UK GDPR NOTICE

Privacy Policy

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. Who we are

This website is operated by **Datazero Ltd** trading as **NumberGroup** (“we”, “us”, “our”). Datazero Ltd is registered in England & Wales, company number **07390438**, registered office **International House, 36-38 Cornhill, London EC3V 3NG** . We are a UK communications provider regulated by Ofcom and we are the data controller for personal data collected through this website and our services.

Our Data Protection Officer is Jody Samuel. For any privacy question, data request or complaint, contact us at help@numbergroup.com .

2. What data we collect

- **Identity & contact data:** name, company name, email address, phone number, billing/postal address.
- **Payment data:** we do not store card numbers. Card payments are handled by Stripe; Direct Debit mandates (where used) are handled by our payment provider. We retain transaction references, amounts, dates and the last four digits of the card for accounting and refunds.
- **Transaction & service data:** numbers purchased, Membership status, certificates issued, port instructions, support tickets.
- **Call routing data:** when you use a number we issued, our upstream carrier records the calling number, dialled number, time, duration and a routing reference. This is required by law and by the network.
- **Call recordings & transcription (transcribed service, where you enable it):** if you switch on our transcribed call-intelligence service for one or more of your numbers, we record the audio of calls on those numbers and process it to produce a transcript, an AI summary and call signals (category, outcome, resolution and caller-mood indicators). Call content is transcribed and analysed only by AI models running on our own infrastructure: servers and transcription computers we operate in a datacentre in the Isle of Man. Audio recordings are encrypted by us before they are stored, and the encrypted files are kept with Cloudflare in Western Europe (see section 5). For these calls **you are the data controller and Datazero Ltd is your processor** — you choose which numbers are enabled and you are responsible for telling your callers that calls are recorded and analysed. Transcription applies only to calls made after you switch the feature on.
- **Recording links:** transcribed and Call IQ emails to the business include a secure, access-controlled link to play the recording of a call. Sending a text message or a recording link directly to a caller is not currently offered; if we introduce it, we will update this notice first.
- **Voice fingerprints (biometric data):** on numbers where transcribed or Call IQ is enabled, our systems create a voice fingerprint — a numerical summary of voice characteristics — from the speakers on each call. We use caller fingerprints to recognise repeat callers who **withhold their number**, so that their calls can be grouped together in caller history and repeat nuisance, abusive or fraudulent calls from withheld numbers can be spotted. Voice characteristics used to identify a person are biometric special-category data under UK GDPR Article 9. Datazero Ltd carries out this processing as controller. It is not used for marketing or general profiling, and the results are not used to make automated decisions about anyone. See section 4 and our Appropriate Policy Document .
- **Technical data:** IP address, browser, device and session identifiers used to operate and secure the site.
- **Correspondence:** emails, contact form submissions, and support tickets you send us.

3. How we use it

- To provide the service: provisioning numbers, routing calls, issuing certificates, processing payments, handling ports.
- To answer support enquiries and contact you about your account or order.
- To meet our legal and regulatory obligations (Ofcom, HMRC, anti-fraud, lawful intercept requests).
- To keep the site and network secure (rate limiting, fraud detection, logging).
- Where you enable the transcribed service: to record, transcribe and analyse calls on your enabled numbers and deliver the results to you (by email, in the Call IQ portal, through alerts you choose to receive, through MCP/API access you set up for your own systems or AI agents and, if you choose, to your CRM via an encrypted webhook), acting as your processor.
- To improve our services: we derive de-identified, aggregated learnings from processing (for example general rules and quality measures about how calls of a certain kind tend to go). These do not identify you or any business and contain no call content. Customers own their data; those de-identified learnings belong to us.

We do not run paid advertising and we do not send unsolicited marketing. If we ever do email you about something other than your account, it will be because you asked us to, and there will be a one-click unsubscribe.

4. Legal basis (UK GDPR Article 6)

- **Contract:** to deliver the number, certificate or Membership you bought.
- **Legal obligation:** tax records, Ofcom General Conditions, lawful intercept and emergency-services obligations.
- **Legitimate interest:** securing the site, fraud prevention, and contacting you about your service. We've balanced these against your rights and only rely on them where the impact on you is minimal.
- **Consent:** for any non-essential cookies, and for any optional communications you opt into.

Special-category data. Call recordings and transcripts created through transcribed and Call IQ may incidentally contain special-category data (UK GDPR Article 9); for that content the customer is the controller and is responsible for its own lawful basis and for informing its callers.

Voice fingerprints. Datazero Ltd creates and matches voice fingerprints as controller (see section 2). Our Article 6 basis is legitimate interests (Article 6(1)(f)): recognising repeat callers who withhold their number and protecting businesses and the network from nuisance, abusive and fraudulent calls. Because this is biometric data, we also rely on the "substantial public interest" condition in Article 9(2)(g), with Schedule 1, Part 2, paragraph 10 of the Data Protection Act 2018 (preventing or detecting unlawful acts). Our Appropriate Policy Document explains how we comply. Grouping is automatic, but no decision with legal or similarly significant effects is made from it, and any action on a suspected fraudulent or abusive caller is reviewed by a person first. You have the right to object to this processing (see section 8). Ask us about it at help@numbergroup.com .

5. Who we share data with

We use a small number of trusted suppliers to run the service. We don't sell your data, and we don't share it for advertising. Call recording, transcription and AI call intelligence (transcribed and Call IQ) run on our own infrastructure: call content is analysed only by AI models running on our own servers and computers, not by the AI suppliers listed below. The table below lists our main processors (suppliers acting on our instructions) and the independent recipients we share limited data with by law or to deliver the service. Our full, current sub-processor list gives the purpose, location and transfer safeguard for each one:

Supplier	Purpose	Location
Stripe Payments UK Ltd	Card payments & checkout	UK / EEA / US (SCCs)
Freshworks (Freshdesk)	Support tickets & enquiries	EU / US (SCCs)
Vercel Inc.	Website hosting & delivery	UK / EU / US (SCCs)
Neon Inc.	Website, account & billing database (not call recordings or transcripts)	EU / US (SCCs)
Cloudflare, Inc.	Audio storage: encrypted storage of call audio; sign-in to the Call IQ portal and MCP service; secure network edge	Audio storage: Western Europe (EEA); sign-in/edge: global (UK IDTA / SCCs; UK Extension to EU-US DPF)
Postmark (ActiveCampaign, LLC)	Delivery of transcribed and Call IQ emails to customers	US (UK Extension to EU-US DPF / SCCs)
Slack Technologies	Internal operational alerts to our team: call metadata and alert summaries only (no audio or transcripts)	US (UK Extension to EU-US DPF / SCCs)
Functional Software, Inc. (Sentry)	Error monitoring	EU — Germany (UK adequacy)
Hetzner Online GmbH	Encrypted off-site backup copy (for disaster recovery)	EU — Germany (UK adequacy)
BT Wholesale (BT plc)	Number porting & call delivery	UK
Acrobits s.r.o.	Softphone app (Members only)	EU
Anthropic, PBC	AI language processing for support drafting & internal workflows (not call recordings, transcripts or other call content)	US / EU (UK IDTA / SCCs; zero-retention where configured)
OpenRouter, Inc. (and its underlying model providers)	AI model routing for some opted-in internal workflows (not call recordings or transcripts)	US (UK IDTA / SCCs)
Ofcom & lawful authorities	Regulatory disclosures, emergency services	UK

Where your data is. Our call-processing servers and databases are in a datacentre in the Isle of Man. The Isle of Man is not part of the UK, but personal data can flow there lawfully from the UK and the EU: it is covered by UK adequacy regulations (it is one of the jurisdictions recognised as adequate under section 17A and Schedule 21, paragraph 5 of the Data Protection Act 2018) and by an EU adequacy decision (Commission Decision 2004/411/EC, confirmed in the European Commission's January 2024 review). Data protection there is overseen by the Isle of Man Information Commissioner. An encrypted backup copy of this data is also held off-site with Hetzner Online GmbH in Germany (EU), for disaster recovery; Germany is covered by UK adequacy regulations.

Where a supplier processes data elsewhere outside the UK, we rely on UK adequacy regulations, the UK International Data Transfer Agreement or Addendum, EU Standard Contractual Clauses with the UK Addendum, or the UK Extension to the EU-US Data Privacy Framework, plus additional safeguards where appropriate.

6. Cookies

We use essential cookies that are needed for the site and our customer services to work (session, security, checkout, and sign-in to the Call IQ portal and MCP service). See our Cookies Policy . We don't use advertising cookies, third-party trackers, or cross-site profiling. If we ever add analytics, we'll ask first and you'll be able to decline without losing any functionality.

7. How long we keep it

- **Account & transaction records:** 6 years after account closure (UK tax and accounting law).
- **Number ownership & certificate records:** for the lifetime of the number plus 6 years — we may need to prove chain of ownership for a number long after a sale.
- **Call routing logs:** retained by our upstream carrier in line with their regulatory obligations (typically 12 months).
- **Call audio recordings (transcribed and Call IQ):** kept for a rolling 30 days from the date of the call, then deleted.
- **Voice fingerprints:** 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, or sooner if you successfully object.
- **Transcripts, summaries and data extracted from calls:** kept for the term of the customer's contract, then deleted within 60 days after it ends unless the customer asks for an export first.
- **Backups:** overwritten on a rolling cycle of no more than 35 days. An encrypted backup copy is also held off-site in Germany, for disaster recovery, and is kept on the same rolling cycle. Data deleted from our live systems is not restored from backup.
- **Legal hold:** we may keep specific data longer only where it is needed to establish or defend a legal claim, to comply with a legal obligation, or for a regulatory investigation, and only for that purpose.
- **De-identified learnings:** these are not personal data and are kept as part of our services.
- **Support tickets:** up to 3 years from last contact.
- **Marketing consent:** until you withdraw it.

8. Your rights

Under UK GDPR you have the right to:

- **Access** a copy of the data we hold about you.
- **Rectify** anything that's wrong.
- **Erase** data we no longer have a lawful reason to keep.
- **Restrict** or **object to** certain processing.
- **Receive** your data in a portable format.
- **Withdraw consent** at any time (for anything we process on consent).
- **Object to voice fingerprinting.** If you tell us you object, we will stop matching your voice and delete your fingerprint, unless we have compelling legitimate grounds (for example an open fraud investigation), which we will explain. To help us find it, tell us the approximate date and time of your call and the number you called.

Email help@numbergroup.com (subject "Data request") or call 0800 310 1010, and we'll respond within one calendar month. If you called a business that uses our services, that business controls the recording of your call: ask them first, and we will help them. Our Your Data Requests page explains how to ask for a copy of your data ("send me my data") or for it to be deleted ("delete my data"), what deletion covers, and how we confirm it. We may need to verify your identity before releasing personal data. Subject access requests are free; we may charge a reasonable fee only if a request is manifestly unfounded or excessive.

9. Security

We use encryption in transit (TLS) for all web traffic, encryption of call audio before it is stored, encrypted database storage, access controls, audit logging, and least privilege for staff access. No system is ever completely secure, but we take this seriously and review it regularly.

If we ever suffer a personal data breach that's likely to risk your rights and freedoms, we'll notify the ICO within 72 hours where required, and we'll tell affected customers directly without undue delay.

10. Children

Our service is sold to businesses and adults. We don't knowingly collect data from anyone under 18. If you believe a child has provided us with personal data, contact us and we'll delete it.

11. Changes

We'll post any changes here with an updated revision date. For material changes affecting existing customers, we'll email you in advance.

12. Complaints

Talk to us first — help@numbergroup.com — and we'll try to put things right. If you're not satisfied, you can complain to the Information Commissioner's Office at ico.org.uk or on 0303 123 1113.

13. More about your information

- **Where we get it.** Mostly from you. We also receive: call details from our upstream carrier when calls use our numbers; call recordings and the voices of callers and staff on numbers where a business has enabled transcribed or Call IQ; company names and addresses from public records (Companies House) when you use our porting form; credit information from a credit reference agency when we carry out a credit check; and reports of fraud or abuse from other customers and networks.
- **What you must give us.** To buy a number, take out Membership or port a number we need your name, contact details and billing details, and some of it (for example invoice records) is required by tax law. If you don't provide it, we can't provide the service. Anything else is optional.
- **Copies of transfer safeguards.** You can ask for a copy of the safeguards we rely on for transfers outside the UK (see section 5) by emailing help@numbergroup.com. We may remove commercially confidential parts.
- **Data Protection Officer.** Our Data Protection Officer is Jody Samuel, Director. You can contact our DPO at help@numbergroup.com (subject "Data protection").

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.