PRIVACY POLICY

Last updated: November 28, 2024

This Privacy Policy for **GROUP-IB GLOBAL PRIVATE LIMITED** (**“Group-IB”,** "**we**," "**us**," or "**our**"), describes how and why we might collect, store, use, and/or share ("**process**") your information when you download and use our application(s), such as our mobile application — Group-IB Unified Risk Platform (**“Group-IB URP”**) or any other application of ours that links to this Privacy Policy (“**Application**”).

We know that data privacy is a top issue today, and we want you to enjoy your interaction with the Application whilst knowing that we value your information and that we protect it.

We take data security extremely seriously and are committed to processing it responsibly and in compliance with applicable data protection laws.

We use a variety of measures to keep your data confidential and secure, including restricting access to your data on a need-to-know basis and ensuring appropriate technical, legal and organizational safeguards to protect your data.

If you have any requests concerning your information we process as well as any questions or comments regarding this Privacy Policy and processing practices, please email us at privacy@group-ib.com.

By using the Application, you agree to this Privacy Policy. If you do not agree with our policies and practices, please refrain from using our Application.

This Privacy Policy is available both in the Application settings section and on the application store page of the application.

1. INFORMATION WE COLLECT

Personal information you disclose to us

We collect personal information that you voluntarily provide to us when you use the Application, express an interest in obtaining information about us or our products and services, or otherwise when you contact us.

Information that you share with us directly. The personal information we collect depends on the context of your interactions with us and the Application, the choices you make, and the products and features you use. The personal information we collect may include the following:

- **Email address.** Retrieved from your existing Group-IB account via the Single Sign-On (SSO) process. No additional registration occurs within the Application. We also process your email address to validate who you are if you need to recover your account or your account has been compromised, and also to notify you about your account vulnerability, e.g. suspicious logins or other unusual activity that could be related to a compromise of your Application account or one of your accounts in other resources that integrate with the Application.
- **Identity information.** Retrieved from your existing Group-IB account via the Single Sign-On (SSO) process. During registration of the Application account, you may provide us your real name. If we have detected any suspicious activities on your side or have a reasonable doubt about whether you are the rightful account holder of the Application account associated with your email address, we may ask you for a copy of your physical identification such as a passport or a national ID, drivers’ license or any similar document which we then use to confirm your claim to the account.

Sensitive information. We do not process sensitive information.

Data we collect automatically. We collect information specified in this section to ensure that we deliver the most optimized version of the Application for your device and to detect suspicious and/or fraudulent activity. The information we collect automatically may include the following:

- **Device Data.** When you download and open the Application, we automatically collect information about the type of device you have downloaded the app on and your device identifier.
- **Location data.** We collect location information based on your IP address or, where applicable, from your device's location services, if enabled.
- **Login history and Application account history.** When you use the Application to log into a resource account, we collect and process information associated with your login activity including your IP address, what resource you logged in to, fact that you logged in, time of your session.
- **Results of your biometric data check.** We don't receive any biometric data from your device itself but binary information on whether you passed the check or not. All biometric data (fingerprint scan, face recognition etc.) are autonomously processed on your device.

We only request access to data necessary to perform the core functions of the Application. Access to additional data, such as Contacts or Location, is requested only when necessary for specific features, and you may decline such access.

By accepting this Privacy Policy you acknowledge and agree that Group-IB will share your personal data with resources to which accounts you connect the Application, including data on suspicious activities we detect, for the purpose of ensuring the highest cyber-security level possible and keeping you safe from potential fraudulent activities. We conclude special data processing agreements (DPA) governing mutual obligations in respect of your personal data processing with all resources.

Application data. If you use our Application, we may automatically collect and transmit the following data about your device, network connection, and other relevant information during a user session to ensure the highest level of cybersecurity:

- **Custom values/attributes**: Anonymized user identifier, optional data block connected to anonymized user identifier, session identifier in the user's personal account, custom key-value combination (attribute).
- **Information to identify the user's browser and device**: IP address, User-Agent, Accept-Encoding, Accept-Language, Parameters of the device screen, Time zone, CPU, Package name (Android app specific), Bundle Id (iOS app specific), Mobile subscriber identifier (Android app specific), Unique mobile device identifier (IMEI) (Android app specific), Mobile operator identifier, Mobile operator name, Mobile operator country, SIM card serial number (Android app specific), SIM card country (Android app specific), SIM card mobile operator identifier (Android app specific), SIM card mobile operator name (Android app specific), SIM card status (Android app specific), Software version (Android app specific), Group identifier for GSM networks (Android app specific), Mobile device hardware identifier (Android app specific), URL of the MMS agent (Android app specific), MMS agent (Android app specific), Mobile phone type (Android app specific), Flag for data exchange availability (Android app specific), Flag for roaming mode (Android app specific), Flag for ICC card availability (Android app specific), Application package name for receiving SMS messages (Android app specific), Mobile phone model and manufacturer (Android app specific), Motherboard model of the mobile device (Android app specific), Bootloader of the mobile device (Android app specific), Brand of the mobile device (Android app specific), Name of the mobile device (Android app specific), Displayed name of the mobile device (Android app specific), Mobile device fingerprint (Android app specific), Mobile device chip name (Android app specific), Mobile device host (Android app specific), Mobile device identifier (Android app specific), Product name (Android app specific), Mobile device radio chip identifier (Android app specific), Manufacturer of the accelerometer chip (Android app specific), Accelerometer name (Android

app specific), Mobile device serial number (Android app specific), ANDROID_ID value (Android app specific), Integral accelerometer measurement (Android app specific), Technology for data transfer (iOS app specific), Flaf for VoIP support (iOS app specific), Wi-Fi MAC address, Wi-Fi network SSID, Information about the first installed applications, List of installed applications (iOS app specific).

- **Information about device location:** Identifiers of the cell tower to which the device is connected (iOS app specific), Device coordinates based on the device's GPS/Glonass module, Device coordinates based on network connection, Wi-Fi access points identifiers.
- **Information about device:** Device battery (iOS app specific), Installed keyboards (iOS app specific), Audio data (iOS app specific), Proxy/VPN data (iOS app specific), Data about active calls (iOS app specific), Data about user authentication mode for this device (iOS app specific), Data about device (iOS app specific).
- **Signs Of Compromised User Device:** Description of certificates and packages signed by them (apps installed on the device) (Android app specific), Flag for viewing the device screen via remote access tools.
- **Information About User Behavior:** User activity in the protected app, Data from device sensors

Mobile Device Access. We may request access to certain features on your mobile device, such as Bluetooth, calendar, camera, and other functionalities. If you wish to change these access permissions, you can adjust them in your device's settings.

Push Notifications. We may request to send you push notifications regarding your account or features of the Application. You can opt-out of receiving these notifications by adjusting your device's settings.

This information is primarily needed to maintain the security and operation of our Application, for troubleshooting, and for our internal analytics and reporting purposes.

All personal information that you provide to us must be true, complete, and accurate, and you must notify us of any changes to such personal information.

2. HOW WE PROCESS YOUR INFORMATION

We process your personal information for various reasons, depending on how you interact with our Application. These include:

- **To facilitate account authentication and manage user accounts.** We process your information to verify your identity, enable secure access to your account via the Single Sign-On (SSO) process, and ensure your account remains functional. This may also include using biometric data, where applicable, processed locally on your device.
- **To deliver services and facilitate their use.** We process your personal information to provide you with the services and features you request through the Application, including real-time threat alerts and updates from the Group-IB Threat Intelligence.
- **To respond to user inquiries and provide support.** We may process your personal information to respond to any questions, requests, or concerns you have, and to resolve any issues related to the use of our services and/or Application.
- **To send administrative information.** We process your personal information to send you important updates about the Application, including notifications about changes to our terms, policies, and other service-related information.
- **To request feedback.** We may process your personal information when necessary to request feedback regarding your experience with the Application.
- **For marketing and promotional purposes.** With your consent or in accordance with your marketing preferences, we may process your personal information to send you promotional communications,

including updates about our products and services. ou can opt out of receiving marketing emails from us at any time by clicking the unsubscribe link included in the emails or by contacting us directly.

- **To ensure the security and integrity of the Application.** We process your personal information as part of our ongoing efforts to protect the Application, including monitoring for fraud and suspicious activity, identifying potential security threats, and preventing unauthorized access.
- **To analyze usage trends and improve our services.** We may process your information to better understand how users interact with the Application, allowing us to enhance its performance, usability, and features based on real-time usage data.
- **To evaluate the effectiveness of marketing and promotional campaigns.** We may process your personal information to assess the impact and relevance of our marketing initiatives. This enables us to tailor future communications and promotions to better suit your preferences and interests.

3. PURPOSES AND THE LEGAL GROUND OF DATA PROCESSING

The law requires us to explain the valid legal bases on which we rely to process your personal information. Depending on the specific context in which we collect and process your data, we may rely on one or more of the following legal bases:

- **Performance of a contract.** We may process your personal information when we believe it is necessary to fulfill our contractual obligations to you. This includes providing access to our Application, services, or products, and taking any other steps at your request.
- **Legitimate interests.** We may process your information when we believe it is reasonably necessary to achieve our legitimate business interests, provided that such interests are not overridden by your fundamental rights and freedoms. For example, we may process your personal information for some of the purposes described in order to:
    - Send you notifications about updates, special offers, discounts, or promotions on our products and services.
    - Develop, improve, and display personalized and relevant content within the Application, tailored to your preferences.
    - Analyze usage trends and performance data to improve the Application's functionality, user engagement, and overall experience.
    - Support our marketing activities, including market research and targeted advertising.
    - Identify, prevent, and address technical issues, security threats, and fraudulent activity that could compromise user accounts or our services.
    - Understand how users engage with our products and services, so we can refine and enhance their experience.

  When we rely on legitimate interests, we ensure that we make it clear to you either in this Privacy Policy or at the point of data collection what those interests are. If we transfer your personal information to third parties for processing, such transfers are governed by legally binding Data Processing Agreements (DPAs) to protect your personal data.
- **Legal obligations.** We may process your personal information when it is required to comply with legal obligations, including obligations to regulatory authorities, law enforcement, or courts. This also applies when we must protect our legal rights, respond to official requests, or comply with legal processes (e.g. litigation, etc.).

4. WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION

We may share your personal information with third parties under the circumstances described below. We ensure that any such sharing is done in compliance with applicable laws and with appropriate safeguards in place to protect your privacy. All third parties with whom we share data are required to provide the same or equivalent level of data protection as outlined in our Privacy Policy.

- **Service Providers, Consultants, and Other Third Parties.** We may share your data with vendors, contractors, service providers, or agents ("third parties") who perform services for us or on our behalf and require access to such information to perform their work. These third parties may include entities providing cloud services, analytics, payment processing, order fulfillment, marketing, customer support, and website hosting services. Importantly:
  - They are subject to Data Processing Agreements (DPAs) and confidentiality obligations.
  - They may only process personal information in accordance with our instructions and cannot use it for their own purposes, including marketing.
  - We do not permit them to sell, rent, or disclose your personal information for purposes outside the services they provide to us.
  - They are required to implement appropriate security measures to protect your data and retain it only for as long as necessary.
- **Business Transfers.** We may share or transfer your information in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business by another company. In such cases, we will notify you if your personal information becomes subject to a different Privacy Policy.
- **Affiliates.** We may share your information with our affiliates, including subsidiaries, joint ventures, or other companies under common control. All such affiliates are required to adhere to this Privacy Policy and implement appropriate security measures.
- **Business Partners.** We may share your information with our business partners to offer you certain products, services, or promotions. Our business partners are contractually obligated to use your data only for the purposes specified by us and in line with the legal requirements.
- **Legal Requests and Law Enforcement.** We may disclose your personal information:
  - In response to subpoenas, court orders, or other legal processes.
  - To comply with legal obligations or regulatory requirements.
  - When we believe in good faith that disclosure is necessary to protect our rights, prevent fraud, or ensure the safety of you or others.
- **Cross-Border Data Transfers.** Your personal information may be transferred to and processed in countries outside of your jurisdiction, including to service providers located outside the European Economic Area (EEA). When we transfer your personal data outside the EEA or other regions with comprehensive data protection laws, we ensure that appropriate safeguards, such as Standard Contractual Clauses (SCCs), are in place to protect your information in accordance with applicable data protection laws.

5. HOW LONG DO WE KEEP YOUR INFORMATION?

We retain your personal information only for as long as necessary to fulfill the purposes described in this Privacy Policy or as required by law. The length of time we keep your information depends on the type of data and the purpose for which it was collected. This includes retention to comply with legal obligations (e.g., tax, accounting, or other regulatory requirements), resolve disputes, and enforce our agreements.

- **Account data.** We retain your personal information as long as your account is active. If you deactivate or delete your account, we will retain your information only for as long as required by law or for legitimate business purposes.
- **Billing data.** We retain billing and payment information for as long as legally required, or as needed for legitimate business purposes such as maintaining financial records and fulfilling audit obligations.
- **Operational and product data.** Data necessary for the operation and improvement of our services, such as usage information, bug reports, and feedback, is retained only for as long as necessary.
- **Backup and archive data.** In some cases, your personal information may be stored in backup archives. This data will be securely stored and isolated from further use until deletion is possible.

Once we no longer need to retain your personal information for ongoing business or legal reasons, we will delete, anonymize, or de-identify the data. If immediate deletion is not possible (e.g., due to backup systems), we will securely store and isolate the data until deletion is feasible.

In some cases, we may retain aggregated or de-identified data indefinitely for statistical or business planning purposes, as this information is no longer considered personal data under applicable data protection laws.

6. HOW DO WE KEEP YOUR INFORMATION SAFE

We implement appropriate physical, technical, and organizational measures to protect your personal information from unauthorized access, disclosure, alteration, or destruction. These include encryption, access controls, and regular security monitoring.

However, please note that no method of data transmission over the Internet or electronic storage is completely secure, and we cannot guarantee absolute security. While we strive to protect your personal data, transmission of information to and from our Services is at your own risk. We recommend that you take precautions such as using strong passwords and accessing our Services in a secure environment.

If you have questions about the security of your personal data, please contact us at privacy@group-ib.com.

7. WHAT ARE YOUR PRIVACY RIGHTS

You have the following rights regarding the processing of your personal data, subject to applicable data protection laws:

- **Right to Information.** You have the right to receive clear and transparent information about how we process your personal data. This information is provided in this Privacy Policy.
- **Right of Access.** You can request access to the personal data we hold about you, including a copy of your data, and obtain information on how it is processed.
- **Right to Rectification.** If your personal data is inaccurate or incomplete, you have the right to request that we correct or update it.
- **Right to Erasure ("Right to be Forgotten").** You have the right to request the deletion of your personal data under specific circumstances, such as when the data is no longer necessary for the purposes for which it was collected, or if you have withdrawn your consent and there is no other legal ground for processing. Note: Account creation and management are not conducted within the Application. To delete your account, please contact us directly via: erasure@group-ib.com.
- **Right to Object.** You have the right to object to the processing of your personal data in certain circumstances, particularly where the processing is based on legitimate interests and we have no overriding legal grounds to continue such processing.

- **Right to Restriction of Processing.** You can request that we restrict the processing of your personal data under certain conditions, such as if you contest the accuracy of the data, if the processing is unlawful, or if we no longer need the data but you require it for legal claims.
- **Right to Lodge a Complaint. I**f you believe we have infringed your rights or misused your personal data, you have the right to lodge a complaint with a data protection authority in your country of residence.

Opting Out of Marketing and Promotional Communications. You can unsubscribe from our marketing and promotional communications at any time by:

- Clicking the unsubscribe link in any marketing email we send you,
- Or contacting us directly.

Please note that even if you opt out of marketing communications, you may still receive administrative messages necessary for your account management or other service-related communications.

Account Information. If you would like to review, update, or delete the information in your account, or terminate your account, you can do so by by contacting us at: erasure@group-ib.com.

Upon your request to delete or terminate your account, we will deactivate your account and remove your personal data from active systems. However, we may retain certain data to:

- Prevent fraud or abuse,
- Comply with legal obligations,
- Resolve disputes,
- Or enforce our agreements.

8. CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy from time to time to reflect changes in our practices, legal requirements, or other operational reasons. Each updated version will be identified by an "Updated" or "Revised" date, and the changes will take effect as soon as the updated Privacy Policy is accessible. We encourage you to regularly review this Privacy Policy to stay informed about how we protect your personal information.

9. MISCELLANEOUS

Language. Non-English translations of this Privacy Policy are provided for convenience only. In the event of any ambiguity or conflict between translations, the English version shall prevail.

10.CONTACT INFORMATION

GROUP-IB GLOBAL PRIVATE LIMITED

Our business address is: 138634, Singapore, 2 Fusionopolis Way, #15-04

privacy@group ib.com