

Introduction

Welcome to Perfix. We (“Perfix”, “we”, “us”, or “our”) are committed to protecting the privacy of our users in Israel. This Privacy Policy explains what personal data we collect through the Perfix mobile application and related services (“Service”), how we use and share that data, and the rights you have regarding your information. We adhere to the requirements of the Israeli Protection of Privacy Law, 1981 and its implementing regulations, and we align with international best practices to handle your information lawfully and transparently. By using the Perfix app, you agree to the terms of this Privacy Policy. If you do not agree with any part of this Policy, please discontinue use of the Service.

Data Controller

The Service is operated by Ahmad Haj Yahya (a registered Israeli entity), which is the “data controller” responsible for your personal data. Our personal data database is duly registered with the Israeli Privacy Protection Authority, in accordance with legal requirements. If you have any questions or concerns about this Policy or your data, please contact us at the email provided in the Contact Us section below.

Personal Data We Collect

We collect various categories of personal information from our users (both Customers and service providers) to operate and improve the Service. These include:

Information You Provide Directly

This is information you give us when using Perfix. For example:

- **Account Information (Customers):** When you sign up as a customer seeking services, we collect your full name, email address, and phone number (verified via a one-time passcode SMS). You will choose a password for your account. We also ask for your general location details (such as city) and the specific address where you need the service.
- **Account Information (Service Providers):** If you register as a service provider (professional), we collect your name, email, phone number, and a profile photo. We also ask for professional details such as your business or company name (if applicable), a short bio/description of your services, the service categories you offer, and the cities or regions you serve. To verify your identity and qualifications, we may collect copies of documents you upload – for example, a government-issued ID, professional licenses or certificates, and a few recent invoices or references from the last 3 months. You will set a password for your account (verified via a one-time passcode SMS). All information is provided by you during sign-up and profile setup.
- **Service Request Details:** When a Customer posts a job request through the app, we collect the details of that request. This typically includes a title or description of the task, answers to any service-specific questions (for example, the type of problem,

preferred timing, etc.), the level of urgency, and any media attachments. Customers can upload images or short videos to illustrate the issue or project (for instance, a photo of a leaky pipe or a video of a malfunctioning appliance).

- **Messages and Communications:** If you send messages or correspond with other users through any in-app messaging features (or via integrated channels), those communications may be stored. Likewise, when you contact us for support or inquiries – whether through an in-app contact form, by email, or via our WhatsApp Business chat – we will receive and retain the information you provide (such as your name, email, and the content of your message). Additionally, if the app allows you to leave reviews or ratings (e.g. a customer reviewing a service provider), we collect any feedback you submit.

Information We Collect Automatically

When you use the Perfix app, we automatically gather certain technical and usage data to help us ensure the Service works correctly, maintain security, and improve the user experience. This includes:

- **Device and Usage Data:** We log information about the mobile device and app environment you use. For example, we may collect your device model, operating system version, unique device identifiers, and the interface language you manually select within the app (we record this preference solely to display the Service in your chosen language and do not automatically read your device's system-language setting). We also record usage information such as the screens or pages you view, features you tap or use, the dates and times of your visits, and any errors or crash reports. This information helps us troubleshoot issues and understand how people use the app so we can improve it.
- **Push Notification Tokens:** If you enable push notifications on the Perfix app, our system will generate a unique device token so that we can send notifications to your phone. We keep track of whether you have notifications enabled. We only use these device tokens to send you relevant alerts (for example, a notification that “You received a new quote on your job request” or other important account updates). You can control push notifications in your device or app settings at any time.
- **Location Information (Precise and Approximate):** We use location information to help you complete sign-up and to match Customers with nearby Service Providers. If you grant the app permission, we may collect your precise geolocation (GPS) during sign-up (and when you use location-based features) to suggest or autofill your address and service area. We do not continuously track your location and we do not collect location in the background. If you do not grant permission, you can still enter your address/city manually and we will use that information (or a general/approximate location) for matching and service functionality.

Attribution, Analytics, and App Performance Data: We use analytics, crash reporting, and mobile measurement technologies (such as Google Firebase services and AppsFlyer) to understand how our app is used, measure the effectiveness of our marketing campaigns, detect fraud, and improve reliability. These tools may collect or receive identifiers such as an app-instance ID, AppsFlyer ID, advertising identifiers (for example, Android Advertising ID (GAID) or iOS Advertising Identifier (IDFA), where permitted), IP address, and information

about installs and events within the app (for example, sign-up completion, request creation, and basic in-app actions).

Information from Third-Party Sources

Users (both Customers and service providers) on Perfix can sign up and log in using third-party accounts such as **Google, Facebook, or Apple**. When you choose one of these login methods, we receive the personal information you explicitly authorize the third-party platform to share with us — typically including your **full name, email address, and a unique platform-specific user ID**. We do not receive your password or any sensitive account data from those platforms.

We use **Firebase Authentication** to enable these social login options. This means that your login data is securely handled by **Google Firebase**, and may be stored or processed on servers located in the **United States**. These transfers are protected by **Standard Contractual Clauses (SCCs)** and a **Data Processing Addendum (DPA)** that ensure the data is safeguarded under both Israeli and European privacy standards.

Social login is designed to simplify registration and authentication. Your data from these platforms is used only to create and manage your Perfix account and is not shared with other users unless you explicitly add that information to your public profile. By using social login, you consent to the sharing and processing of this information for the purposes of account creation, login, and account management.

Age Restrictions & Children's Privacy

Perfix is intended for adult users and is not directed to children under 18 years of age. We do not knowingly collect personal information from anyone under 18. If you are under 18, **do not use the Perfix app or submit any personal data to us**. In the event we learn that we have inadvertently collected information from a minor under 18 without appropriate consent, we will promptly delete that data. Parents or guardians who believe their child has provided personal information to Perfix can contact us to request deletion of such data. By using the service, you confirm that you meet the minimum age requirement (see Terms of Use eligibility) or are using the Platform with a parent/guardian's consent and supervision, as allowed by law.

Data Use & Third-Party Services

We use the personal data we collect from you to operate, maintain, and improve the Perfix service in compliance with Israeli privacy law and data protection principles. This includes using your information to create and manage your account, to connect Customers with service providers, to facilitate communications, and to carry out any transactions or actions you request on the Platform. For example, we use the details you provide (such as your service request information and general location) to match you with suitable professionals in your area, and we use provider profile information (skills, qualifications, etc.) to showcase professionals to potential customers. We also process data to send you important notifications about your account activity (e.g. notifying you that you received a new quote or a job status update) and to respond to you when you contact customer support.

WhatsApp Updates and Notifications from Perfix: If you choose to communicate with us or receive service updates via WhatsApp, we may send you transactional messages (for example, verification codes, reminders, updates about your service requests, and customer support responses) using the WhatsApp Business Platform (for example, via Twilio). To do this, we share your phone number and the content of the message with our messaging provider and with WhatsApp/Meta. You can opt out of WhatsApp messages at any time by following the instructions in the message (such as replying “STOP” where applicable) or by contacting us, and we will use alternative channels where available (such as in-app notifications or email).

Communications: We use your contact information (phone number, email) to verify your identity and to enable communication on the Platform. For instance, when you register or log in, we may send a verification code (OTP) via SMS or email to confirm it’s you. When a Customer and service provider agree to a job, we will share the necessary contact details between those two parties to facilitate the service (for example, providing the provider with the customer’s first name, phone number, and service address, and providing the customer with the provider’s name and phone number). We also might use your provided contact info to communicate with you regarding support inquiries – for example, if you reach out via an in-app support chat or via WhatsApp, we will reply through the same channel using the information you provided. We do not use your contact details to send unsolicited marketing messages. Marketing emails or notifications will only be sent to you if you have given opt-in consent, as described below.

WhatsApp Communication with Providers: Perfix may facilitate direct communication between Customers and Service Providers using WhatsApp. In particular, when a Seeker taps the WhatsApp icon by a Provider’s quote, the app will launch WhatsApp on the Seeker’s device and (when supported) prefill a short message referencing the specific service request. The actual conversation then occurs on WhatsApp’s platform. Perfix does not receive or store the contents of user-to-user WhatsApp messages exchanged between Users in these chats.

Providers are permitted to contact a Seeker via WhatsApp only after one of these has occurred: (i) the Seeker has initiated the chat by tapping the icon and sending the first message; or (ii) the Seeker has formally accepted the Provider’s quote; or (iii) The seeker has permitted us to share their contact number with the provider when posting the request. Outside those scenarios, Providers must not contact Seekers via WhatsApp. Please note that WhatsApp may collect metadata (for example, phone numbers, timestamps, and device information) according to its own privacy policy, and Perfix is not involved in and does not control WhatsApp’s data handling for user-to-user chats.

Optional Marketing Communications: From time to time, we may want to send you news, updates, or promotions about Perfix (such as information on new features or special offers). We will only send marketing or promotional communications if you have explicitly consented (opted-in) to receive them. For example, during registration or in your account settings, we might ask if you wish to subscribe to a newsletter or receive deals – this choice is up to you. If you do opt in, you can withdraw your consent at any time. Every marketing email will include an “unsubscribe” link, and app notifications can be turned off. If you opt out or unsubscribe, we will stop sending you promotional messages. *(Please note that even if*

you opt out of marketing, we will still send you essential service-related communications as noted above, since those are necessary for the functionality of the Platform and are not promotional in nature.) We do not share your personal information with third-party companies for their own marketing or advertising purposes without your explicit consent.

Third-Party Service Providers

In providing the Perfix service, we rely on trusted third-party service providers to perform certain functions, and we disclose personal data to them only as needed for those services. For example:

- **Messaging and communications:** We use Twilio (or similar communications providers) to deliver SMS messages and WhatsApp messages, such as one-time passcodes (OTP), reminders, and service updates. This means your phone number and the relevant message content are processed through the provider's systems to reach you.
- **Email delivery:** We may use email delivery providers (for example, SendGrid) to send account or support emails.
- **App infrastructure and authentication:** We use Google Firebase for services such as authentication, push notifications (Firebase Cloud Messaging), and app performance monitoring (for example, crash reporting).
- **Attribution and analytics:** We use AppsFlyer to measure app installs and in-app events that are related to marketing campaign performance and fraud prevention. This may involve processing device identifiers (such as an AppsFlyer ID and, where permitted, an advertising identifier).
- **Location and maps:** We use Google Maps services to help you autofill addresses or display maps for service locations; Google may process the address you input and, if you grant permission, your location to provide map functionality.

These third-party providers only receive the information necessary to perform their functions and are not authorized to use your data for other purposes. We require our service providers to protect personal data and to act consistently with this Policy and applicable law.

Like many mobile apps, Perfix uses SDKs and similar technologies (for example, Firebase and AppsFlyer) to operate the app, measure performance, understand usage, attribute installs, and prevent fraud. These technologies may use identifiers such as an app-instance ID and advertising identifiers (where permitted) and may collect technical information (such as device information and IP address). Where required (for example, iOS App Tracking Transparency), we will request your permission before using advertising identifiers for analytics or attribution, and we provide options to limit such collection as described in this Policy.

Legal Compliance & Data Disclosure

We may use or disclose personal information if required to do so by law or in the good-faith belief that such action is necessary to comply with legal obligations. For example, if we receive a verified request from law enforcement or a court order relating to a user's data, or if it's necessary to investigate or enforce legal rights (including investigation of potential fraud, security issues, or violations of our Terms of Use), we may disclose information to the appropriate authorities or parties. We will ensure any such disclosure is legally permitted and limited to the information required.

Additionally, if Perfix is ever involved in a **merger, acquisition, or sale of assets**, personal data may be transferred to the successor entity as part of that transaction (we will notify users and ensure the new entity honors the protections outlined in this Policy). In all cases, we will only use and share your personal information for the purposes described in this Policy (or closely related purposes that would be reasonably expected), not for unrelated purposes.

Legal Basis for Processing

We process your personal data lawfully, relying on the following legal bases under applicable law (including principles aligned with GDPR where relevant):

- **Performance of a Contract:** Much of our data processing is done so that we can provide you with the service you requested. When you use Perfix, you enter into an agreement to use our Platform, and we must process certain data to fulfill our obligations – for example, using your profile and request details to connect you with service providers, and relaying messages or quotes as part of the service. This contractual necessity covers core functions like account creation, facilitating bookings, and communications between users.
- **Consent:** For any processing that is not strictly necessary for the core service, we will seek your consent. This includes things like sending you marketing emails or push notifications beyond routine service updates, or accessing optional device features (such as your precise location or contacts, if we ever introduce such features). Where consent is required, you have the right to withdraw it at any time, and we will stop the processing. (For instance, you can opt in to our newsletter and later opt out, or grant the app permission to use your location and later revoke it.)
- **Legal Obligation:** We may need to process and retain certain data to comply with our legal obligations. For example, Israeli law might require us to keep records of transactions or communications for a certain period, or to maintain information for tax, accounting, or privacy regulatory purposes. If we receive government requests or need to preserve data due to legal disputes, doing so is based on compliance with law.
- **Legitimate Interests:** We may process data as necessary for Perfix's legitimate interests – in a manner that does not override your rights and freedoms. This can include improving and developing our platform, troubleshooting and fixing bugs, preventing fraud and ensuring security, and sharing minimal data with third-party service providers to operate the service. For instance, analyzing how users navigate the app can help us refine the user experience (done in aggregate, without profiling individuals), and monitoring for suspicious activity helps us keep the platform safe. When we rely on legitimate interests, we balance our interests against your privacy rights, and we limit the processing and implement safeguards to mitigate privacy impact. If you have any questions about the specific legal basis for a particular processing activity, you can contact us for more information.

(Note: As Perfix primarily operates in Israel, our privacy practices are designed to meet the requirements of the Israeli Privacy Protection Law. We also align with international best practices (including GDPR principles) for transparency and user rights. The above legal bases are provided for clarity and to ensure you understand why we collect and use your information.)

Data Retention

We retain your personal data only for as long as necessary to fulfill the purposes outlined in this Policy, or as required by law — particularly under the applicable statutes in Israel. This means we will keep your information as long as you have an account or ongoing service usage, and for a reasonable period thereafter for legitimate business or legal purposes. For instance, we might retain certain transaction records or communications to comply with financial regulations, resolve disputes, enforce our agreements, or satisfy legal obligations. Once personal data is no longer needed for these purposes, we will either delete it or anonymize it so that it can no longer be associated with you.

We also implement the following practices regarding data retention:

- **Account Deletion:** When you delete your account (or request deletion), as described in the User Rights section, we remove your personal data from active databases. Remaining information (if any) will be stored only as required by law and will be disposed of when no longer legally necessary.
- **Backups:** We maintain secure backups of our database for reliability. Deleted personal data will be removed from active systems immediately and will be purged from our backups in the ordinary backup rotation cycle. Backups are automatically cycled and old data is overwritten regularly. We do not access data in backups except for restoration purposes or as required by law.
- **Periodic Review:** We conduct regular reviews of stored data and remove or anonymize any information no longer necessary for our business, legal, or operational needs.

User Rights & Data Deletion

Access and Correction

You have the right to access the personal data we hold about you and to request correction or updates to any information that is inaccurate or outdated. Much of your data is accessible directly by logging into your Perfix account (for example, you can see your profile details, posted jobs, etc.). If you need to change something that is not editable in the app (such as a phone number change that requires re-verification), you can contact us and we will assist in updating your information once we verify the request is legitimate. We want to ensure your data is accurate and up-to-date.

Deletion (Right to be Forgotten)

You have the right to delete your account and personal data. You can exercise this right by using the Delete Account feature in the app settings or by contacting us with a deletion request. Once we receive such a request (and verify it's from you), we will erase or anonymize the personal data we have about you from our active systems, except for data we are required to keep for legal reasons. For example, we may need to retain certain transaction records, communications, or other information to comply with financial reporting laws, to resolve disputes, or to demonstrate compliance with legal obligations. Any retained information will remain subject to the protections of this Privacy Policy and applicable law. We do not keep data indefinitely without purpose; when we no longer have a lawful reason to retain your data, we securely delete it. Even after account deletion, please note that some content you contributed might persist in a manner that does not identify you (for example, a

review you wrote may remain visible but attributed to an anonymous or generic user). We take care to remove personal identifiers from any user-generated content that remains publicly available after your account is deleted. If complete removal of certain content is required by law, we will of course comply with that requirement.

Withdrawal of Consent

Where we rely on your consent for any processing (such as sending marketing communications or using certain optional features), you have the right to withdraw that consent at any time. For example, you can unsubscribe from marketing emails by clicking the “unsubscribe” link, or adjust your app settings to disable marketing notifications or other optional data collections. If you withdraw consent, we will stop the processing that was based on consent. There is no penalty or loss of core service for opting out of marketing – you can continue to use Perfix normally. (However, choosing to disable certain permissions or data uses might affect non-essential features. For instance, if in the future you grant and then revoke location access, you might not be able to use a map-based feature, but you can still manually enter address information.)

Objection and Restriction

Under Israeli law, you have the right to request that we cease using your data for direct marketing purposes, or to object to processing that you believe significantly infringes your privacy or interests. We honor all such valid requests. You also have rights to request that we limit processing in certain cases – for example, if you contest the accuracy of your data, you can ask us to pause processing (other than storage) until we verify and correct the data. While Israeli law does not enumerate all GDPR rights of objection/restriction in the same way, we voluntarily extend similar controls to our users whenever feasible.

Non-Discrimination

We will not discriminate or retaliate against you for exercising any of your data rights. For instance, if you choose to opt out of marketing or request deletion of your data, we will not deny you access to the service (aside from the natural consequence that deletion of your data means we cannot provide certain functionalities). Our service may require some data to function, so if you request deletion of all essential data, we may not be able to continue providing service, but we will inform you if that is the case.

To exercise any of your rights or make inquiries about your data, you can contact us at the email address provided in the **Contact Us** section of this Policy. We will respond in accordance with applicable law. For certain requests, we may need to verify your identity (to protect your privacy and ensure we don’t disclose your data to someone else). We will inform you of the outcome of your request or any action taken as a result.

Account Data upon Termination

If you delete your Perfix account, we handle your data in accordance with this Policy and our Terms of Use. In short, we will remove personal data from active use, and after fulfillment of any legal retention obligations, we will purge or anonymize the data. We maintain secure backups of our database for reliability; when you delete data or your account, that data will

be removed from active systems immediately and then overwritten or purged from backups in the ordinary backup rotation cycle. We do not actively use data from archived backups except if needed for disaster recovery or legal obligations.

User-Generated Content

Please be aware that content you post publicly on Perfix (such as reviews, ratings, or profile information intended to be visible to other users) may remain on the platform even if you deactivate or delete your account. This content is part of the service (for example, your reviews help other users even after you leave). However, if you are no longer a user, we will anonymize your public content – it will not be associated with your full identity. For instance, a review you wrote might display as from “Former User” or simply no longer show your last name or contact info. We will not display any personal contact information that was once part of your profile after your account is deleted. If law requires that certain content be taken down entirely, we will do so. Our goal is to respect your privacy choices while preserving the integrity of information that other users may have relied on. If you have specific concerns about content you posted and how it is handled upon termination, please contact us.

International Data Transfers

To provide our services, we store and process your personal data in secure data centers located in the European Union and may transfer it to trusted service providers outside of your country. Specifically:

- **Data Storage:** Your account data is stored in the **European Union (Germany)** on servers provided by **Amazon Web Services (AWS)**, which offers an **adequate level of protection** under Israeli and European privacy regulations.
- **Communications Services:** We use **Twilio** for SMS, WhatsApp, and email delivery. These communications are processed in the **United States**, protected by **Standard Contractual Clauses (SCCs)** under our **Data Protection Addendum (DPA)** with Twilio. These clauses ensure your data receives a high level of protection even outside the EU.
- **Push Notifications and Maps:** We use **Google Firebase** for push notifications and **Google Maps API** for location-based features. These services may involve transferring certain data to the **United States**, also protected by **SCCs** under our **Google Cloud Data-Processing Addendum**, which we accepted on **May 16, 2025**.

Attribution and analytics: We use AppsFlyer for attribution and measurement. Depending on how the AppsFlyer SDK is configured and where its service providers operate, data may be processed in Israel, the European Union, the United States, and other jurisdictions. Where required, we rely on contractual safeguards (such as Data Processing Addenda and Standard Contractual Clauses) to protect international transfers.

- **Additional Safeguards:** We implement industry-standard security measures, including encryption at rest and in transit, to protect your data during these transfers.
- **User Rights:** You have the right to request access to, correction of, or deletion of your data, as well as to object to or restrict certain processing. To exercise these rights, please contact us at support@perfixapp.com.

Third-Party Links and Integrations

The Perfix app may include links or integrations to third-party services that are not operated by us. For example, we provide an option in the app to contact our support via a WhatsApp chat. This means that if you tap the WhatsApp support link in Perfix, your WhatsApp application will open, and the conversation will take place on WhatsApp's platform.

Additionally, we may include other external services in the future, such as payment processing systems, location verification tools, or links to external resources for customer support.

Please be aware that any information you share with third-party services is governed by their own privacy policies and terms, not by Perfix's Privacy Policy. For example, if you use WhatsApp to chat with a service provider or with our support team, WhatsApp may collect metadata about the conversation (such as your phone number, the fact that you contacted our number, etc.) under their terms. We do not control how WhatsApp or any other external service uses your data. We recommend reviewing the privacy policies of those third-party services before engaging with them.

That said, we will not intentionally share your personal data with third-party platforms without your action. We only facilitate the connection (like opening WhatsApp on your device at your request). We do not send WhatsApp any data from our side except what is necessary to start the chat (and that is handled by your own WhatsApp app).

In Summary:

Whenever you leave the Perfix app or send information through an external service, that service's privacy practices apply. We encourage you to be cautious about sharing sensitive information via channels that we don't control. If you have any questions about which features involve third parties, feel free to ask us. We are happy to clarify what is internal to our system and what goes external.

Data Security

We take the security of your personal data very seriously and implement a range of technical and organizational measures to safeguard it. While no system can be 100% secure, we follow industry standards and Israeli legal requirements (such as the Privacy Protection (Data Security) Regulations, 2017) to protect your information from unauthorized access, alteration, disclosure, or destruction. Our security measures include:

- **Encryption:** We utilize encryption protocols to protect data in transit. For example, information exchanged between the app and our servers is encrypted via HTTPS. Where applicable, we also employ encryption at rest for sensitive information.
- **Access Controls:** We restrict access to personal data to authorized personnel who have a need to know that information for their job duties. All staff with access to personal data are subject to confidentiality obligations and receive training on data protection best practices.
- **Secure Storage:** Our databases and servers are secured in controlled environments with strong firewall protection and other safeguards. We use reputable cloud

providers (such as AWS in the EU region) that maintain robust security certifications and compliance standards.

- **Monitoring and Testing:** We monitor our systems for potential vulnerabilities and attacks, and we perform regular security assessments (including penetration testing and code reviews) to identify and fix potential weaknesses.
- **Incident Response:** We have an incident response plan in place to handle any suspected data breach or security incident. In the unlikely event of a data breach affecting user information, we will notify affected users and regulators as required by law and take all necessary steps to mitigate the issue.

Our security program is designed to meet the standards set by Israeli regulations for data security. For instance, the law categorizes databases by their risk and sensitivity levels and mandates certain measures accordingly (like maintaining access logs and an incident response plan). We constantly update and improve our security measures to meet or exceed industry standards and to adapt to new threats. Protecting your data is one of our top priorities, and we invest appropriate resources and expertise to do so. If you have specific questions about our security practices, feel free to contact us – we can share more details as appropriate (within the bounds of not exposing sensitive security information).

Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technologies, legal requirements, or for other operational reasons. If we make material changes to how we handle your personal data, we will notify you through appropriate channels. For example, we might display a notice within the app, send an email to our users, or provide an alert upon your next login, informing you of what's changing. The “Last Updated” date at the top of this Policy will always indicate when the latest changes were made.

Whenever we update the Policy, the new version will be posted and will be effective as of the stated date. In some cases, if required by law or if the changes materially affect your rights or obligations, we might request your consent to the updated terms. Otherwise, your continued use of the Perfix Service after the effective date of the updated Policy will constitute your acceptance of those changes. We encourage you to review this Privacy Policy periodically to stay informed about how we are protecting and using your information. If you do not agree with any updates to the Policy, you should stop using the app. You may also delete your account if you wish. Of course, you can always contact us if you have specific concerns.

Contact Us

If you have any questions, concerns, or requests regarding this Privacy Policy or your personal data, please feel free to contact us. We are here to help and address any issues you might have about your privacy.

Privacy Contact Email: support@perfixapp.com

You can reach out to us via email for matters such as: asking about your personal data, making a rights request (access, correction, deletion, etc.), reporting a security issue, or to inquire more about our privacy practices. We will respond as promptly as we can.

Additionally, if you prefer or if required, you may contact us by mail. Our business mailing address is:

Ahmad Haj Yahya
Rehov Haifa, Tayibe, 4040000, Israel

(Note: The above address will be updated with our official registered business address once available. Email is the fastest way to reach us for privacy matters.)

By communicating with us, we may keep a record of the correspondence to help resolve your inquiry and for our records. We will use any information provided in your request (including your contact info) only to address your request and for necessary follow-up.