

PRIVACY POLICY

Remote Physical Phones and Customer-Owned SIM Cards

Version 1.2

Last updated: 20 October 2026

1. CONTROLLER AND SCOPE

- 1.1 Controller and contact.** HiveReach is operated by Yevgeniy Kovalev, a sole trader registered in Poland in the Central Register and Information on Economic Activity, trading as HiveReach. NIP: 5272991183. REGON: 521331015. Correspondence address: ul. Okólnik 11A, lok. 77, 00-368 Warszawa, Poland. For privacy enquiries and requests, contact support@hivereach.app. Customer-service telephone: +48 507 275 570. HiveReach, we and us refer to this proprietor.
- 1.2 Scope.** This Policy explains how we process personal data when you visit hivereach.app, create an account, purchase or share access to a physical phone, order or store a SIM, contact support, or appear in information processed through the service. It covers our website and supported access applications. It explains the data we use, its purposes, recipients, locations and retention, and how you can exercise your rights.
- 1.3 Terms and privacy rights.** The [Terms of Service](#) and [Acceptable Use Policy](#) govern the service. Acknowledging this Policy or accepting those documents does not waive privacy rights, constitute consent to every processing activity, or provide consent for another person whose information appears on a phone.
- 1.4 Age and authorised users.** Account Holders and Authorised Users must be at least 18. Organisations use the service through authorised adult representatives. Information about children can nevertheless appear in customer content or correspondence; it remains subject to applicable data-protection requirements. Contact us if you believe a child has created an account or unnecessary information about a child has been submitted.

2. OUR ROLE AND CUSTOMER CONTENT

- 2.1 Processing as controller.** We are the controller where we decide the purposes and essential means of processing, including account administration, billing administration, our verification policy, support, connection-history collection and our own security monitoring and abuse investigations. Our responsibilities for those activities apply independently of any customer's responsibilities.
- 2.2 Processing on customer instructions.** A business customer may be the controller of employee, client or correspondent information it uses through a rented phone, or may act as a processor for its own client. Where HiveReach processes personal data on that customer's documented instructions and an Article 28 data processing agreement is required, that agreement must be in effect before the processing begins. Contact support@hivereach.app to arrange it. This Policy does not replace that agreement or make our own security monitoring processing solely on customer instructions.
- 2.3 Other services.** Mobile carriers, installed applications, websites, social networks and sign-in or payment providers process information under their own roles and privacy notices. Your carrier contract and carrier account belong to your separate relationship with the selected operator. Using those services through a HiveReach phone does not make HiveReach their operator.
- 2.4 Other people's information.** Customer content, support attachments, invitations and misuse reports can concern people who have no HiveReach account. Their rights continue to apply. Business customers must give the notices and have the authority required for their own processing. We assess our own information duties under Article 14 GDPR and any applicable exception; a customer's acceptance does not discharge those duties automatically. Requests concerning processing we perform solely on another controller's instructions are referred to that controller, with assistance as required.

3. INFORMATION WE PROCESS AND ITS SOURCES

- 3.1 Account and access information.** We process your email address, any supplied name or display name, contact and verification information, password hash where password login is used, sign-in-provider identifiers, account settings, invitations, access permissions and records of acceptance of applicable terms. An Account Holder supplies an invitee's email address and proposed access permissions. Google or Apple supplies the identifiers and permitted profile information needed for the sign-in method you choose.
- 3.2 Orders and transactions.** We process the selected country and carrier, device and SIM assignments, subscription dates, order and purchase references, billing details, amounts, payment and refund status, Stripe customer and transaction references, and required tax records. Payment providers receive payment credentials through their payment flow. HiveReach receives the transaction and billing information needed to administer your purchase.
- 3.3 SIM records.** Records can include the SIM serial number or ICCID, assigned telephone number where available, PIN and PUK codes, activation information, pictures of SIM packaging, purchase receipts, storage and handling records, and a delivery address where you request shipment. We obtain these from you, the physical SIM and its packaging, local purchasing and handling, and relevant retailer or carrier communications.
- 3.4 Technical and connection information.** Use of the service generates device, rack and account identifiers, authentication and controller-session references, connection times and events, observed IP addresses, source ports where reliable, limited browser or application information, network observations, faults and administrative records. Detailed connection history is described in section 7. Screen images and their analysis are a separate category described in section 8.
- 3.5 Support and reports.** We process messages, contact details, delivery information, attachments and reports you or another person send to us. Please omit unrelated personal information and avoid sending passwords, identity documents or sensitive material unless we specifically explain a necessary and lawful reason. A public-demo visitor's device and browser can also generate the limited technical information needed to provide and protect that demonstration.
- 3.6 Required and optional information.** Account contact details, applicable verification, payment information and the identifiers needed to allocate and control a phone are necessary for the relevant service. Without them, we may be unable to register an account, accept an order or grant access. Optional profile information, optional support attachments and consent-based analytics are not required to rent a phone. Any specific legal obligation to supply information is identified in the relevant context.

4. PURPOSES AND LEGAL BASES

- 4.1 Individual contracts.** We use Article 6(1)(b) GDPR for processing objectively necessary to take steps you request before a contract or to perform our contract with you. This includes creating and administering your account, allocating a phone, organising an agreed SIM purchase or return, providing remote access, handling payments and refunds, and answering contractual support requests.
- 4.2 Organisational accounts and invitations.** Where you represent an organisation or use access arranged by another person, Article 6(1)(f) GDPR supports necessary administration of that relationship. Our interests are providing the service requested by the Account Holder, managing authorised access and communicating with the appropriate representatives. A contract with an organisation is not automatically a contractual legal basis for every employee's or correspondent's data.
- 4.3 Security and service integrity.** We rely on Article 6(1)(f) GDPR for necessary and proportionate measures to prevent fraud, account compromise and misuse, protect people and equipment, investigate incidents and establish or defend legal claims. These interests concern verification records, relevant technical records, connection history and the monitoring described below. We assess the necessity and proportionality of these measures, taking account of people's rights, reasonable expectations and less intrusive alternatives. Verification records help us address identity fraud and impersonation, investigate relevant misuse and resolve verification-related disputes or legal claims.

- 4.4 Legal duties and rights requests.** Article 6(1)(c) GDPR applies to processing required by an applicable legal obligation, including specified tax and accounting records, handling data-protection requests, and compliance with binding legal process.
- 4.5 Enquiries and disputes.** Article 6(1)(f) GDPR supports answering noncontractual enquiries, investigating reports, resolving complaints and protecting legal rights. Where a request concerns your contract or a legal duty, the corresponding basis above applies. We limit any retained evidence to the issue and the period for which it remains necessary.
- 4.6 Consent and analytics.** We rely on Article 6(1)(a) GDPR for optional website analytics and any other processing for which we request your consent. Google Analytics is activated only after you consent, as described in section 12. You may withdraw consent at any time without affecting the lawfulness of processing carried out before withdrawal.
- 4.7 Sensitive information and new purposes.** Where processing involves special categories of personal data or criminal-offence information, we apply the additional requirements of Articles 9 and 10 GDPR. Before materially changing a purpose, we assess compatibility and any further legal basis, notice or consent required.

5. IDENTITY AND TELEPHONE VERIFICATION

- 5.1 When Stripe Identity applies.** Stripe Identity is required for the purchasing Account Holder where the selected carrier does not require customer identity verification. Where the carrier requires identification, you complete that procedure directly with the carrier and HiveReach does not require a duplicate Stripe Identity check or routine documentary proof of the carrier check. We do not independently confirm your subscriber identity or successful SIM activation under that arrangement. Access and billing follow the Terms.
- 5.2 Information available to HiveReach.** Our application uses the verification status and the technical references needed to associate the verification with your HiveReach account and relevant order, including the Stripe verification-session reference and verification date. Identity documents and selfie images are submitted directly to and held by Stripe. HiveReach personnel do not view or download those images, and we do not store copies in our application databases.
- 5.3 Stripe's role and notices.** Stripe processes verification information on our behalf and acts as an independent controller for its own purposes, including fraud prevention, security and legal compliance. Verification can include document checks and facial matching. See [Stripe's Privacy Policy](#) and the [Stripe Identity terms](#). Information and any required consent are presented in the verification flow. Accepting this Policy does not constitute biometric consent.
- 5.4 Available carrier alternative.** Where the catalogue offers a carrier that performs its own required identification, choosing that carrier avoids a duplicate HiveReach Stripe Identity check. The carrier determines its identification procedure, which may itself involve an identity provider or biometric checks. If the requested location has no such carrier option and the required Stripe verification is not completed, we cannot supply that selected service. Contact us about verification difficulties or to challenge a verification result; mandatory rights remain applicable.
- 5.5 Verification evidence and retention.** We arrange for Stripe to retain verification evidence on our behalf for up to three years following the relevant verification. We retain only the minimum account or order reference, Stripe verification reference, verification date and result needed to link the verification to the relevant customer for the same period. Retention serves the fraud, impersonation, misuse and related dispute or legal-claims purposes in section 4.3. We arrange deletion by the end of that period and earlier when the information is no longer necessary or applicable law requires earlier deletion. A specific lawful investigation, legal claim or binding preservation obligation may justify retaining only relevant evidence longer, with a documented purpose and review date. These periods do not extend the separate screenshot or detailed connection-history periods. You may request access, deletion or a review of retention at support@hivereach.app.
- 5.6 Biometric identifiers and Stripe's separate processing.** Stripe states that biometric identifiers created to conduct verification are removed from its systems within one year. This is separate from retention of

the original identity-document and selfie images and other verification information. Stripe may retain information for its own purposes under its privacy notice for a different period from HiveReach's instructions. See [Stripe's identity-information guidance](#). Requests concerning Stripe's independent processing may also be sent to privacy@stripe.com.

- 5.7 **Telephone checks and invited users.** Telnyx processes the telephone number and verification delivery information needed for a separately applicable phone check. Confirming an email address or telephone number establishes control of that contact method, not necessarily a person's legal identity. The purchaser-verification requirement does not automatically require government-ID checks for every invited user. Proportionate re-verification may be requested in the circumstances described in the Terms.

6. SIM PURCHASES AND ACTIVATION MATERIAL

- 6.1 **Purchase and activation.** A local Host Manager obtains the selected prepaid SIM from an available retailer on HiveReach's instructions for your order. We keep the purchase and handling records needed to perform that service. You register and activate the SIM, complete carrier identity checks and pay the mobile plan directly with the carrier using your own device. We do not activate it for you or routinely track activation completion.
- 6.2 **Delivery of activation details.** We send the SIM details and packaging pictures in a password-protected ZIP by email and send the archive password separately by SMS. The ZIP is generated at the time of sending; HiveReach does not retain a separate generated archive in its application afterward. The underlying SIM records and pictures are held separately for the purposes described in this Policy. Delivery involves our email and SMS providers, and the delivered email and attachment remain subject to the recipient's mailbox and the delivery providers' retention arrangements.
- 6.3 **Refund enquiries.** For a SIM refund request, we may check available technical SIM and network information, request proportionate confirmation and contact the carrier where necessary to clarify activation or registration. These are request-specific checks. Network connectivity alone is not conclusive proof that a particular person registered the SIM. Unrelated personal information may be redacted.
- 6.4 **Stored SIMs and shipment.** After rental ends, a SIM that remains yours is stored separately without a fixed storage expiry until you request its return or give other lawful instructions. We keep the minimum ownership, identification, location and contact records needed to safeguard it and carry out those instructions. A requested shipment involves the address and delivery information needed by the relevant host and delivery provider. Closing an account does not transfer ownership of your SIM or automatically resolve its return.

7. REMOTE SESSIONS AND CONNECTION HISTORY

- 7.1 **Remote access.** We transmit screen and control data to provide the remote-phone session you request. Applications, files, logged-in accounts and other content can remain on your assigned phone between sessions during the rental. Disconnecting ends control access in accordance with session-authorisation rules; it does not reset the phone. Camera, microphone and outgoing-call availability is governed by the selected service and the Terms.
- 7.2 **Detailed connection records.** Detailed connection-history collection is active for rented phones and covers the Account Holder and invited users connecting through supported browser or application clients. Records include the rental owner and connected account identifiers; email and any verified telephone number observed at the time, with verification date or an indication that verification is unavailable; access and invitation references; authentication and controller-session identifiers; connection times, reconnections and termination; the observed client IP address and source port where reliable; limited browser or app information; phone, rack and location identifiers; and related order and payment references.
- 7.3 **Phone network observations.** During control we also check the phone's external IPv4 and IPv6 addresses and record observation times and unsuccessful checks. A check describes the probe's

connection. VPNs, different routes and shared networks can cause another application to use a different address. An observation does not prove which address was used between checks or establish which natural person performed every action.

- 7.4 Limits and purpose.** This connection history is used to investigate misuse, protect accounts and the service, resolve disputes and respond to individually assessed lawful requests. It does not contain passwords, verification codes, cookies, access tokens, message content or network-traffic content. Guest demonstration sessions and separate staff connections are outside this particular log. We do not retain separate controller-session summary records; the detailed connection history remains a distinct record category.
- 7.5 Retention and corrections.** Each detailed session and its events are retained for up to 365 days after confirmed termination. Where termination cannot be confirmed, the reference point is the last established authorisation deadline, with the uncertainty recorded. The period is HiveReach's security and dispute-handling period, not a general legal obligation to retain every connection for one year. Selected records may be preserved under a documented, justified case hold. Historical records show what was observed; a correction can be recorded without falsely rewriting that history.

8. SCREEN MONITORING AND AUTOMATED ANALYSIS

- 8.1 Periodic full-screen capture.** During authorised remote-control sessions, we periodically capture full-screen images for security, abuse detection and investigation. Capture can occur without taps or swipes, and a temporary disconnection may not stop it until session authority expires. This monitoring does not cover the shared public demonstration phone. Relevant privacy information is provided before capture begins.
- 8.2 Information visible on screen.** Images can contain private messages, photographs, account details, credentials and sensitive or financial information about you or other people. Prohibited use does not mean that such information is automatically excluded or masked. Omitting sensitive details from an analysis explanation does not remove them from the original image.
- 8.3 Analysis in Poland.** Images are analysed on a dedicated HiveReach-owned server in Poland for indications of a possible AUP or Terms violation or security threat. The server does not retain screenshot copies after analysis. We do not send screenshots to an external AI service provider for this analysis.
- 8.4 Results and model use.** Analysis produces a flag and explanation. Security credentials and other sensitive details are omitted from the saved explanation. A flag indicates a possible issue, not a finding that a breach or crime occurred. We do not use images or information extracted from them to train models.
- 8.5 Human access and decisions.** Only authorised HiveReach personnel may review relevant images or access a phone for a documented legitimate security investigation, necessary support or maintenance, or a lawful obligation. Curiosity-driven viewing is prohibited. Adverse enforcement based on an analysis flag requires meaningful review by a person who can assess the context and reject or reverse the proposed outcome. Urgent protective restrictions are subject to prompt review. You may provide an explanation and request review through support@hivereach.app.
- 8.6 Storage and ordinary retention.** Source images are stored on HiveReach-owned host machines at the originating phone location. Screenshots and their associated capture metadata, flags and explanations are retained for up to 30 days from the associated image's capture and are deleted earlier when no longer necessary. We do not make screenshot backups. Analysis does not restart the retention period or permit a separate image archive on the Polish server.
- 8.7 Evidence after an established violation.** Following an established AUP violation, we may preserve only the relevant screenshots and associated records beyond the ordinary period while necessary to address that violation, an appeal or related legal claims. The hold identifies its purpose, scope and review date, restricts access and ends when its justification ends. An automated flag alone does not justify longer storage, and a violation does not justify retaining unrelated images. A binding legal preservation obligation may independently require retention of specified evidence.

- 8.8 Privacy protections.** Monitoring is not provided as an employee-performance surveillance service and must not be used for covert monitoring. We do not sell screen captures or use them to train models. Monitoring is covered by a documented data protection impact assessment, and we review its necessity, scope and safeguards when the processing changes. Acknowledgement of monitoring does not provide consent on behalf of another person or waive the right to object.

9. SHARED ACCESS LOCAL HOSTS AND DEMONSTRATIONS

- 9.1 Shared access.** An Account Holder controls invitations and can revoke access. Each invited user has an individual HiveReach identity. Authorised users of the same phone can see content already present through their permitted access; sharing does not itself create isolated Android profiles or sign existing accounts out. Access records support administration and attribution of sessions, with the limitations described in section 7.
- 9.2 Host Managers.** Host Managers provide local premises, SIM purchasing and handling, and instructed equipment maintenance for HiveReach. They may have physical or technical access to phones and host machines. Their permitted role does not include moderation or viewing, copying or using customer content for their own purposes. Any access necessary for an authorised task must be confined to that task. Physical custody and technical capability are not represented as an inability to see customer information.
- 9.3 Public demonstration phone.** The public demonstration is shared between visitors and is separate from a dedicated rental. Do not sign into personal or client accounts or leave confidential information on it. Apps, logins, downloads or settings left behind may remain visible to later visitors. The rental screenshot-monitoring programme and detailed paid connection-history log do not cover this demonstration; technical processing necessary to deliver and secure access still applies.

10. SERVICE PROVIDERS AND OTHER RECIPIENTS

- 10.1 Recipients by function.** Information is made available to authorised personnel and relevant service providers for the functions below. Professional advisers may receive information needed for advice or a dispute; delivery providers and retailers receive information necessary for an agreed transaction. A provider may act as a processor for one activity and as an independent controller for its own account administration, security, compliance or other separately disclosed purposes.
- 10.2 Hosting and database.** AWS provides application, relay and storage infrastructure, including storage of website and legal-document assets. The application deployment uses US East, Northern Virginia. Supabase hosts the database containing account, rental, transaction, support and security records in US East. Provider support or administration can involve other locations. See [AWS privacy information](#) and [Supabase's Privacy Policy](#).
- 10.3 Payments and communications.** Stripe handles payments and, where applicable, identity verification. Telnyx handles telephone verification and service SMS delivery. Resend handles outgoing email and its contents; its email storage is in the United States. Infomaniak handles incoming support email and attachments; its Mail infrastructure and backups are hosted in Switzerland. See [Stripe](#), [Telnyx](#), [Resend](#) and [Infomaniak](#) for their respective notices.
- 10.4 Sign-in analytics and connectivity.** Google and Apple provide optional sign-in. Google Analytics measures eligible website activity as described in section 12. Cloudflare provides connection relay and related usage services through its network. These functions can involve international processing. See [Google's Privacy Policy](#), [Sign in with Apple privacy information](#) and [Cloudflare's Privacy Policy](#).
- 10.5 Error reporting.** Sentry receives sanitised technical error messages and stack traces through US ingestion endpoints. Its configured integration excludes request bodies, cookies, user identities, query strings, breadcrumbs and stack locals. Session replay, profiling and tracing are disabled. See [Sentry's Privacy Policy](#). Error reporting is separate from rental-screen monitoring.
- 10.6 Telegram notification only.** Telegram delivers only a generic operational notification that a new HiveReach support message has arrived. It does not receive the customer's support-message text,

attachments, screenshots or analysis results through this notification. The support conversation is handled in HiveReach's support systems and applicable email services.

- 10.7 Authorities and legal requests.** We assess the requester, legal authority, scope, necessity and applicable transfer rules before preserving or disclosing information. A discretionary request alone does not authorise disclosure. We comply with binding legal process and valid preservation duties, and may make a narrowly justified emergency disclosure where law permits it to address an imminent threat of death or serious physical harm. Notice is given where required or appropriate and lawful; legal prohibitions or lawful investigation needs can limit notice.

11. PROCESSING LOCATIONS AND INTERNATIONAL TRANSFERS

- 11.1 Location of phones and images.** Physical phone and host-machine locations comprise the United States, Canada, the United Kingdom, Ireland, Germany, Australia and New Zealand, subject to actual catalogue availability. The originating location stores its own screenshot images; relevant images are processed in Poland without a retained Polish image copy after analysis. This does not mean that each image is copied to every listed country. Administration is carried out from Poland.
- 11.2 Other processing locations.** The phone's country is not the only location of processing. Application and database hosting uses US East; outgoing email storage and Sentry ingestion are in the United States. Stripe processes and stores Identity verification data in the United States. Infomaniak Mail is hosted in Switzerland. Supabase's contractual and support arrangements can also involve Singapore. Telecommunications, sign-in, payment and global network providers may process information in additional countries under the arrangements applicable to their services.
- 11.3 Adequacy and contractual safeguards.** EU adequacy decisions apply only within their scope. Relevant recognised destinations include the United Kingdom, Switzerland and New Zealand; Canada's decision covers qualifying commercial organisations. The US adequacy framework covers participating organisations. Australia has no general EU adequacy decision. Where a transfer is not covered by an applicable adequacy decision, we use the European Commission's standard contractual clauses and any supplementary measures necessary for that transfer.
- 11.4 Provider terms.** The standard service terms for AWS, Supabase, Resend, Telnyx and Cloudflare incorporate data-processing provisions and, for covered transfers, standard contractual clauses. The safeguards applying to a transfer depend on the recipient, service and processing involved. Our arrangements with separate Host Managers are described below.
- 11.5 Host arrangements and information requests.** Host Managers process personal data under written arrangements that specify permitted instructions, confidentiality, security, access restrictions, incident handling and deletion obligations. Where their access involves a transfer not covered by an applicable adequacy decision, the arrangements include the applicable standard contractual clauses and supplementary safeguards. You may request information about the safeguards relevant to your data, including a copy of applicable contractual provisions, at support@hivereach.app. Protected commercial information may be redacted while preserving meaningful information about the safeguards.

12. COOKIES AND WEBSITE ANALYTICS

- 12.1 Essential storage.** Essential cookies and similar storage support authentication, session security, request-forgery protection, invitation handling and support continuity. They are used where necessary for communications or the service you request. Login sessions have a 30-day inactivity limit and a 365-day absolute limit. Guest support access expires after seven days without qualifying activity. Expiry of a cookie or session does not itself delete the underlying account or conversation.
- 12.2 Google Analytics scope.** With your consent, we use Google Analytics 4 on eligible public marketing pages, signup, sign-in and the generic account-ready page when production analytics is enabled. Google Analytics scripts are excluded from the dashboard, checkout, administration, recovery and verification links, sign-in callbacks, and app or rack handoffs. Measurement concerns website discovery, page use and generic account-readiness events; we do not intentionally include form values, email addresses, account identifiers, authentication tokens or support content.

- 12.3 What Accept and Reject do.** We do not load Google Analytics or initiate its measurement requests before you choose Accept. Choosing Reject keeps Google Analytics disabled. Accept allows analytics cookies and measurement of website use through information such as a sanitised page address, referral origin, event timing, browser information and analytics identifiers. Google also receives the IP address needed for the network request. Advertising storage and user data, personalised advertising, Google signals and enhanced measurement remain disabled.
- 12.4 Change your choice.** Your choice is stored in your browser for 180 days. Use Analytics settings in the website footer to change it. Choosing Reject after Accept withdraws your analytics consent, stops further Google Analytics measurement and removes accessible Google Analytics cookies. If browser storage is unavailable, you may need to choose again. Consent withdrawal does not affect the lawfulness of earlier processing.
- 12.5 Retention and further information.** Google Analytics event-level retention is set to 14 months; aggregate reports may remain available longer. The browser-cookie lifetimes in section 12.6 are separate from this retention period and from the 180-day period for remembering your analytics choice.
- 12.6 Analytics cookies and other tracking tools.** These first-party cookies are set for our website through Google Analytics only after you choose Accept.

Cookie	Purpose	Default expiry
_ga	Distinguishes browsers for website measurement.	2 years from setting or most recent renewal.
ga<container-id>	Maintains Google Analytics session state.	2 years from setting or most recent renewal.

While your analytics consent remains valid, Google Analytics renews these expiry periods when it runs on an eligible page. Browser settings and privacy controls may shorten a cookie's actual lifetime. Renewing a cookie does not itself grant or renew consent.

We do not use additional optional website-analytics services, advertising or remarketing pixels, or tools for replaying website interactions or generating heatmaps. Rental-screen monitoring is described separately in section 8.

13. RETENTION DELETION AND PRESERVATION

- 13.1 Purpose-specific periods.** We keep personal data only for a necessary purpose and an applicable retention period. The ordinary 30-day periods below do not override the specific rules for verification evidence and its associated account references, detailed connection history, active services, stored SIMs or statutory records. A maximum is not a requirement to retain every record for the entire period. We delete information earlier when its purpose and lawful justification have ended.
- 13.2 Screenshots and analysis.** Ordinary screenshots and associated capture metadata, flags and explanations are retained for up to 30 days from the image's capture. Related screenshot-access records are retained for up to 30 days from their creation. There are no screenshot backups, and no screenshot copies remain on the Polish server after analysis. The limited established-violation and binding-preservation exceptions in section 8.7 apply; they do not extend retention of unrelated records.
- 13.3 Detailed connection history.** Detailed rental connection history follows the separate period of up to 365 days after session termination or the last established authorisation deadline described in section 7.5. A documented case hold can preserve selected relevant records for a necessary longer period. Holds have review dates, normally at intervals of no more than 90 days; review is not automatic authority to renew a hold indefinitely. Separate controller-session summaries are not retained.
- 13.4 Accounts and ordinary operational records.** Information necessary to administer an active account, current access, an order or an unresolved service request is retained for that purpose. After closure or completion and once the relevant operational purpose ends, ordinary account and support records, including related correspondence and attachments, are deleted within up to 30 days. The minimum verification-reference records described in section 5.2 follow the period in section 5.5. Records required

for a continuing SIM-storage service, a specific legal duty or a justified dispute are limited to that continuing purpose and follow the corresponding rule below.

- 13.5 SIM information.** We retain the minimum SIM ownership, identification, location and contact information while holding your SIM or completing an agreed purchase, shipment or return. Other SIM details and packaging images are deleted within up to 30 days after they are no longer needed for the agreed handling or support. The generated ZIP is not separately archived in HiveReach's application. Keeping a SIM does not justify retaining unrelated account content or screenshots.
- 13.6 Device content after rental.** When the relevant rental ends or becomes On Hold under the Terms, a seven-calendar-day grace period preserves the assignment and device data without ordinary remote-control access. If the rental is not restored, we wipe customer data within the following 24 hours, subject to mandatory retrieval rights, an applicable DPA and lawful retention of necessary evidence. The phone is not reassigned until wiping is confirmed, and your retained SIM is removed. Eligible statutory retrieval does not require buying a renewal. These rules do not change the separate retention periods for account, payment or monitoring records.
- 13.7 Tax accounting and transaction evidence.** Required invoices and tax records are retained for the applicable statutory period. Under ordinary Polish tax rules, this is generally until the relevant tax liability limitation period expires, normally five years from the end of the calendar year in which payment was due, with statutory extensions where applicable. Particular recordkeeping duties can differ; for example, applicable VAT One Stop Shop records have a ten-year period. Only relevant record categories are retained on this basis; screenshots and unrelated account content do not become tax records.
- 13.8 Disputes and legal duties.** Where a specific complaint, established breach, claim or binding legal obligation requires preservation, we retain only the necessary information for the documented case period or applicable duty. We record a review date and remove the hold when its justification ends. A complaint or exercise of a privacy right is not itself misconduct. Lawful preservation does not authorise unrelated use, indiscriminate extension of retention or reuse of an unwiped phone. For screenshots and their associated monitoring records, the narrower preservation conditions in section 8.7 apply.
- 13.9 Provider-held information.** The 30-day periods for HiveReach operational records are not a representation that every provider-held record follows that period. Stripe Identity evidence and related reference records follow section 5.5, with Stripe's separate processing explained in section 5.6. Google Analytics follows section 12.5. Resend's standard email and delivery-log retention is 30 days on its standard plans, with an additional backup cycle of seven days; remaining customer data is deleted within 90 days after termination of HiveReach's Resend service account, which is separate from closing an individual HiveReach customer account. Sentry's published error-event retention is 30 days on its Developer plan and 90 days on paid plans. Sentry also publishes a separate production-backup deletion cycle of 30 or 90 days from backup creation, depending on the data type. The applicable service plan and deletion controls govern those provider-held operational copies; contact us for the arrangements relevant to your data.
- 13.10 Backups and deletion requests.** We do not back up screenshots. Deletion of other application records and related recovery copies under our control follows the applicable purpose and up-to-30-day deletion process; provider recovery copies can follow the separate cycles described above. Deleted information restored for recovery must remain subject to its deletion instruction. A copy in your own mailbox or a third party's independently controlled service is governed by that recipient's responsibilities. Processor-held copies remain subject to our applicable instruction and oversight duties.

14. SECURITY AND ACCESS CONTROLS

- 14.1 Safeguards.** Controls include encrypted transport, protected credentials, access permissions and encrypted screenshot storage. Authorised review can require decrypting an image; encryption does not mean that HiveReach can never access it. SIM activation archives are password-protected, with the password delivered separately. Technical permissions, local physical access, provider access and deletion remain part of our security responsibilities. No system can guarantee absolute security.

- 14.2 Incidents and account protection.** Protect your login and application credentials, grant shared access carefully and revoke access when authority ends. Report suspected compromise to support@hivereach.app. We assess incidents, take appropriate measures and notify the competent authority and affected people where the applicable legal thresholds require notification. A security investigation is confined to relevant information and does not authorise unrelated viewing.

15. YOUR RIGHTS AND COMPLAINTS

- 15.1 Data-protection rights.** Subject to the applicable conditions and exceptions, you may obtain confirmation and access to your personal data, correct inaccuracies, request erasure or restriction, and receive data covered by the portability right in a structured, commonly used, machine-readable format. You may withdraw consent for consent-based processing. Some records may need to remain for a legal obligation, protection of another person's rights or a justified legal claim; we explain an applicable limitation.
- 15.2 Right to object.** You may object, for reasons relating to your particular situation, to processing based on legitimate interests, including connection-history processing and monitoring. We assess the objection and stop the affected processing unless applicable law permits continuation on compelling legitimate grounds or for legal claims. You may object to direct marketing at any time if it occurs. The ordinary service-complaint route does not replace these rights.
- 15.3 Automated decisions and human review.** You may contest a verification or enforcement result, provide your perspective and request review. HiveReach can review its service-eligibility or enforcement decision and seek assistance from Stripe where necessary; review does not guarantee that a provider's verification result can be changed. Monitoring flags do not by themselves decide a final adverse outcome. Automatic payment-related access controls or urgent protective measures remain subject to the Terms and applicable law. Where Article 22 GDPR applies, its protections and any required safeguards apply; this Policy is not consent to a solely automated decision with legal or similarly significant effects.
- 15.4 Making a request.** Email support@hivereach.app or write to our correspondence address. Include enough information to locate the relevant account or activity; do not send a passport or selfie unless a proportionate verification step is specifically explained. We may request additional information only where reasonably needed to verify authority or identity. A person without a HiveReach account may also contact us about information concerning them.
- 15.5 Timing and charges.** We respond to GDPR requests without undue delay and normally within one month. Where law permits an extension because of complexity or the number of requests, it can be up to two additional months; we explain the reason within the first month. Requests are ordinarily free. Any lawful refusal or fee for a manifestly unfounded or excessive request is explained, together with available remedies. The Terms' separate commitment to respond to service complaints and enforcement appeals within 14 calendar days remains applicable.
- 15.6 Supervisory authority.** You may complain to the President of Poland's Personal Data Protection Office, UODO, at uodo.gov.pl, or to another competent supervisory authority, including in the EU country of your habitual residence, workplace or the alleged infringement. You do not have to contact HiveReach first. Applicable court remedies and other mandatory privacy rights remain available.

16. POLICY CHANGES AND FURTHER INFORMATION

- 16.1 Updates.** We publish a dated version when this Policy changes and provide additional notice where required for a material change. Where new consent is necessary, it is requested separately. Updating this Policy does not retrospectively create consent or authorise a new purpose, transfer or monitoring activity that requires further legal conditions.
- 16.2 Further information.** Contact support@hivereach.app for information about a particular processing activity, relevant recipients and safeguards, retention affecting your data, a privacy request or a review of an enforcement decision. This Policy applies alongside any more specific privacy information provided for the relevant feature, subject to your mandatory rights.