

Helix Privacy Policy

Last updated: 22 October 2026

The named policies and notices below form the Parts of this Privacy Policy. The consumer health notice is also provided on its own directly accessible webpage. Numbered section references remain local to the named Part. Standalone copies of relevant sections are provided through the Legal Centre for direct access; they do not narrow these provisions. Existing mandatory-law and subject-specific priority rules remain. Privacy notices do not themselves replace separate consent.

Contents

Part 1. Privacy Policy

Part 2. Cookie and Similar Technologies Policy

Part 3. Privacy Information and Visibility Schedule

Part 4. Future Family and Genetic Information Notice and Consent Choices

Part 5. Consumer Health Data Privacy Notice

Part 6. Account and Data Deletion Notice

Part 7. California Notice at Collection and US Privacy Rights

Part 1. Privacy Policy

1 Who is responsible and what this policy covers

Helix Match Global Inc., 254 Chapman Rd., Ste 209, Newark, DE 19702, United States, operates HelixMatchGlobal.com and the Helix application. We are the controller of personal information processed for our service purposes. Contact Legal@helixmatchglobal.com for access, correction, deletion, consent withdrawal, complaints, source-data concerns or information about applicable representatives. This policy covers visitors, members, people appearing in submitted content and donors or other individuals whose information is listed from external sources. It covers dating, relationships, marriage-intention matching, co-parenting discovery, donor and donor-bank discovery, genetic-information comparisons, AI illustrations and discussion of fertility expenses. Availability does not mean every feature is lawful in every country. The Terms govern service use. This policy explains processing; reading it or using an account does not itself constitute explicit consent to optional sensitive processing. Where needed, we request permission before the relevant activity. The Consumer Health Data Privacy Notice supplements this policy for covered health information. Mandatory law controls any conflict.

2 Information collected and sources

2.1 Account information: name/display name, date of birth, email/phone, account identifiers, login credentials or authentication tokens, preferences, account status and necessary recovery records, received from you and the authentication functions you use. We collect verification information only if a verification process is offered and explain the check at that time. We do not claim all profiles are identity or age verified.

2.2 Profile and family preferences: photographs, introductions and any offered video, city/region/country, height, eye/hair colour, education, occupation, lifestyle, relationship status, family goals, donor/co-parent categories, selected sex or gender information, sexual orientation or other preferences you choose to disclose. Race/ethnicity, religion, sex-life information and health information can be specially protected. You may omit optional details; some features require relevant inputs.

2.3 Health and genetic information: voluntarily submitted carrier conditions, test status, report extracts or permitted reports, diseases, fertility/reproductive information and comparison results. Information may come from you, a separately authorised integration or a lawfully used donor source. A badge or absence of overlap is not verified medical status. Do not supply relatives' or another person's records without proper authority.

2.4 Interactions: searches, filters, profile views, likes, rejections, matches, saved profiles, generation requests, outputs, delivery records and safety reports. These interactions can themselves reveal health, sexual orientation or family intentions.

2.5 Messages and support: messages, permitted attachments, complaints and correspondence. If calls are provided, participant, time and duration metadata may be processed. This policy does not authorise routine call recording or transcription; any such feature requires its own notice and lawful basis before use. Messages are not represented as end-to-end encrypted. Authorised access for support, safety and legal handling is limited to the relevant need.

2.6 AI inputs and inferences: permitted photos and selected traits, including eye/hair colour, height, self-described race/ethnicity and sex/gender information; simplified phenotype-calculation inputs and outputs; prompts, generated images and generation metadata. Derived probabilities and illustrative outputs may be personal and sensitive information even if not clinically valid.

2.7 Payment information: subscription status, order references, receipts, transaction dates, amounts and refund/chargeback records. Apple, Google or any separately disclosed payment provider may process payment

details directly. Helix Helper currently does not process user-to-user reimbursement payments or collect a commission; discussion records and voluntarily submitted expense documents may nevertheless contain sensitive information.

2.8 Technical information: IP address, approximate IP-derived region, device/browser/app version, session identifiers, operational logs, errors, security events and consent records. Discovery uses selected cities/regions and global searches, not precise live GPS tracking. An IP address or voluntarily supplied billing/support address can reveal additional location information. Do not post exact addresses in profiles or messages.

2.9 External sources: donor-bank publications and other donor sources only where we have an appropriate lawful basis and necessary rights; user reports; authorised providers and account integrations. Source data is not automatically verified. Public availability does not remove privacy, copyright, image or other rights. We limit source use, give legally required notices and address objections and corrections. Where required, we provide source information directly to an affected non-user rather than relying on website publication alone.

3 Purposes and legal bases

Where GDPR-style rules apply, each purpose requires an Article 6 basis and, for special-category data, a separate Article 9 condition. A general legitimate-interest claim or service contract does not replace that condition. Where another law requires express consent, we obtain it. The following purposes describe our framework; only the data necessary for the selected purpose is used.

3.1 Account registration, authentication, requested browsing, communication, subscriptions and support: performance of the service contract or steps requested before it. Sensitive inputs additionally require the applicable explicit consent or other legally available sensitive-data condition.

3.2 Optional sensitive profile fields, genetic comparison and Future Family generation: your specific choices and explicit consent where required. We separately distinguish processing for a requested feature from disclosure to other members and from permission for other users to initiate AI generation involving you. Declining optional processing does not remove access to unrelated services.

3.3 Security, prevention of fraud, proportionate moderation and troubleshooting: legitimate interests in protecting the service and users, assessed against your rights, or legal obligation where applicable. Sensitive information is processed only with a separately applicable condition, such as necessary legal-claims handling where available, rather than automatically on legitimate interests alone.

3.4 Billing records, regulatory responses, mandatory safety reporting and lawful retention: compliance with applicable legal obligations; or necessary establishment, exercise or defence of legal claims where the relevant law permits. Requests from authorities are assessed rather than treated as unrestricted access.

3.5 Non-essential analytics and optional marketing: consent where required for the technology or communication, and another applicable lawful basis only where legally available. Sensitive health/genetic inputs, private messages and identifiable AI inputs are not used for advertising or disclosed to analytics providers for unrelated use. We do not sell personal information or share it for cross-context behavioural advertising under this policy.

3.6 Donor-source listing: an appropriate basis assessed for the actual source and jurisdiction, with any required sensitive-data condition and image/data rights. We do not treat a donor bank's publication or a scraping/search provider as automatic permission. If no lawful basis and necessary rights exist, the relevant content must not be processed or displayed.

3.7 General AI model training using personal inputs is not a current processing purpose. Any future proposal requires a separate notice, defined data and retention terms, and necessary optional affirmative consent before collection/use for training. Merely accepting an amended policy is insufficient where specific consent is required. Genuinely anonymous aggregate information may be used for service evaluation, but pseudonymised or re-identifiable records remain protected personal information.

4 Future Family and automated features

4.1 Helix uses its own image-generation model; the current image-generation workflow does not send inputs to a third-party image-generation API. AWS still processes data as hosting infrastructure. Generations use authorised traits and photos, with simplified calculations before image synthesis. Race/ethnicity and gender descriptors do not establish a genetic profile. Images, ranges and probabilities are hypothetical and may be inaccurate or biased.

4.2 Profile visibility is not permission for someone else to use your photograph in AI. Participation in another member's generations requires a separate permission that identifies permitted audiences and sharing. We stop new use when permission is withdrawn. Revocation cannot guarantee retrieval of independently copied outputs; we address copies and retained inputs under our control as required by law.

4.3 Algorithms may filter/rank results, compare selected conditions, generate illustrations or flag suspected abuse. Inputs can include preferences, location choices and interactions. These functions do not establish clinical suitability or a guaranteed match. Where solely automated decisions have legal or similarly significant effects and applicable law protects you, you may seek human review, challenge the result and obtain the information required by law. Human review of a moderation appeal is available by contacting us.

4.4 We do not treat ordinary photographs as biometric identity templates merely because they are images. Any future face-recognition or identity-template feature requires a separate assessment and applicable notice, consent and retention safeguards before use. This policy is not advance authorisation for it.

5 Visibility and sharing with other users

5.1 Profiles are intended for discovery by the audience disclosed in the feature. Selected display name/age, photos, city, family category and optional traits may be visible to permitted viewers globally. Treat chosen public or member-visible information as accessible to that audience, not as confidential clinical information.

5.2 Sensitive fields, carrier status, individual conditions and comparison results require clearly described sharing choices. Full reports must not be published by default. A match does not unlock all records. Likes, matches and Who Liked You reveal only the interaction information that the feature describes.

5.3 Messages and attachments are delivered to intended recipients and accessible to authorised service personnel only for lawful operational, support, safety or legal purposes. Do not send unnecessary medical records, bank credentials or identification. Recipients may copy or disclose information independently; that risk does not remove our duties for our systems.

5.4 Future Family notifications and outputs are shown only as permitted by the relevant choices. A notification must not imply a real shared child or agreement to reproduce. Information is not made public to search engines merely because it was submitted privately. Where a public page or external sharing is offered, that audience and any resulting indexing risk must be disclosed before sharing.

6 Service providers and other disclosures

6.1 We use Amazon Web Services for hosting in Northern Virginia, United States (us-east-1), and Stockholm, Sweden (eu-north-1), and Google Firebase Analytics for usage analytics. Firebase is a third-party provider even though Helix does not sell user data. Hosting in these regions does not mean every provider's support access or analytics processing is confined to them.

6.2 Depending on the function used, authorised processors may handle authentication, delivery of notifications, payments, support, security, diagnostics or moderation. We disclose material recipient details where required and restrict processors through appropriate contracts, purpose limitations, security and deletion requirements. App stores and independent donor banks or clinics may act under their own notices for their separate services.

6.3 We do not intentionally send full genetic reports, carrier-condition selections, private messages, photographs, phenotype inputs, generation prompts or reproductive expense documents as Firebase analytics events. Analytics must be configured to avoid such disclosures; technical identifiers and usage events can still be personal information. Any new analytics system or materially changed purpose requires assessment and updated disclosures and consent where required before activation.

6.4 We disclose information to legal advisers or authorities only on a lawful basis and to the necessary extent for compliance, claims, fraud or serious safety issues. We assess scope, preserve records where lawfully required and notify people where legally required or permitted. We do not promise immunity from lawful legal process or unrestricted voluntary disclosure of reproductive information.

6.5 A business transaction may involve appropriately limited due-diligence disclosures with safeguards. Identifiable sensitive data is not made freely available to investors. A transfer to a successor must respect applicable law, purpose restrictions and required consents, including any stricter dating-service rules. A corporate sale does not create permission for unrelated AI training or advertising.

6.6 We do not provide another user with unrestricted access merely because they pay Premium. Helix does not disclose health data to insurers, employers or advertising buyers for unrelated commercial exploitation under this policy.

6.7 Third parties that receive personal information to provide Helix services are required by contract to provide the same or equal protection described in this policy and required by applicable law, with purpose limits, appropriate security and deletion/return obligations. Their actual roles and data access must match the feature and consent shown to you. Our current image-generation model operates in-house; we do not currently send inputs to an external image-generation API. Before any future third-party AI sharing, we identify the recipient, information and purposes and obtain explicit permission where required. Declining optional AI processing does not authorise unrelated collection or remove access to unrelated purchased features.

6.8 Donor data obtained from another source requires explicit donor permission for Helix's collection and relevant use, together with necessary source and image rights. Public availability is not permission. Listing, sensitive-data processing, image generation, onward sharing and training are distinct uses; we do not infer all of them from one acceptance. We maintain permission evidence and restrict unsupported records.

7 International processing

Your information may be processed in the United States and Sweden and by authorised providers or personnel in other disclosed locations where lawful. Dubai, India and other planned Asian regions are not currently active Helix hosting regions. Before introducing new destinations, we assess localisation and transfer requirements, update relevant notices and obtain any required permission. Where EEA/UK transfers require safeguards, we use an applicable adequacy route only for eligible recipients/activities or appropriate contractual safeguards, including relevant standard clauses and UK mechanisms as applicable, with required risk assessment and supplementary measures. We do not assume AWS hosting alone establishes those safeguards. Contact us for information about applicable safeguards or an appropriately redacted copy. Other countries may have different protections and lawful government-access rules.

8 Retention and deletion

8.1 We retain data only while needed for disclosed purposes and lawful obligations. Account/profile data generally remains while an account is active; optional sensitive inputs and outputs are retained only for the chosen feature and lawful retention purpose. You may request earlier deletion or withdraw future optional processing without deleting the entire account.

8.2 On a deletion request, the ordinary restoration window is up to 30 days. The profile is hidden and new optional generations using that account are stopped. After the window, personal data is deleted or de-identified unless a lawful exception applies. A mandatory shorter period or immediate deletion requirement takes

precedence; the grace period does not override statutory erasure rights or a valid consent withdrawal.

8.3 Billing records are retained for applicable accounting/tax and transaction obligations. Security and abuse records are limited to the proportionate period needed for fraud prevention, an investigation or legal requirements, and are not automatically retained forever. Consent and contract records may be retained as necessary to establish compliance or defend claims, subject to stricter applicable laws.

8.4 Backups follow defined rotation/deletion procedures and are isolated from ordinary use pending removal; a restoration must reapply valid deletion requests. Legal holds are limited to relevant records and reviewed when the hold ends. Technical limitations do not justify indefinite retention. We provide applicable category-specific retention information on request and any additional legally required notices.

8.5 Withdrawal stops future consent-based processing. It does not invalidate earlier lawful use. We delete or restrict associated information where required and instruct processors as applicable. Independent recipients may retain copies outside our control, but we take further steps required by law. The licence in the Terms does not authorise indefinite retained use.

8.6 You can initiate account deletion within the app. Email is an additional support route. Deactivation is not deletion. Before confirmation, we explain the deletion process, any optional recovery choice, expected completion time and lawful retention exceptions. Any recovery window is subject to applicable deletion deadlines and must not prevent an effective deletion request. We delete associated personal information, subject to the limited exceptions explained above, and arrange required processor deletion. Where Sign in with Apple is used, we revoke the associated tokens as required. Deleting an account does not itself cancel an App Store subscription; we provide cancellation guidance without making cancellation a condition of deletion.

9 Security and incidents

We use safeguards proportionate to data sensitivity, including appropriate access restrictions, authentication, secure configuration, encryption, logging, vendor controls and incident procedures. Authorised staff and contractors access data only for their roles; company permission does not mean unrestricted access. Specific implementations must match the actual deployed service. AWS offers HIPAA-eligible services, but eligibility is not a certification of Helix or its configuration. Whether HIPAA and business-associate agreements apply depends on the actual relationship and data. We do not claim blanket HIPAA certification. Other privacy, health-data and breach laws may apply even when HIPAA does not. No electronic service is completely secure. We investigate and contain incidents, remediate and notify affected people, regulators and other parties within applicable deadlines. A breach can include unauthorised disclosure, not only hacking. This policy does not waive your remedies for a failure to meet our obligations.

10 Choices and privacy rights

Contact Legal@helixmatchglobal.com or use available account controls to request access, a copy, correction, deletion, restriction, objection, portability, withdrawal or review, as applicable. State your account and request without sending passwords or full unnecessary medical records. Non-user donors may also contact us. We use proportionate identity/authority checks and protect others' information. We respond within the applicable legal period, explain lawful refusals, provide appeal/complaint routes where required and do not unlawfully discriminate. The usual GDPR period is one month, with lawful extensions and notice; other laws have different deadlines. You may complain to your competent authority without contacting us first. A request does not require buying a subscription or waiving claims. You may decline optional marketing, unsubscribe from promotional email and manage available cookie/app preferences. Necessary account/security messages continue. Where legally required, we respect recognised opt-out signals such as Global Privacy Control. Browser signals do not automatically withdraw every health or AI permission; contact us for those requests.

11 Regional protections

EEA and UK: you have the GDPR rights described above, subject to lawful exceptions, and may contact your local supervisory authority. Explicit consent for sensitive optional processing is separate from contract acceptance. Required local representative/DPO information must be provided through the applicable regional notice where an appointment is necessary. United States: applicable state rights may include knowledge/access, correction, deletion, portability, limits on sensitive-data use, authorised-agent requests, opt-out and appeal. We do not sell or share information for cross-context behavioural advertising under this policy. We do not require a sale authorisation as a condition of use. The separate Consumer Health Data Privacy Notice gives additional health-data information, sources, recipients and rights, including Washington rights where applicable. Genetic and biometric laws can impose additional permissions and deletion rules. Canada: where applicable, we obtain meaningful express consent for sensitive or unexpected processing, permit access/correction and withdrawal subject to law, and apply relevant federal/provincial requirements.

Information processed abroad may be subject to lawful foreign access. Required local-language and provincial notices are additional to this English policy. Other countries: mandatory local privacy, consumer, localisation, age and health/genetic requirements apply. This policy is not a statement that English-only notices or US terms satisfy every market. Features may be restricted until local requirements are met.

12 Children and other people

The service is for eligible adults. Do not submit actual children's photos or unnecessary children's medical or identifying information for AI or profile use. Generated child illustrations are not photographs of actual children. Do not submit a partner's, relative's or donor's sensitive information without a proper lawful basis and rights. If we discover an ineligible minor or unlawfully collected child data, we restrict processing and take required removal/safeguarding action. Contact us to report such information.

13 Updates and contact

We identify material changes and give notice or seek renewed consent where required before a new use. Future model training, payment services, additional regions or analytics vendors are not authorised in advance by this policy. Previously obtained sensitive information is not retroactively repurposed by a general policy update. Privacy, legal, complaints and support contact: Legal@helixmatchglobal.com. Postal address: Helix Match Global Inc., 254 Chapman Rd., Ste 209, Newark, DE 19702, United States. Website: <https://HelixMatchGlobal.com>.

14 Google Play and Android information

Our Android privacy disclosures cover the same Helix services and company identified above. The Google Play Data safety form describes actual collection and sharing, including SDK behaviour; it must remain consistent with this policy. Firebase Analytics can process app interactions, device/app identifiers and diagnostic information depending on configuration. We do not treat its use as an absence of third-party processing. We obtain any required prominent in-app disclosure and affirmative consent before unexpected personal or sensitive information is accessed or collected; a privacy-policy link or operating-system permission alone is not a substitute.

Users can request account deletion from within the app or outside the app through our website's account-deletion information and request route. The separate Helix Account and Data Deletion Notice explains the email route available without reinstalling the app. The public webpage must be linked in Google Play's designated deletion field. We retain only data necessary for lawful obligations or justified security/fraud purposes and explain those exceptions; freezing an account is not deletion. We do not use health or genetic information for personalised advertising. Optional permissions and consent can be declined or withdrawn subject to the functional limits explained at the point of collection.

15 Additional transparency and control

15.1 Account information comes from you and, only if offered and chosen, the sign-in provider you authorise. A sign-in provider may supply an identifier, name and email, including an Apple relay email; permissions identify the actual fields. Unlinking stops future access but does not automatically erase data already lawfully incorporated into your account. We do not gain your external account password. No contact-book upload, social playlist integration, precise GPS tracking, facial biometric verification, call recording or cross-app profile publication is authorised merely because another dating service offers it.

15.2 We process authorised content and related operational records for delivery, safety investigation and support. Reports can concern on-app or connected offline conduct; necessary information may come from the reporter, affected person or lawful authority. We may give a reporter an appropriate status update without disclosing confidential personal information. When a recipient exercises an access right, copies of their conversations may include your messages, with lawful redactions. An unmatched is not necessarily erasure of all copies or safety evidence. We do not promise end-to-end encryption or universal prescreening.

15.3 Discovery and comparison use supplied profile information, city/region choices, preferences, permitted sensitive fields and selected comparison inputs. Results can be affected by privacy settings, available records, eligibility and safety restrictions. These processes generate inferred compatibility or illustrative traits; an inference may be inaccurate and does not certify a person's health or behaviour. You may correct inputs, change filters, withdraw optional consent and ask for meaningful information or human review where law provides it. We do not authorise a solely automated decision with legal or similarly significant effects on the basis of this policy; any such future process requires a specific lawful basis, notice and safeguards.

15.4 Research participation, testimonials, recordings, promotions, events and publicity are not compulsory. If separately offered, we explain the information, purpose, recipient, retention and any incentive at collection. A consent to appear in a campaign is distinct from using Helix. We do not infer permission to publish fertility success stories, treatment details or actual children's images from a reported outcome. Research does not authorise general image-model training or bypass sensitive-data requirements.

15.5 Helix is not part of Match Group or Bumble Group. This policy does not authorise cross-app matching, profiling or routine sharing with other businesses owned by the same investors. Any actual related-company recipient requires an identified role, purpose, appropriate agreement and additional permissions where required. Hashing an email, substituting an ID or aggregating a small group does not by itself make information anonymous. We do not re-identify lawfully de-identified information except as law permits for testing or compliance.

15.6 You can object to direct marketing at any time, use an unsubscribe mechanism in a marketing message, or contact Legal@helixmatchglobal.com. Service, security and transaction notices may still be necessary. Permission for push notifications, camera or photo-library access can be adjusted through device controls; withdraw the associated processing consent separately where needed. A browser cookie choice may not apply to another device, browser or mobile SDK; use the relevant privacy control or contact us. A recognised universal opt-out signal is honoured where law requires. We do not penalise a rights request; if a necessary input is removed, we explain the affected function.

15.7 For California and other applicable US state rights, see the California Notice at Collection and US Privacy Rights. We proportionately verify access/deletion requests and authorised agents without demanding unnecessary health records. Requests are ordinarily free unless a lawful exception permits a proportionate charge or refusal. If we deny a request, we explain why and how to appeal, subject to legally protected information. We respond under the applicable legal deadline, notify any lawful extension and identify available regulator routes. Trade secrets, other people's privacy and security limits apply only as law permits.

15.8 Our retention criteria are category-specific: account and chosen content for the active requested service; optional health/AI data only while its lawful purpose and permission continue; limited purchase records for tax/accounting and disputes; support and safety evidence for the necessary handling and applicable

claim/retention period; consent records to evidence compliance; and isolated backups under the deletion rotation and legal holds. A ban does not authorise retaining all sensitive information indefinitely. The deletion notice governs the optional recovery process. Mandatory regional return/destruction, health-data deletion and consent withdrawal rules take priority. Ask us for the period or criteria applicable to a particular record.

15.9 Security uses proportionate organisational and technical safeguards and restricted authorised access. We investigate suspected incidents and provide notices, cooperation and remedies required by applicable law, including applicable health-data breach rules. No policy is a security certification or an absolute guarantee. Independent providers' own practices apply when you interact directly with them; we remain responsible for our own disclosures and provider obligations.

16 Inactivity and additional feature changes

An inactive account is not an instruction to preserve all information forever. We review inactive account data against the same necessity, deletion and legal-retention criteria and give any required notice before closure. We do not import another service's two-year or four-year inactivity rule as a Helix practice. You may request deletion without waiting for inactivity closure.

A future quiz, community group, share-a-date tool, social import, biometric check, AI messaging feature, contact feature or additional provider requires accurate feature-specific information before use. A jointly run promotion must identify the independent organiser, its data and terms and the choices that apply. No such practice or third-party controller is established merely by listing it as an example.

17 Notifications external links and restricted records

Operational delivery may involve a device notification token, account/contact identifier, message-delivery status and the minimum notification content needed. Device providers may process delivery information under their own terms. Health, genetic, fertility-expense and AI details should not appear in lock-screen previews by default; any richer preview requires the relevant visibility choice. A shared device or forwarded email can expose information to others. Disabling notifications does not delete server records or withdraw a separate feature permission.

Following an external link discloses ordinary connection information to its destination; the destination's practices apply to its independent service. Where Helix records a link interaction, it is usage information subject to the same purpose, consent and retention rules, not permission to export private searches or sensitive URL parameters. A campaign link must not contain medical records or identify a person's carrier condition. This policy does not authorise email-open tracking or cross-site advertising.

Suspension does not stop you from requesting access, correction, deletion or consent withdrawal. We hide or restrict suspended profiles as appropriate and retain only records justified by the actual service, investigation, legal or safety purpose. Reinstatement must respect intervening withdrawal and deletion requests. When processing is restricted under applicable law, we limit further use accordingly; restriction is not a new licence for research or training.

If we must warn a person about a credible safety risk or fraud ban, the warning contains only relevant identifiers and necessary risk information. It is not routine publication of allegations, full reports, medical details or reporter identities. Such handling requires an actual lawful basis and any separately applicable sensitive-data condition. We assess accuracy and conflicting safety needs and provide correction or review where appropriate.

18 Information about people without accounts

A person can be affected by a donor listing, a safety report or an authorised communication without holding a Helix account. The same purpose, rights, security and retention restrictions apply to their personal information. They can contact Legal@helixmatchglobal.com without registering or paying. Where law requires an indirect-collection notice, we provide the applicable information about categories, source, purpose, lawful basis, recipients, retention and rights within the required period; a webpage alone does not establish delivery or an exemption. Request details of the source of a record using its identifier without sending unnecessary medical information.

An inference can be personal or sensitive information even when inaccurate. You may challenge an inferred trait, request correction of its underlying inputs, and exercise applicable deletion, restriction, objection or review rights over the inference. A hypothetical output does not establish a person's actual health, ancestry, fertility or family relationship. Withdrawal and deletion apply to linked derived records where required, as well as to the original uploaded file.

19 Specific notice before an additional optional function

Before an optional verification, social import, contact feature, recording, research activity or new AI function accesses additional personal information, the relevant notice must identify the data, its source, purpose, actual recipients, visibility, retention or destruction criteria, and available refusal and withdrawal routes. Required affirmative permission must precede access. An existing account, operating-system permission, upload licence or website privacy notice does not authorise a materially different function.

Where biometric identification is proposed, a photograph and a derived identification template are treated according to the processing actually performed. The notice and any required written permission must address the template, provider, retention and destruction separately. No such programme is authorised by this policy's general description of photographs. Necessary manual alternatives and other safeguards apply where required by law.

Legally protected restriction and objection requests apply to linked records and inferences as well as visible profile fields. We isolate information retained for a legal hold, assessment or safety purpose from unrelated recommendation, publicity and training uses. A subsequent registration, restored purchase or reinstated account does not silently restore withdrawn sensitive-data permission.

Where you share a profile, data plan or output outside Helix through an authorised feature, disclose only the information and audience permitted for that use. We explain the fields and any external recipient before the share. Third-party recipients may retain their own copies; that does not remove Helix's duties concerning its controlled copies or disclosures. No contact upload, universal profile-sharing permission or cross-app publication right is created by this paragraph.

Part 2. Cookie and Similar Technologies Policy

1 Operator and scope

Helix Match Global Inc., 254 Chapman Rd., Ste 209, Newark, DE 19702, United States, operates HelixMatchGlobal.com and the Helix app. Contact Legal@helixmatchglobal.com. This policy supplements the Privacy Policy and covers cookies, app SDKs, local storage, pixels and comparable device-access technologies actually deployed. It does not authorise hypothetical future trackers.

2 Necessary technologies

Session, authentication, security, load-balancing and preference-record technologies may be used to provide a requested function or meet security needs. Strict necessity is assessed by purpose and local law; it does not permit unrelated analytics or advertising. Operational logs can exist separately from browser cookies and remain subject to the Privacy Policy. Blocking necessary technologies may prevent login or security functions.

3 Optional analytics and preferences

Google Firebase Analytics is used for app usage/performance analytics. Depending on configuration, it processes app-instance/device identifiers, technical information and usage events and may use provider infrastructure outside the hosting regions stated for Helix. Firebase is a third-party service; this is processing even though Helix does not sell user data. Google explains its practices at <https://firebase.google.com/support/privacy>.

Optional analytics and non-essential preference technologies must not activate before consent where required. We do not use genetic reports, condition selections, reproductive documents, private messages, images, prompts or phenotype inputs as analytics event payloads. Information that can be linked to a person is not anonymous simply because names are removed.

4 Advertising and future systems

This policy does not authorise sensitive-data advertising, cross-site marketing trackers or a future analytics vendor. We do not sell personal information or share it for cross-context behavioural advertising under the current Privacy Policy. New technologies require a purpose, necessity and privacy assessment, revised disclosures and any required prior consent. We do not relabel advertising as necessary security.

5 Choices and consent

Where required, the website/app provides accept, reject and customise choices for non-essential technologies, with rejection as accessible as acceptance, optional categories off until chosen and a way to change choices. These choices must operate before optional access, not merely hide a banner. You may also contact Legal@helixmatchglobal.com to withdraw optional analytics consent.

Browser settings may block or erase cookies. App settings and device controls may apply to SDKs and identifiers. Controls vary by browser/device; browser deletion is not account deletion or automatic withdrawal of all genetic/AI permissions. Turning off analytics should not prevent unrelated essential use. We process applicable Global Privacy Control or other legally recognised signals as required.

Consent records identify the choice, notice version, time and relevant device/account context without using unnecessary sensitive data. Withdrawal stops future optional access but does not make earlier lawful processing unlawful. Deleting device storage may require you to set preferences again.

6 Technology inventory and duration

Necessary session/security records last for the relevant session or proportionate security period; persistent preferences last only as needed for the selected function. Optional analytics identifiers and events follow the actual configured retention limits and applicable law. We do not represent every item as a session cookie or rely on a provider's longest default period without assessing necessity.

The deployed website/app must provide a current technology inventory identifying each actual cookie/storage key or SDK, provider, purpose, essential/optional status and expiry or retention period before consent where required. Provider categories are not a substitute for that inventory. Ask Legal@helixmatchglobal.com for details or to report an unlisted technology. This policy does not permit deploying an undisclosed optional tracker.

7 International handling and security

AWS hosts Helix systems in Virginia and Stockholm; Firebase processing is not necessarily limited to those regions. Transfers require applicable safeguards; see the Privacy Policy. We limit access, apply appropriate safeguards and retain choice records only for a justified compliance period. No system is absolutely secure; statutory obligations and remedies remain.

8 Changes and complaints

We date updates and obtain fresh consent when needed before material technology or purpose changes. Questions, preference requests and complaints may be sent to Legal@helixmatchglobal.com or the company address above. You may complain to the competent regulator. Mandatory privacy and electronic-communications rights are not waived.

9 Cookie types related technologies and controls

A first-party technology is set by Helix; a third-party technology is set by another provider. Session storage ordinarily ends with a session, while persistent storage remains for its disclosed lifetime unless removed earlier. Pixels, beacons, tracking links, local storage, app-instance identifiers and SDKs can perform similar device-access or measurement functions; calling one an SDK does not remove applicable consent requirements. Necessary security and authentication functions differ from optional analytics or campaign measurement.

Firebase Analytics is the confirmed analytics service. No Google Maps, social-network plugin, advertising network, email-tracking pixel, contact upload, cross-device advertising graph or automatic photo-optimisation tool is represented as deployed merely by this policy. If an optional embedded third-party service is offered, we identify the provider, data access, purpose and required choice before activation. Third-party links may use separate policies when you leave Helix; they do not excuse our own disclosures.

Non-essential analytics, performance measurement, social sharing and advertising categories must be classified by their actual purpose. No current advertising or social-cookie deployment is authorised here. Information linked with account or device records remains personal information. Health/genetic fields, private content and AI inputs/outputs must not become analytics labels, URLs or event properties.

You can reject or later withdraw optional technologies through the applicable cookie/privacy controls or contact Legal@helixmatchglobal.com. We do not treat continued browsing, a preselected box or an operating-system permission as the separate consent required for another purpose. Browser clearing or identifier reset may require you to set preferences again and does not erase server records automatically. Choices may differ between devices and between the website and app; essential security records and your other feature permissions remain separate. Opt-out industry tools do not replace Helix's own duties or control every provider.

The current inventory must identify actual keys/SDKs, provider identity and privacy link, purpose, category and lifespan or configured retention. We explain material changes and obtain renewed consent where needed before a new purpose begins. We do not invent cookie names or expiration periods. The Privacy Policy, California notice and account-deletion notice provide additional controls and request routes.

10 Browser signals and independent controls

A general browser Do Not Track setting and a legally recognised opt-out preference signal are different. We do not interpret an ambiguous signal as affirmative consent. We honour signals such as Global Privacy Control to the extent required, alongside the choices described above. A Google Analytics browser add-on does not necessarily control Firebase app analytics. Use the relevant app/device privacy controls or contact Legal@helixmatchglobal.com for the applicable Helix choice. Independent industry advertising tools do not operate every tracker or replace a required Helix opt-out.

Part 3. Privacy Information and Visibility Schedule

Helix Match Global Inc. operates HelixMatchGlobal.com. Contact Legal@helixmatchglobal.com; 254 Chapman Rd., Ste 209, Newark, DE 19702, United States. This schedule supplements the Privacy Policy and feature choices. An audience description is a boundary to enforce, not blanket permission to publish sensitive information.

Profile and discovery

Information	Audience and purpose	Permission and boundary
Display name and age	Permitted viewers for account discovery	Avoid unnecessary legal identifiers; age is self-declared unless the stated check occurred.
Profile photos and introduction	Chosen profile audience	Upload and display rights required; separate AI permission. No deceptive synthetic identity or child-only photo.
City and search region	Relevant discovery viewers	Global/city search; no precise live GPS discovery promise. IP/billing information can reveal other location.
Family and donor category	Chosen feature audience	Relevant sensitive processing and sharing choices required. A category is not reproductive consent.
Height eye and hair colour	Selected profile audience	Optional traits may be omitted; not verified inheritance.
Race ethnicity sex gender orientation	Specifically disclosed selected audience	Special-category protections apply; no DNA inference or general training permission.
Education occupation interests	Selected profile audience	Optional supplied information; avoid workplace contact identifiers.
Likes matches saved profiles	Users entitled by the feature	Premium does not confer all-data access. A like is not consent to reproduction or AI use.

Health AI and communication

Information	Audience and purpose	Permission and boundary
CGT status and badges	Expressly authorised audience for informational comparison	Self-declared unless the specific check says otherwise. No clinical clearance.
Conditions and comparison	User and separately authorised recipient	Missing information is not a negative result; sharing separate from processing.
Reports and clinical records	Restricted operational processing and expressly selected recipient	No full public reports by default; no unauthorised relatives' records.
Future Family inputs	Authorised systems/personnel for the requested result	In-house model on AWS; no current personal-input training.
Generation involving another person	Only initiator and recipients allowed by that person's permission	An active profile is not permission; no selected audience by default.
AI images traits notifications	User and separately permitted recipients	Hypothetical AI labels; no verified child, paternity, health, appearance or mutual intention.
Messages attachments	Intended recipients and necessary authorised support/safety access	No end-to-end encryption claim. Recipients can copy; an unmatched is not complete erasure.
Expense discussions evidence	Intended recipients and lawful restricted support/safety handling	Minimise/redact evidence; no Helix custody, guarantee or commission.

Source data administration and rights

Information	Audience and purpose	Permission and boundary
Third-party donor records	Only permitted discovery audience	Explicit donor permission and source/image rights; public accessibility is insufficient. Listing is not AI permission.
Purchase and subscription records	User, necessary personnel and actual payment channel	App-store roles differ; do not send full card data to support.
Analytics technical events	Authorised operational providers and Firebase as configured	No health/genetic fields, private content, photos, prompts or AI traits in event payloads. Identifiers remain personal data.
Consent and safety records	Restricted authorised personnel/providers	Purpose-limited compliance and review; no indefinite all-data ban retention.
Deletion and controlled copies	Authorised privacy personnel/processors	In-app and external requests; recovery window cannot override effective deletion or stricter law.
Accessibility and support requests	Personnel needed to address the request	No diagnosis required; health-revealing information receives appropriate protection.
International hosting	AWS and authorised operational access	Current Virginia us-east-1 and Stockholm eu-north-1; Firebase/other provider locations assessed separately. Future regions not pre-authorised.

Choices and further information

Review the specific fields and audience before sharing. You may request access, correction, deletion, withdrawal, restriction or review under applicable law. Reporters and other recipients may receive a legally appropriate outcome or copy without unrestricted access to another person's records. Helix does not routinely publish profiles on unrelated investor-owned apps. Personal information is not anonymous merely because a name is removed. See the Privacy Policy, Consumer Health Data Notice, California Notice and Account and Data Deletion Notice. Mandatory rights remain, and nothing promises perfect security, donor anonymity or clinical accuracy.

Notifications links and suspension

Notification delivery uses necessary contact/device-delivery information. Preview content must respect the audience and sensitive-data choices; notification permission is not permission to show private health details on a lock screen. External recipients may see a forwarded notification. Link interactions, where recorded, remain usage data under the Privacy Policy. Suspension does not prevent privacy requests; reinstatement respects valid withdrawals and deletions. A necessary safety warning to an affected member is limited to relevant risk information under the Privacy Policy and Community Guidelines.

Part 4. Future Family and Genetic Information Notice and Consent Choices

1 Who processes your information

Helix Match Global Inc., 254 Chapman Rd., Ste 209, Newark, DE 19702, United States, operates these features. Contact Legal@helixmatchglobal.com to ask questions or exercise choices. Read the Privacy Policy, Consumer Health Data Privacy Notice and Terms together with this notice. These choices do not waive statutory claims or approve another person's reproductive arrangements.

2 What the tools do

Carrier comparison uses conditions and statuses you choose to provide. Self-declared status is not authenticated testing. Results may omit variants, conditions and inheritance risks, particularly across different panels. Missing information is not a negative result and no shared condition found is not medical clearance. Obtain clinical confirmation and genetic counselling before reproductive decisions. Future Family processes authorised photographs and selected eye colour, hair colour, height, race/ethnicity and sex/gender-related inputs through simplified phenotype calculations and Helix's own image model. The outputs depict hypothetical children/adults and possible traits. Race/ethnicity and gender identity do not establish DNA or biological inheritance. No number or realistic image is a validated prediction of your particular future child. No image confirms health, paternity, conception, sex, appearance or development. The current workflow does not use a third-party image-generation API. AWS hosts the processing; that is still provider processing. No current general training of the image model on users' personal inputs is authorised by these permissions. Future training requires a separate, specific notice and any required optional consent before use begins.

3 Separate choices

Make each choice separately for the feature and audience identified. Optional choices are not selected by default. Declining an optional choice leaves unrelated features available. A consent for processing does not automatically authorise sharing. Select only choices you understand; no choice is inferred from a subscription or profile upload.

Choice A - Optional sensitive profile processing: I explicitly consent to Helix processing the sensitive fields I select to provide the profile/discovery functions I request. I have been shown the selected fields and purpose before submission. I understand optional fields can be omitted.

Choice B - Sensitive profile sharing: I explicitly consent to the specific sensitive fields I select being shown to the audience identified in the sharing screen. I understand whether that audience consists of other eligible profile viewers, matches or specifically selected recipients. Full medical/genetic reports are not included by default.

Choice C - Carrier comparison processing: I explicitly consent to Helix processing the conditions, carrier status and permitted report information I select to calculate an informational comparison. This does not certify either person's results. I have authority to submit my inputs.

Choice D - Carrier result sharing: I explicitly consent to the selected comparison result or status being disclosed to the particular user or recipient group shown before sharing. This does not authorise disclosure of a full report or unselected conditions. Where law requires separate health-sharing consent, this is separate from Choice C.

Choice E - My requested Future Family generation: I explicitly consent to processing my selected photos and traits for the requested phenotype calculation and AI illustration. I understand the limits above and have authority for my own inputs. Processing another participant's data requires that participant's applicable permission or another established lawful basis; my choice cannot supply it.

Choice F - Other users initiating generations involving me: I optionally permit Helix to use the selected photos/traits for generations initiated by the audience I choose. My choice identifies mutual matches, selected users or other eligible viewers; no audience is selected by default. I understand the initiating user will see the permitted output and may receive the disclosed notification. I may disable future participation without deleting my dating profile.

Choice G - Sharing an output: I authorise the selected output to be sent to the recipients/audience identified at this step. I understand a recipient may copy it. The result remains labelled as hypothetical AI content and must not imply the other person has agreed to a relationship or child. A separate participant's privacy settings and rights still apply. There is no active training checkbox in this current release. A future optional training request must identify exact input categories, model-improvement purpose, recipients, retention, withdrawal consequences and safeguards. It must not be preselected, required for unrelated service use or combined with the requested-image permission.

4 Withdrawal and consequences

Change the relevant feature controls where offered or email Legal@helixmatchglobal.com identifying the choice to withdraw. We stop new consent-based use for that purpose and delete/restrict related inputs and outputs where required. Withdrawal does not invalidate earlier lawful processing, but an output's independent copy may remain with a recipient. We address controlled copies and processors as required by law. No indefinite licence or general-training right survives merely because a generation occurred. You may withdraw another-user participation while retaining your own image feature, or request deletion of a report while keeping your account. A feature may cease to work if a necessary input or permission is removed; unrelated services remain available. Mandatory erasure deadlines prevail over the ordinary account restoration period.

5 Input and output restrictions

Do not upload actual children's photos, unauthorised partners' or donors' images, relatives' reports or scraped images for AI. A donor-bank listing does not establish AI rights. No sexualised child imagery, intimate-image abuse, harassment, face impersonation or false parentage claims are permitted. Helix may reject or remove inputs/outputs for legal or safety reasons. Report concerns to Legal@helixmatchglobal.com.

6 Short notice displayed with every result

AI illustration only. Trait estimates use simplified assumptions and may be wrong. This is not a prediction of a particular child, medical advice, a genetic test, paternity evidence or a promise of conception, health or appearance. Consult qualified professionals for reproductive decisions.

7 Accuracy labels reporting and rights

Helix is not a medical device and does not diagnose, treat, cure or prevent a medical condition. Consult a qualified healthcare professional for medical advice, diagnosis or treatment. This description does not exempt an actual regulated function from law. An adult illustration is not a forecast of a child's development or gender identity. AI results can contain bias, inconsistencies or invented details and may resemble outputs produced for others. No exclusivity, protectable copyright or scientific accuracy percentage is promised.

Report an unsafe or offensive generated result using the in-app reporting function without leaving the app, or contact Legal@helixmatchglobal.com. Do not redistribute harmful output as evidence. No automated output authorises a medical, parenting or payment decision. Listing a donor, liking a profile or paying for Premium does not replace explicit participant permission. Source and image rights must also be established. The separate donor permission form applies where third-party donor inputs are proposed.

To record a choice, Helix identifies the specific fields, purpose, audience, notice version, person giving permission and time. Independent choices remain separately revocable. General service feedback and

aggregate service statistics do not create permission to train on your photos, genetic records or sensitive traits. Publicity, research and any future third-party AI transmission require their own disclosures and lawful permissions.

10 Reviewing generated material before sharing

Review every illustration and associated text before downloading or sharing it. Output can contain visual defects, fabricated details, bias or misleading traits even when it looks realistic. Do not claim that a clinician, laboratory or depicted person validated it, or present a generated age progression as evidence of identity. Permission for one generation does not authorise later generations with new inputs, public marketing or a different audience. Report unsafe output through the app or Legal@helixmatchglobal.com. Helix may refuse or restrict prohibited generations; this does not establish that every permitted output is accurate or safe.

11 Consent to a calculation is not consent to a depicted relationship

A request to generate an illustration and permission to use another adult's inputs are distinct choices. Neither establishes that the people depicted are dating, engaged, married, planning a pregnancy or consenting to donor or co-parenting arrangements. Do not use an output as evidence of such agreement, a real pregnancy or a person's reproductive capacity. A realistic likeness or displayed notification is not authentication. Report an unauthorised use by identifying the generation or record; no account or subscription is required to raise a rights complaint.

Part 5. Consumer Health Data Privacy Notice

1 Scope and responsible entity

Helix Match Global Inc., 254 Chapman Rd., Ste 209, Newark, DE 19702, United States, processes consumer health data for HelixMatchGlobal.com and the Helix app. Contact Legal@helixmatchglobal.com to exercise rights or ask questions. This standalone notice provides additional health-data disclosures, including under Washington's My Health My Data Act where applicable. It supplements the Privacy Policy; it is not consent to collection or sharing and does not reduce protections under other laws.

2 Categories collected

Where relevant to a requested feature and lawfully provided, we process reproductive/fertility information and family-building intentions; selected diseases, carrier conditions, test statuses and report information; health/genetic comparison results; donor health/history information from lawful sources; and AI inputs or outputs/inferences that reveal or imply health, genetic or reproductive information. Associated profile, account and technical identifiers can link these categories to a person. Health-related searches, filters, likes, messages, expense discussions or attachments can reveal a person's attempt to obtain health/reproductive services, preferences or treatment-related costs. Location choices and approximate technical location may become health data when they identify or infer such activity. We do not use precise-location geofences around health facilities to identify care-seekers, track them or deliver health-related advertising. This notice does not authorise collecting unneeded information or any future biological sample, biometric template or model-training dataset.

3 Sources

We receive data from the individual and the features they request; another user only where that submission is authorised and lawful; separately authorised laboratory/provider integrations if offered; and donor banks or other external sources only where an appropriate lawful basis and necessary rights exist. We generate comparisons and illustrative inferences from authorised inputs. Public availability alone is not permission for sensitive-data reuse. Technical records arise from operating and protecting the service.

4 Purposes

We use only necessary and lawfully authorised information to provide selected sensitive-profile/discovery functions, carrier comparison, requested Future Family calculations/illustrations, intended communications and expense discussions; deliver support; secure the service and investigate abuse; process valid privacy requests; meet legal requirements; and establish or defend lawful claims where permitted. Sensitive-data conditions apply separately to safety or legal handling where required. General training of the image model on personal inputs is not a current purpose. Any future training proposal requires separate disclosures and any required optional consent in advance. Health/genetic data and private content are not used for advertising or sold under this notice.

5 Categories shared and recipients

Other members receive only the selected profile/health fields, status or comparison results, messages/expense attachments and AI outputs that the relevant permission and feature disclose. Report documents are not public by default. A match does not grant all-data access. A user's own consent cannot authorise another person's data without their lawful permission.

Processors receive only what is needed for hosting, authorised support/security, delivery and other requested operational functions under applicable contracts. Amazon Web Services is the confirmed hosting provider. Google Firebase Analytics receives technical usage information under the Privacy Policy, but genetic reports, condition choices, private messages, photos, AI prompts/traits and reproductive expense documents must not

be included as analytics payloads. Health-related usage and identifiers must be assessed to prevent inadvertent health disclosure. An independent laboratory, clinic or donor bank receives health data from Helix only where you expressly request and lawfully authorise the relevant transfer or another applicable legal requirement permits it. Listing an institution does not mean records are automatically transmitted to it. Competent authorities, courts and professional advisers receive only information lawfully necessary for the relevant process, safety response or legal claim. A successor or transaction counterparty is subject to applicable health-data purpose, confidentiality and consent restrictions; financing is not permission for unrestricted health-data access. Helix does not routinely share consumer health data with affiliates under this notice. If a specific affiliate is to receive it, Helix must name it and obtain the required permissions before sharing. Categories of independent recipients include the selected other members, separately authorised healthcare providers/donor banks, lawful authorities and advisers; processor categories are described above. We do not sell consumer health data. No sale authorisation is sought as part of registration.

6 Consent and withdrawal

Where applicable, we obtain consent before collecting health data for a specified purpose and separate consent before sharing it, except to the extent a statutory requested-service or other lawful exception actually applies. The request identifies the categories, purpose, recipient categories and withdrawal method. General acceptance, a broad licence or agreement to a Privacy Policy does not replace the required permission. We do not infer a health-sharing permission from Premium payment. You can withdraw future consent through relevant controls or Legal@helixmatchglobal.com. We stop the affected consent-based activity and delete/restrict data as required. A selected feature may no longer work without necessary data, but unrelated access is not conditioned on unnecessary permission. Withdrawal does not validate past unlawful processing or invalidate earlier lawful use.

7 Access deletion and appeals

Where the applicable law provides them, you may confirm whether we collect/share/sell health data; access it and obtain the legally required list of recipients and contact information; withdraw consent; and request deletion. We verify requests proportionately, accept authorised representatives as law permits and provide accessible requests without unlawful discrimination. For Washington rights, we respond without undue delay and within 45 days, with a lawful extension of up to 45 additional days where necessary and timely notice. We delete applicable records and notify relevant processors, contractors, affiliates and other recipients as the law requires. For qualifying archived/backup systems, any statutory delay is used only as allowed, with the required isolation and outer deadline; Washington permits certain backup delay up to six months. The ordinary 30-day account restoration option does not override these rights. If we deny a request, we explain the basis and how to appeal. Email Legal@helixmatchglobal.com with the request and reason for appeal. For Washington appeals, we respond within 45 days with the result and reasons and, if denied, provide an online mechanism or other method to contact the Washington Attorney General at <https://www.atg.wa.gov/file-complaint>. Different applicable laws may require a shorter deadline or additional rights, which prevail.

8 Retention and protection

Health data is retained only for the selected purpose and a valid legal retention basis, with restricted access and appropriate safeguards. We do not keep full reports merely because it might be useful later or claim anonymity when re-identification remains possible. Account closure, consent withdrawal and processor deletion follow the Privacy Policy and stricter applicable rules. Helix does not promise absolute security or waive breach notification/remediation duties.

9 Changes and contact

Before new health categories, purposes or recipients are introduced, we update disclosures and obtain any required affirmative permission. Future payment facilitation, hosting regions or AI training are not authorised by this notice. Contact Legal@helixmatchglobal.com or Helix Match Global Inc., 254 Chapman Rd., Ste 209, Newark, DE 19702, United States.

10 Further health categories and regional rights

Consumer health data can also include mental-health disclosures, counselling, treatment and procedure histories, medications, bodily measurements, reproductive or sexual health, gender-affirming care, genetic characteristics, attempts to obtain care, accessibility requests that reveal a condition, and health information in safety reports. Helix does not collect every category as a mandatory field; information may be provided through optional content or necessary support. Identifiers and inferences can link it to you. Do not submit another person's records without authority. No biometric identification or precise-location healthcare tracking is authorised by this notice.

This notice also applies to Nevada consumer health data where its law covers the processing. Applicable rights include confirmation, access, required recipient information, withdrawal, deletion, appeals and non-discrimination, with the timing and exceptions required by that law. Contact Legal@helixmatchglobal.com for the initial request and for an appeal identified as Health Privacy Appeal. We explain a denial, any lawful extension and the relevant regulator route. Washington's specific rights and 45-day periods above remain. We do not geofence a healthcare facility to identify or track care-seekers or send health-related advertising, sell consumer health data, or obtain a sale authorisation through general acceptance.

For an authorised health-data sharing choice, the collection purpose, data categories, intended recipient categories and withdrawal route must be disclosed separately from general dating acceptance. Corporate ownership changes, source-bank publication and another member's consent do not waive these protections. The California notice and other applicable privacy rights remain additional. Required notices of a health-data security incident are not waived by the no-medical-advice disclaimer.

11 Health information in accessibility and safety communications

Health data may arise from non-prescription treatment discussions, accessibility assistance, a safety complaint or an inference about seeking care even if no medical field is completed. The purposes and protections in this notice apply to such information. Necessary safety warnings to affected people must be limited and lawfully justified; the existence of a report does not permit public disclosure of a person's diagnosis, genetic report or reporter identity. A sensitive datum is not excluded from this notice merely because it came through chat, a support form or an external source.

12 Inferred health information and non-members

Health-related inferences and identifiers remain protected where the applicable law covers them even if an inference is wrong or the affected person has never joined Helix. A rights request may identify the listing, message or generation involved without creating an account. No generated appearance is proof of a diagnosis, reproductive capacity, genetic relationship or treatment outcome. Necessary identity checks must be proportionate; a request to correct or remove such an inference does not require a full medical record. The collection, sharing, withdrawal and deletion requirements above continue to apply to these records.

Part 6. Account and Data Deletion Notice

Helix Match Global Inc. | HelixMatchGlobal.com

Request deletion within Helix

Use the account deletion option in the Helix app's account settings and follow the confirmation instructions. Deactivation or hiding a profile is not account deletion. If you cannot access the app, use the outside-app route below; you do not need to reinstall Helix to submit a request.

Request deletion outside the app

Email Legal@helixmatchglobal.com with the subject Delete Helix Account. Identify the email address or account identifier associated with your Helix account and state that you want the account and associated personal data deleted. You may send this request even if you cannot sign in. We use proportionate verification before acting to prevent unauthorised deletion; never send your password, full payment details or unnecessary medical/genetic records. Support will explain any additional verification necessary and acknowledge the request.

What deletion covers

We close your account, remove your profile from discovery and delete associated account/profile information, uploaded photos, personal AI inputs and outputs, messages and other associated personal information held by Helix, except to the extent lawful retention is necessary. We arrange required deletion by service providers. Other users' independently held copies, recipients' records and a donor bank's independent records may require separate requests. We do not treat freezing an account as deletion.

Recovery, timing and retained information

Before confirming deletion, we explain the completion period and any optional recovery choice. The ordinary account recovery period is up to 30 days; it must not override an effective deletion request, applicable deadlines or a user's decision to proceed with deletion. If verification or an applicable legal requirement affects timing, we explain that rather than promising an unsupported universal completion period.

Limited billing/tax records, records necessary for security, fraud prevention, safety, legal claims or compliance may be retained only for the applicable legal obligation or necessary purpose. Access and further use are restricted. Backups remain isolated from ordinary use and are removed under the applicable rotation process, subject to lawful holds. We explain applicable retention grounds and timing when responding to your request, including any request we cannot fully fulfil. See the Privacy Policy for additional detail and rights.

Subscriptions and sign-in

Deleting your account or uninstalling Helix does not itself cancel a subscription billed by Apple or Google. Manage the subscription in the purchasing store's subscription settings. Cancellation guidance does not block account deletion. Eligible refunds remain subject to mandatory law and the Refund and Cancellation Policy. If Sign in with Apple was used, associated tokens are revoked as required.

Contact

Helix Match Global Inc., 254 Chapman Rd., Ste 209, Newark, DE 19702, United States. Email Legal@helixmatchglobal.com. Website <https://HelixMatchGlobal.com>.

Additional privacy and appeal options

You may request deletion of selected health, genetic or AI information without closing your entire account where applicable. Withdrawal of optional processing/sharing can be exercised independently. An unmatch, a cookie reset, revoking a device permission or unlinking a sign-in provider does not necessarily erase information

already held; state the data and right you wish to exercise. No new purchase or subscription cancellation is required to submit a deletion request.

If we cannot fully act, we explain the lawful reason, relevant retention criteria and appeal route. Email Legal@helixmatchglobal.com with the subject Privacy Appeal and identify your request; applicable state health/privacy and EU/UK remedies remain available. We use proportionate verification, consider authorised agents where law permits and do not discriminate against a rights request. Relevant account and processor copies are handled under the Privacy Policy, Consumer Health Data Notice and stricter regional rules.

Suspended accounts and renewed access

An account suspension, ban, ongoing refund request or inability to sign in does not prevent a deletion or other privacy request through Legal@helixmatchglobal.com. Any permitted legal/safety retention remains limited to its justified scope and period. Restoration or a later registration does not silently reactivate a revoked AI participation permission, revive data already erased or authorise new use of a retained medical record. Subscription recovery and consent recovery are distinct.

Part 7. California Notice at Collection and US Privacy Rights

Helix Match Global Inc. operates HelixMatchGlobal.com and the Helix app. Contact Legal@helixmatchglobal.com or write to 254 Chapman Rd., Ste 209, Newark, DE 19702, United States.

1 Notice at collection

This notice supplements the Privacy Policy for California residents and describes applicable US state privacy rights. Helix Match Global Inc. is responsible for its processing. It is intended to be available at or before relevant collection. The categories below describe Helix functions and information you choose to provide; they do not assert that every category is collected from every user or that Helix already operated every feature for a full prior year. The Privacy Policy describes sources, recipients and legal bases in more detail.

2 Categories purposes and retention criteria

Identifiers and contact/account data include your name or display name, account ID, contact details, date of birth, sign-in credentials or tokens, and IP/device identifiers. Sources are you, an authorised sign-in provider if used, and operation of the service. Purposes are account access, delivery, support, rights handling and security. Account records are held for the active service and the disclosed recovery/deletion process; limited consent, security and legal evidence is retained only while the relevant purpose or legal obligation requires.

Customer records and commercial data include contact details, purchase channel, order and entitlement history, price, billing/refund and dispute records. Payment stores or providers may separately hold full payment details; Helix does not obtain full card details merely because you buy through a store. Purposes are purchases, entitlement restoration, refunds, fraud prevention and accounting. Retention follows applicable transaction, tax, audit and dispute obligations rather than a perpetual account licence.

Protected characteristics and sensitive information may include age, gender, race/ethnicity, religion if voluntarily supplied, relationship or family intentions, sexual orientation/sex-life information, reproductive/health and genetic information, carrier statuses and permitted reports, and associated inferences. Authentication credentials are also sensitive where legally defined. Processing is limited to the selected discovery, comparison, communication or AI purpose, required support/safety handling or another lawful specified purpose. Optional processing and sharing require the relevant separate choices. Retention ends when the purpose/permission ends subject to actual legal exceptions; sensitive information is not kept simply for possible later training.

Internet/network activity and approximate location include searches, feature interactions, likes/matches, logs, device/app/browser details, IP-derived area and selected city/region. We use them to operate, protect, troubleshoot and assess the service and, where permitted, provide optional analytics. Technical and analytics records are held only for the operational or permitted analysis need, with the applicable configuration and restricted legal records. Discovery is not represented as precise live GPS tracking. This notice does not authorise new precise geolocation or health-facility tracking.

Visual, electronic and communication information includes photos, profile text, messages, attachments, generated images, safety reports and support exchanges. Purposes are chosen display/delivery, requested generation, support and lawful moderation. Retention follows the selected service, audience, deletion, incident or dispute purpose. Other recipients may independently retain copies. No call-recording or audio/video feature is created by this category description.

Professional, education and personal preference information includes optional occupation, education, interests and desired family or match characteristics you supply. Helix does not represent that it obtains protected school records from an educational institution. Inferences include informational compatibility and hypothetical appearance/trait outputs from authorised inputs. These can be inaccurate. They support the requested feature

and are subject to the input/output permissions, retention and deletion rules; no clinical or credit/employment eligibility decision is established.

No collection of biometric identifiers for unique identification, government ID programme or biological samples is authorised merely by this notice. If such a verification process is introduced, a specific prior notice must identify actual categories, purpose, recipients, retention/destruction and legally required permissions. A photograph or generated illustration is not automatically a biometric identification template.

3 Disclosures and sale or sharing choices

For the categories above, recipients are the audiences you lawfully choose, operational hosting/support/security/analytics providers limited to their function, Apple/Google or another actual payment channel for purchase handling, separately authorised independent clinics/labs/banks, advisers and competent authorities where lawful, and a constrained business successor subject to required safeguards. AWS hosting and Firebase Analytics are identified in the Privacy Policy. An independent recipient's role differs from a contracted processor's. No routine investor-family cross-app sharing is authorised.

Helix does not sell personal information or share it for cross-context behavioural advertising under the current policy. We do not sell consumer health/genetic information. Using Firebase is still third-party processing; whether an actual SDK configuration meets California's definitions depends on its use, contract and data flows, not on payment changing hands. Health, genetic, private-message, image and sensitive-trait content must not be sent as analytics payloads. Hashed identifiers remain personal information where linkable.

You may communicate a Do Not Sell or Share or targeted-advertising opt-out to Legal@helixmatchglobal.com and use applicable privacy/cookie controls. We honour legally recognised opt-out preference signals such as Global Privacy Control where applicable; a signal may apply to a browser/device rather than every account unless law requires or we can associate it. No account is required solely to opt out. If a new sale, sharing, targeted advertising or incompatible sensitive-data use is proposed, required notice, choice and consent must precede it. We have no actual knowledge of selling/sharing information of persons under 16; the service prohibits all under-18 accounts.

4 California rights and requests

Subject to applicable law, you may request the categories and specific pieces of personal information, sources, business/commercial purposes, categories of recipients, and relevant sale/sharing disclosures; correct inaccurate information; request deletion; obtain portability; opt out of sale/sharing; and limit sensitive-information use where it falls outside legally permitted purposes. Necessary requested-service use is not general permission to infer traits for advertising. We do not discriminate for exercising rights. Any future lawful incentive requires its own terms, value explanation and voluntary opt-in; no incentive is established here.

Email Legal@helixmatchglobal.com identifying the right and information concerned, or use the in-app applicable request route. We verify access, correction and deletion proportionately, while not demanding identity verification for an opt-out where prohibited. Authorised agents may submit evidence of authority and we may verify the consumer as law permits. We acknowledge applicable California requests within the legally required period, ordinarily 10 business days, and respond to verifiable access/correction/deletion requests within 45 calendar days, with any permitted extension and notice. Opt-out and limitation requests follow their shorter applicable deadlines. We explain a denial and protected information exceptions. No fee applies except a lawful proportionate exception for qualifying excessive or unfounded requests.

California residents may also request applicable direct-marketing disclosure information under California Civil Code section 1798.83. We do not disclose personal information to others for their independent direct marketing under the current policy. This statement does not eliminate any applicable request right. No privacy request waives an injury, consumer or statutory claim.

5 Other US state rights and appeals

Where an applicable state law grants rights, you may confirm processing, access, correct, delete, obtain a portable copy and opt out of sale, targeted advertising or profiling for legally significant decisions. Additional rights may include information about specific third-party recipients, sensitive-data consent, revocation or review of an automated decision, depending on the state. Washington and Nevada consumer health rights are separately described in the Consumer Health Data Notice. Those rights can apply even where a general state privacy law has a threshold or exclusion.

If a request is denied, email Legal@helixmatchglobal.com with the subject Privacy Appeal, identify the request and explain the concern. We respond with reasons within the applicable statutory deadline and tell you how to contact your state Attorney General or other competent regulator if the appeal is denied. An appeal or agent process is not a barrier to urgent or otherwise available rights. Necessary security, other people's rights and legal retention exceptions are applied only as law permits.

6 Updates and contact

The Privacy Policy, visibility schedule, deletion notice and sensitive-feature notices remain part of the information you should review. Contact the company using the details above for category-specific retention information, accessibility assistance, a request or complaint. Material changes to purposes or practices require updated notice and any required consent before the new use. A website notice cannot replace a legally required in-app permission or deletion control.

7 Accuracy of inferred sensitive information

Applicable access, correction, deletion, limitation and review rights can extend to linked inferences as well as information you directly supplied. You may identify a disputed inference and request review without accepting that it is true. We explain any lawful limits and appeal route. A hypothetical child image or inferred trait does not establish a medical condition or biological relationship. No new sale, advertising use, biometric programme or model-training permission is created by this clarification.