your call and the number you called. Our Your Data Requests page explains the process.

7. Review

We review this document at least once a year, and sooner if the processing changes — for example new software, a new purpose, or the fraud voice matching in section 2 being switched on — or if the law or ICO guidance changes.

Datazero Ltd, trading as NumberGroup. Registered in England and Wales, company number 07390438. Registered office: International House, 36-38 Cornhill, London EC3V 3NG. ICO registration ZA261621.

Datazero Ltd, trading as **NumberGroup**. Registered in England and Wales, company number 07390438. Registered office: International House, 36-38 Cornhill, London EC3V 3NG. Member of the Communications Ombudsman alternative dispute resolution scheme.

This document is published at numbergroup.com/terms and is free to access. For an accessible copy or a hard-copy printout, email help@numbergroup.com.

© 2026 Datazero Ltd. All rights reserved. Document version 1.0, effective 1 November 2026.