UK GDPR ARTICLE 28 TERMS

Data Processing Addendum

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. Parties and scope

1.1 In this Addendum, **Customer** means the person or organisation receiving NumberGroup services. **Datazero Ltd** means Datazero Ltd (company number 07390438), trading as NumberGroup.

1.2 This Addendum applies where Datazero Ltd processes personal data on the Customer's behalf as a processor, including customer-controlled call recordings, transcripts, AI summaries and other AI output, data extracted from calls, the Call IQ portal, MCP/API access, caller SMS delivery, caller recording-link features, webhooks and related support data.

1.3 It does not apply to processing where Datazero Ltd acts as controller, including account administration, billing, fraud prevention, network security, the voice fingerprints described in the Privacy Policy, and legal compliance. Those controller purposes are described in the Privacy Policy.

2. Roles

2.1 For customer call recordings, transcripts, AI output, data extracted from calls, caller-message recipients, CRM/webhook payloads and other data the Customer chooses to process through the services, the Customer is the controller and Datazero Ltd is the processor.

2.2 The Customer is responsible for its own lawful basis, caller notices, staff notices, and instructions to Datazero Ltd. Datazero Ltd processes the data only to provide, secure, operate, maintain and support the contracted services, and to derive de-identified learnings under clause 10, unless UK law requires otherwise.

3. Processing details

- **Subject matter:** hosted telecoms, call recording, transcription, AI call intelligence (transcribed, Call IQ and MCP/API access), playback, caller SMS, recording links and webhook delivery.
- **Duration:** for the term of the services, plus the retention periods in clause 9 or any period required by law.
- **Data subjects:** Customers, Customer staff, callers, call participants, support contacts and webhook recipients.
- **Personal data:** names, phone numbers, call metadata, audio recordings, transcripts, summaries, sentiment/outcome labels and other data extracted from calls, message delivery details, email addresses, IP/log data and support correspondence.
- **Special-category data:** call content may incidentally contain special-category data. Where special-category data appears in call content, the Customer remains responsible for its Article 9 condition.
- **Location:** recordings, transcripts and extracted data are processed and stored on servers and transcription computers Datazero Ltd operates in a datacentre in the Isle of Man. Encrypted audio files are stored with Cloudflare in Western Europe (EEA). Other sub-processors and their locations are listed on our Sub-processors page.

4. Customer instructions

4.1 The Customer instructs Datazero Ltd to process the personal data as necessary to provide the services, comply with the Agreement, follow any documented Customer configuration or support instruction, derive de-identified learnings under clause 10, and meet legal obligations applying to Datazero Ltd.

4.2 Datazero Ltd will tell the Customer if, in its opinion, an instruction infringes UK GDPR or other UK data-protection law, unless law prevents us from doing so.

4.3 If Datazero Ltd is required by law to process Customer-controlled personal data other than on the Customer's instructions, it will tell the Customer of that legal requirement before processing, unless the law prohibits this on important grounds of public interest.

5. Security and confidentiality

5.1 Datazero Ltd will implement appropriate technical and organisational measures, including those in Annex 1.

5.2 People authorised to process the data are bound by confidentiality obligations and receive access only where needed for the service, support, security or compliance.

6. Sub-processors and transfers

6.1 The Customer gives general authorisation for Datazero Ltd to use the sub-processors listed on our Sub-processors page, for the purposes stated there.

6.2 Datazero Ltd will give at least 30 days' notice of any new or replacement sub-processor (by email to the Customer's account address and by updating that page), allowing the Customer to object on reasonable data-protection grounds. If we cannot reasonably accommodate the objection, the Customer may end the affected service without penalty.

6.3 Datazero Ltd will impose on each sub-processor, by written contract, data-protection obligations that are substantially the same as those in this Addendum, and remains responsible to the Customer for each sub-processor's performance of those obligations.

6.4 Where personal data is processed outside the UK, Datazero Ltd will use an appropriate transfer safeguard: UK adequacy regulations (which cover the Isle of Man and the EEA), the UK International Data Transfer Agreement, approved standard contractual clauses with the UK Addendum, or the UK Extension to the EU-US Data Privacy Framework where the recipient is certified.

7. Assistance, breaches and audits

7.1 Datazero Ltd will provide reasonable assistance for data-subject requests, security obligations, DPIAs, consultations with the ICO, and Customer compliance obligations, taking account of the nature of the processing and information available to Datazero Ltd.

7.2 For data-subject requests, Datazero Ltd will, within 10 working days of a Customer request, locate the data linked to a phone number or email address, and provide an export or carry out an erasure as described on our Your Data Requests page. If a data subject contacts Datazero Ltd directly about

Customer-controlled data, we will pass the request to the Customer without undue delay and will not respond to it ourselves unless the Customer instructs us to or the law requires it.

7.3 Datazero Ltd will notify the Customer without undue delay, and in any event within 48 hours, after becoming aware of a personal-data breach affecting Customer-controlled data, and will provide information reasonably available to help the Customer meet its notification duties.

7.4 Datazero Ltd will make available to the Customer all information necessary to demonstrate compliance with Article 28 of UK GDPR and this Addendum, and will allow for and contribute to audits, including inspections, conducted by the Customer or by an auditor the Customer appoints. Audits must be on reasonable notice, proportionate, subject to confidentiality, and must not compromise the security or confidentiality of other customers or the network.

8. Return and deletion

8.1 At termination, Datazero Ltd will, at the Customer's choice, return Customer-controlled personal data in a common machine-readable format or delete it. Where data is returned, Datazero Ltd will then delete its remaining copies. Unless the Customer asks for an export within 30 days of termination, we will delete it within 60 days of termination. In each case this is subject only to retention required by UK law or a legal hold (clause 9.4).

8.2 Copies in backups are not deleted individually but are overwritten on our normal backup cycle of no more than 35 days. Deleted data is not restored from backup.

8.3 On request, Datazero Ltd will confirm in writing what was deleted and when.

9. Retention

9.1 **Audio recordings.** Audio is kept for a rolling 30 days from the date of the call and then deleted.

9.2 **Transcripts and extracted data.** Transcripts, summaries, call signals and other structured data extracted from calls are kept for the term of the services and deleted in line with clause 8 after it ends.

9.3 The Customer may instruct shorter retention, or deletion of specific calls, at any time. These are default periods. We may change them by giving at least 30 days' notice, and we will not extend a period without the Customer's agreement.

9.4 **Legal hold.** Where data is needed to establish, exercise or defend legal claims, to comply with a legal obligation, or for a regulatory investigation, we may suspend deletion of that specific data for as long as necessary, restrict its use to that purpose, and tell the Customer unless the law prevents us.

10. Service improvement and de-identified learnings

10.1 In providing the services, Datazero Ltd develops general knowledge about how calls work and how to analyse them well — for example rules, prompts, quality measures, scores, patterns and model improvements. The Customer instructs Datazero Ltd to derive such learnings from processing the Customer's data, provided they are kept only in a form that is de-identified and aggregated, so that they do not identify, and cannot reasonably be used to identify, any individual or the Customer, and do not contain call content.

10.2 Once in that form, those learnings are not personal data, are not Customer data, and are owned by Datazero Ltd. They are not affected by deletion of the Customer's data. Datazero Ltd will not attempt to re-identify any individual or Customer from them.

11. Order of precedence

11.1 If this Addendum conflicts with the General Conditions or any Schedule, this Addendum controls for processor obligations under UK GDPR Article 28. The General Conditions continue to control commercial, telecoms and liability terms.

Annex 1 — Technical and organisational measures

- **Encryption:** audio is encrypted by us before it is stored, and our storage provider never holds the key; data is encrypted in transit between our systems and to customers.
- **Our own infrastructure:** transcription, AI analysis and the call databases run on servers and computers Datazero Ltd operates; call content is analysed only by AI models running on that infrastructure.
- **Access control:** customer sign-in is restricted to authorised users; each customer account sees only its own data; staff access is least-privilege and logged, and staff access our systems only over a private, access-controlled network.
- **Card data:** card numbers and related card details are automatically removed from transcripts and AI output; the same removal is being introduced for stored audio, which until then is protected by encryption, access control and the retention periods in clause 9.
- **Monitoring and resilience:** error and availability monitoring; backups on a rolling cycle; documented incident response.
- **Minimisation:** default retention periods (clause 9); internal operational alerts carry call metadata and alert summaries only, not audio or transcripts, as described on the Sub-processors page.

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.