Privacy Policy of The Global Risks Alliance (GRA)

Welcome to the privacy policy of The Global Risks Alliance (GRA). This policy will help you understand what data we collect, why we collect it, and what your rights are in relation to it.

Latest update: May 08, 2026

Table of contents

Owner and Data Controller

The Global Risks Alliance

Owner contact email: contact@theglobalriskalliance.com

Type of Data we collect

Among the types of Personal Data that The Global Risks Alliance (GRA) collects, by itself or through third parties, there are:

- first name
- last name
- gender
- date of birth
- phone number
- VAT Number
- company name
- profession
- physical address
- fax number
- country
- state
- county
- email address
- ZIP/Postal code
- various types of Data
- city
- Tax ID
- field of activity
- User ID
- number of employees
- website
- Trackers
- Usage Data
- unique device identifiers for advertising (Google Advertiser ID or IDFA, for example)
- username
- Universally unique identifier (UUID)
- general activity data
- body measurements & indexes
- movement activity

- food related activity
- sleeping activity
- heart rate and other vital data
- blood type
- payment info
- geographic position
- Full access
- Read only access
- Read metadata
- Modify
- Insert and import
- Compose
- Basic settings management
- Sensitive settings management
- budget
- academic background
- billing address
- picture
- answers to questions
- clicks
- keypress events
- motion sensor events
- mouse movements
- scroll position
- touch events
- Data communicated while using the service
- profile picture
- screenshots
- workplace
- purchase history
- shipping address
- number of Users
- session statistics
- device information
- Data communicated in order to use the Service
- IP address
- Calendar permission
- Contacts permission
- Camera permission
- Precise location permission (continuous)
- Precise location permission (non-continuous)
- Approximate location permission (continuous)
- Approximate location permission (non-continuous)
- Microphone permission
- Phone permission
- Sensors permission
- SMS permission
- Storage permission
- Reminders permission
- HomeKit permission
- Motion sensors permission
- Bluetooth sharing permission
- Social media accounts permission
- Microphone permission, without recording
- NFC Reader permission
- Biometric Data access permission
- Media Library permission (Music)
- Photo Library permission
- Health Data read permission
- Health Data update permission
- Siri permission
- Apple's speech recognition servers permission
- TV Provider permission
- Google Assistant permission
- Google Home permission
- Call permission
- Camera permission, without saving or recording
- Write-only Photo Library permission

- name
- marital status
- social media accounts
- language
- user content
- contact info
- password
- Social Security number (SSN)
- house number
- prefix
- data relating to the point of sale
- Twitter handle
- order ID
- referral URL
- page views
- province
- latitude (of city)
- longitude (of city)
- metro area
- geography/region
- app information
- device logs
- operating systems
- browser information
- launches
- number of sessions
- session duration
- scroll-to-page interactions
- video views
- browsing history
- search history
- interaction events
- page events
- custom events
- Application opens

Complete details on each type of Personal Data collected are provided in the dedicated sections of this privacy policy or by specific explanation texts displayed prior to the Data collection.
Personal Data may be freely provided by the User, or, in case of Usage Data, collected automatically when using The Global Risks Alliance (GRA).
Unless specified otherwise, all Data requested by The Global Risks Alliance (GRA) is mandatory and failure to provide this Data may make it impossible for The Global Risks Alliance (GRA) to provide its services. In cases where The Global Risks Alliance (GRA) specifically states that some Data is not mandatory, Users are free not to communicate this Data without consequences to the availability or the functioning of the Service.
Users who are uncertain about which Personal Data is mandatory are welcome to contact the Owner.
Any use of Cookies – or of other tracking tools — by The Global Risks Alliance (GRA) or by the owners of third-party services used by The Global Risks Alliance (GRA) serves the purpose of providing the Service required by the User, in addition to any other purposes described in the present document and in the Cookie Policy.

Users are responsible for any third-party Personal Data obtained, published or shared through The Global Risks Alliance (GRA).

Mode and place of processing the Data

Methods of processing

The Owner takes appropriate security measures to prevent unauthorized access, disclosure, modification, or unauthorized destruction of the Data.
The Data processing is carried out using computers and/or IT enabled tools, following organizational procedures and modes strictly related to the purposes indicated. In addition to the Owner, in some cases, the Data may be accessible to certain types of persons in charge, involved with the operation of The Global Risks Alliance (GRA) (administration, sales, marketing, legal, system administration) or external parties (such as third-party technical service providers, mail carriers, hosting providers, IT companies, communications agencies) appointed, if necessary, as Data Processors by the Owner. The updated list of these parties may be requested from the Owner at any time.

Place

The Data is processed at the Owner's operating offices and in any other places where the parties involved in the processing are located.

Depending on the User's location, data transfers may involve transferring the User's Data to a country other than their own. To find out more about the place of processing of such transferred Data, Users can check the section containing details about the processing of Personal Data.

Retention time

Unless specified otherwise in this document, Personal Data shall be processed and stored for as long as required by the purpose they have been collected for and may be retained for longer due to applicable legal obligation or based on the Users' consent.

The purposes of processing

The Data concerning the User is collected to allow the Owner to provide its Service, comply with its legal obligations, respond to enforcement requests, protect its rights and interests (or those of its Users or third parties), detect any malicious or fraudulent activity, as well as the following:

- Contacting the User
- Displaying content from external platforms
- Analytics
- Content commenting
- Data transfer outside the EU
- Handling activity data
- Handling payments
- Hosting and backend infrastructure
- Infrastructure monitoring
- Interaction with external social networks and platforms
- Location-based interactions
- Platform services and hosting
- Registration and authentication
- Registration and authentication provided directly by The Global Risks Alliance (GRA)
- Remarketing and behavioral targeting
- Social features
- Spam and bots protection
- Tag management
- Handling activities related to productivity
- Data transfer outside of the UK
- Collection of privacy-related preferences
- Device permissions for Personal Data access
- Managing contacts and sending messages
- Managing data collection and online surveys
- Building and running The Global Risks Alliance (GRA)
- Advertising
- Traffic optimization and distribution

Detailed information on the processing of Personal Data

Advertising

This type of service allows User Data to be utilized for advertising communication purposes. These communications are displayed in the form of banners and other advertisements on The Global Risks Alliance (GRA), possibly based on User interests. This does not mean that all Personal Data are used for this purpose. Information and conditions of use are shown below.
Some of the services listed below may use Trackers to identify Users or they may use the behavioral retargeting technique, i.e. displaying ads tailored to the User's interests and behavior, including those detected outside The Global Risks Alliance (GRA). For more information, please check the privacy policies of the relevant services.
Services of this kind usually allow Users to opt out of such tracking. Users may learn how to opt out of interest-based advertising more generally by visiting the relevant opt-out section in this document.

▶

Jetpack

Company: Jetpack Digital LLC

Place of processing: United States

Personal Data processed: Trackers +1

Analytics

The services contained in this section enable the Owner to monitor and analyze web traffic and can be used to keep track of User behavior.

▶

Google Analytics Demographics and Interests reports

Company: Google LLC +1

Place of processing: United States +1

Personal Data processed: Trackers +1

▶

WordPress Stats

Company: Automattic Inc. +1

Place of processing: United States +1

Personal Data processed: Trackers +1

▶

Yandex Metrica

Company: YANDEX, LLC

Place of processing: Russian Federation

Personal Data processed: Trackers +1

▶

Business Contact

Company: Italiaonline S.p.A.

Place of processing: Italy

Personal Data processed: Trackers +1

▶

Google Analytics 4

Company: Google LLC +1

Place of processing: United States +1

Personal Data processed: number of Users +3

▶

YouTube Analytics and Reporting API

Company: Google LLC +1

Place of processing: United States +1

Personal Data processed: Data communicated in order to use the Service +6

▶

WooCommerce Order Attribution Tracking

Company: The Global Risks Alliance (GRA)

Personal Data processed: page views +3

Building and running The Global Risks Alliance (GRA)

Key components of The Global Risks Alliance (GRA) are built and run directly by the Owner by making use of the software listed below.

▶

WordPress (self-hosted)

Company: The Global Risks Alliance (GRA)

Personal Data processed: billing address +26

▶

Ghost with User subscriptions

Personal Data processed: email address

Collection of privacy-related preferences

This type of service allows The Global Risks Alliance (GRA) to collect and store Users' preferences related to the collection, use, and processing of their personal information, as requested by the applicable privacy legislation.

▶

iubenda Privacy Controls and Cookie Solution

Company: iubenda srl

Place of processing: Italy

Personal Data processed: IP address +1

Contacting the User

▶

Contact form

Company: The Global Risks Alliance (GRA)

Personal Data processed: city +23

▶

Phone contact

Personal Data processed: phone number

▶

Mailing list or newsletter

Personal Data processed: city +16

Content commenting

Content commenting services allow Users to make and publish their comments on the contents of The Global Risks Alliance (GRA).
Depending on the settings chosen by the Owner, Users may also leave anonymous comments. If there is an email address among the Personal Data provided by the User, it may be used to send notifications of comments on the same content. Users are responsible for the content of their own comments.
If a content commenting service provided by third parties is installed, it may still collect web traffic data for the pages where the comment service is installed, even when Users do not use the content commenting service.

▶

Comment system managed directly

Personal Data processed: email address +7

Device permissions for Personal Data access

The Global Risks Alliance (GRA) requests certain permissions from Users that allow it to access the User's device Data as described below.

▶

Device permissions for Personal Data access

Personal Data processed: Apple's speech recognition servers permission +31

Displaying content from external platforms

This type of service allows you to view content hosted on external platforms directly from the pages of The Global Risks Alliance (GRA) and interact with them. Such services are often referred to as widgets, which are small elements placed on a website or app. They provide specific information or perform a particular function and often allow for user interaction.
This type of service might still collect web traffic data for the pages where the service is installed, even when Users do not use it.

▶

Google Fonts

Company: Google LLC +1

Place of processing: United States +1

Personal Data processed: Trackers +1

▶

GitHub button and social widgets

Company: GitHub Inc.

Place of processing: United States

Personal Data processed: Usage Data

▶

Google Maps widget

Company: Google LLC +1

Place of processing: United States +1

Personal Data processed: Trackers +1

▶

Gravatar

Company: Automattic Inc. +1

Place of processing: United States +1

Personal Data processed: email address +1

▶

Instagram widget

Company: Meta Platforms, Inc. +1

Place of processing: United States +1

Personal Data processed: Trackers +1

▶

Vimeo video

Company: Vimeo, LLC

Place of processing: United States

Personal Data processed: Trackers +1

▶

YouTube video widget

Company: Google LLC +1

Place of processing: United States +1

Personal Data processed: Trackers +1

▶

YouTube video widget (Privacy Enhanced Mode)

Company: Google LLC +1

Place of processing: United States +1

Personal Data processed: Trackers +2

▶

Google Programmable Search Engine

Company: Google LLC +1

Place of processing: United States +1

Personal Data processed: Trackers +1

▶

Adobe Fonts

Company: Adobe Systems Incorporated

Place of processing: United States

Personal Data processed: Usage Data +1

▶

YouTube IFrame Player

Company: Google LLC +1

Place of processing: United States +1

Personal Data processed: Data communicated in order to use the Service +6

▶

Google Calendar widget

Company: Google LLC +1

Place of processing: United States +1

Personal Data processed: Trackers +1

▶

SoundCloud widget

Company: SoundCloud Limited

Place of processing: Germany

Personal Data processed: Usage Data

▶

YouTube Data API

Company: Google LLC +1

Place of processing: United States +1

Personal Data processed: Data communicated in order to use the Service +6

▶

Font Awesome

Company: Fonticons, Inc.

Place of processing: United States

Personal Data processed: Trackers +1

Handling activities related to productivity

This type of service helps the Owner to manage tasks, collaboration and, in general, activities related to productivity. In using this type of service, Data of Users will be processed and may be retained, depending on the purpose of the activity in question.
These services may be integrated with a wide range of third-party services disclosed within this privacy policy to enable the Owner to import or export Data needed for the relative activity.

▶

Gmail

Company: Google LLC +1

Place of processing: United States +1

Personal Data processed: city +19

Handling activity data

This type of service allows the Owner to use the activity or biometric data collected by your device in order for The Global Risks Alliance (GRA) to operate or to provide specific features. This may include movements, heartbeat, change in altitude or data about the surroundings.
Depending on what is described below, third parties may be involved in the activity tracking.
Most devices allow for the User to control which Data is accessed or stored.

▶

Activity data tracked by your device

Personal Data processed: blood type +8

Handling payments

Unless otherwise specified, The Global Risks Alliance (GRA) processes any payments by credit card, bank transfer or other means via external payment service providers. In general and unless where otherwise stated, Users are requested to provide their payment details and personal information directly to such payment service providers. The Global Risks Alliance (GRA) isn't involved in the collection and processing of such information: instead, it will only receive a notification by the relevant payment service provider as to whether payment has been successfully completed.

▶

Payment by bank transfer

Company: The Global Risks Alliance (GRA)

Personal Data processed: company name +4

▶

PayPal

Company: PayPal Inc.

Place of processing: See the PayPal privacy policy

Personal Data processed: various types of Data as specified in the privacy policy of the service

▶

Stripe

Company: Stripe, Inc. +2

Place of processing: United States +2

Personal Data processed: various types of Data as specified in the privacy policy of the service

▶

Apple Pay

Company: Apple Inc.

Place of processing: United States

Personal Data processed: billing address +10

Hosting and backend infrastructure

This type of service has the purpose of hosting Data and files that enable The Global Risks Alliance (GRA) to run and be distributed or to provide a ready-made infrastructure to run specific features or parts of The Global Risks Alliance (GRA).

Some services among those listed below, if any, may work through geographically distributed servers, making it difficult to determine the actual location where the Personal Data are stored.

▶

GitHub Pages

Company: GitHub Inc.

Place of processing: United States

Personal Data processed: various types of Data as specified in the privacy policy of the service

Infrastructure monitoring

This type of service allows The Global Risks Alliance (GRA) to monitor the use and behavior of its components so its performance, operation, maintenance and troubleshooting can be improved.
Which Personal Data are processed depends on the characteristics and mode of implementation of these services, whose function is to filter the activities of The Global Risks Alliance (GRA).

▶

Pingdom

Company: Pingdom AB

Place of processing: Sweden

Personal Data processed: Trackers +1

Interaction with external social networks and platforms

This type of service allows interaction with social networks or other external platforms directly from the pages of The Global Risks Alliance (GRA).
The interaction and information obtained through The Global Risks Alliance (GRA) are always subject to the User's privacy settings for each social network.
This type of service might still collect traffic data for the pages where the service is installed, even when Users do not use it.
It is recommended to log out from the respective services in order to make sure that the processed data on The Global Risks Alliance (GRA) isn't being connected back to the User's profile.

▶

YouTube button and social widgets

Company: Google LLC +1

Place of processing: United States +1

Personal Data processed: Usage Data

▶

PayPal button and widgets

Company: PayPal Inc.

Place of processing: See the PayPal privacy policy

Personal Data processed: Trackers +1

▶

Reddit button and widgets

Company: reddit inc.

Place of processing: United States

Personal Data processed: Trackers +1

▶

Pinterest "Pin it" button and social widgets

Company: Pinterest, Inc.

Place of processing: United States

Personal Data processed: Trackers +1

Location-based interactions

▶

Geolocation

Personal Data processed: geographic position

Managing contacts and sending messages

This type of service makes it possible to manage a database of email contacts, phone contacts or any other contact information to communicate with the User.
These services may also collect data concerning the date and time when the message was viewed by the User, as well as when the User interacted with it, such as by clicking on links included in the message.

▶

Mailchimp

Company: Intuit Inc.

Place of processing: United States

Personal Data processed: company name +13

Managing data collection and online surveys

This type of service allows The Global Risks Alliance (GRA) to manage the creation, deployment, administration, distribution and analysis of online forms and surveys in order to collect, save and reuse Data from any responding Users.
The Personal Data collected depend on the information asked and provided by the Users in the corresponding online form.

These services may be integrated with a wide range of third-party services to enable the Owner to take subsequent steps with the Data processed - e.g. managing contacts, sending messages, analytics, advertising and payment processing.

▶

Data provided via online forms, managed directly

Company: The Global Risks Alliance (GRA)

Personal Data processed: answers to questions +23

▶

Elementor Form Widget

Personal Data processed: Data communicated while using the service

Platform services and hosting

These services have the purpose of hosting and running key components of The Global Risks Alliance (GRA), therefore allowing the provision of The Global Risks Alliance (GRA) from within a unified platform. Such platforms provide a wide range of tools to the Owner – e.g. analytics, user registration, commenting, database management, e-commerce, payment processing – that imply the collection and handling of Personal Data.

Some of these services work through geographically distributed servers, making it difficult to determine the actual location where the Personal Data are stored.

WordPress.com

Company: Automattic Inc. +1

Place of processing: United States +1

Personal Data processed: various types of Data as specified in the privacy policy of the service

WooCommerce

Company: The Global Risks Alliance (GRA)

Personal Data processed: billing address +11

Registration and authentication

By registering or authenticating, Users allow The Global Risks Alliance (GRA) to identify them and give them access to dedicated services.
Depending on what is described below, third parties may provide registration and authentication services. In this case, The Global Risks Alliance (GRA) will be able to access some Data, stored by these third-party services, for registration or identification purposes.
Some of the services listed below may also collect Personal Data for targeting and profiling purposes; to find out more, please refer to the description of each service.

YouTube OAuth

Company: Google LLC +1

Place of processing: United States +1

Personal Data processed: various types of Data as specified in the privacy policy of the service

GitHub OAuth

Company: GitHub Inc.

Place of processing: United States

Personal Data processed: various types of Data as specified in the privacy policy of the service

Google OAuth

Company: Google LLC +1

Place of processing: United States +1

Personal Data processed: various types of Data as specified in the privacy policy of the service

Gmail permissions to access User Data (OAuth addition)

Company: Google LLC +1

Place of processing: United States +1

Personal Data processed: Basic settings management +7

WordPress.com Single Sign On

Company: Automattic Inc. +1

Place of processing: United States +1

Personal Data processed: Trackers +1

Twitch.tv Authentication

Company: Twitch Interactive, Inc.

Place of processing: United States

Personal Data processed: various types of Data as specified in the privacy policy of the service

Direct registration and profiling

Company: The Global Risks Alliance (GRA)

Personal Data processed: billing address +38

Registration and authentication provided directly by The Global Risks Alliance (GRA)

By registering or authenticating, Users allow The Global Risks Alliance (GRA) to identify them and give them access to dedicated services. The Personal Data is collected and stored for registration or identification purposes only. The Data collected are only those necessary for the provision of the service requested by the Users.

Direct registration

Personal Data processed: academic background +9

Remarketing and behavioral targeting

This type of service allows The Global Risks Alliance (GRA) and its partners to inform, optimize and serve advertising based on past use of The Global Risks Alliance (GRA) by the User.
This activity is facilitated by tracking Usage Data and by using Trackers to collect information which is then transferred to the partners that manage the remarketing and behavioral targeting activity.
Some services offer a remarketing option based on email address lists.
Services of this kind usually allow Users to opt out of such tracking. Users may learn how to opt out of interest-based advertising more generally by visiting the relevant opt-out section in this document.

▶

Remarketing with Google Analytics

Company: Google LLC +1

Place of processing: United States +1

Personal Data processed: Trackers +1

▶

Google Ads Remarketing

Company: Google LLC +1

Place of processing: United States +1

Personal Data processed: Trackers +1

Social features

▶

Public profile

Personal Data processed: city +15

Spam and bots protection

This type of service analyzes the traffic of The Global Risks Alliance (GRA), potentially containing Users' Personal Data, with the purpose of filtering it from unwanted parts of traffic, messages and content that are recognized as spam or protecting it from malicious bots activities.

▶

Akismet

Company: Automattic Inc. +1

Place of processing: United States +1

Personal Data processed: Usage Data

Google reCAPTCHA

Company: Google LLC +1

Place of processing: United States +1

Personal Data processed: answers to questions +8

Cloudflare Bot Management

Personal Data processed: app information +37

Tag management

This type of service helps the Owner to manage the tags or scripts needed on The Global Risks Alliance (GRA) in a centralized fashion.
This results in the Users' Data flowing through these services, potentially resulting in the retention of this Data.

Google Tag Manager

Company: Google LLC +1

Place of processing: United States +1

Personal Data processed: Usage Data

Traffic optimization and distribution

This type of service allows The Global Risks Alliance (GRA) to distribute their content using servers located across different countries and to optimize their performance.
Which Personal Data are processed depends on the characteristics and the way these services are implemented. Their function is to filter communications between The Global Risks Alliance (GRA) and the User's browser.
Considering the widespread distribution of this system, it is difficult to determine the locations to which the contents that may contain Personal Information of the User are transferred.

Cloudflare

Personal Data processed: various types of Data as specified in the privacy policy of the service

Information on opting out of interest-based advertising

In addition to any opt-out feature provided by any of the services listed in this document, Users may learn more on how to generally opt out of interest-based advertising within the dedicated section of the Cookie Policy.

Further information about the processing of Personal Data

Analysis and predictions based on the User’s Data (“profiling”)

The Owner may use the Personal and Usage Data collected through The Global Risks Alliance (GRA) to create or update User profiles. This type of Data processing allows the Owner to evaluate User choices, preferences and behaviour for the purposes outlined in the respective section of this document. User profiles can also be created through the use of automated tools like algorithms, which can also be provided by third parties. To find out more about the profiling activities performed, Users can check the relevant sections of this document. The User always has a right to object to this kind of profiling activity. To find out more about the User's rights and how to exercise them, the User is invited to consult the section of this document outlining the rights of the User.

Automated decision-making

Automated decision-making means that a decision which is likely to have legal effects or similarly significant effects on Users, is taken solely by technological means, without any human intervention. The Global Risks Alliance (GRA) may use the Users' Personal Data to make decisions entirely or partially based on automated processes according to the purposes outlined in this document. The Global Risks Alliance (GRA) adopts automated decision-making processes as far as necessary to enter into or perform a contract between Users and Owner, or on the basis of the Users' explicit consent, where such consent is required by the law. Automated decisions are made by technological means – mostly based on algorithms subject to predefined criteria – which may also be provided by third parties. The rationale behind automated decision-making is:

to enable or otherwise improve the decision-making process; to grant Users fair and unbiased treatment based on consistent and uniform criteria; to reduce the potential harm derived from human error, personal bias and the like which may potentially lead to discrimination or imbalance in the treatment of individuals etc.; to reduce the risk of Users' failure to meet their obligation under a contract. To find out more about the purposes, the third-party services, if any, and any specific rationale for automated decisions used within The Global Risks Alliance (GRA), Users can check the relevant sections in this document. Consequences of automated decision-making processes for Users and rights of Users subjected to it

As a consequence, Users subject to such processing, are entitled to exercise specific rights aimed at preventing or otherwise limiting the potential effects of the automated decisions taken. In particular, Users have the right to:

obtain an explanation about any decision taken as a result of automated decision-making and express their point of view regarding this decision; challenge a decision by asking the Owner to reconsider it or take a new decision on a different basis; request and obtain from the Owner human intervention on such processing.

To learn more about the Users' rights and the means to exercise them, Users are invited to consult the section of this document relating to the rights of Users.

Personal Data collected through sources other than the User

The Owner of The Global Risks Alliance (GRA) may have legitimately collected Personal Data relating to Users without their knowledge by reusing or sourcing them from third parties on the grounds mentioned in the section specifying the legal basis of processing. Where the Owner has collected Personal Data in such a manner, Users may find specific information regarding the source within the relevant sections of this document or by contacting the Owner.

Push notifications

The Global Risks Alliance (GRA) may send push notifications to the User to achieve the purposes outlined in this privacy policy.

Users may in most cases opt-out of receiving push notifications by visiting their device settings, such as the notification settings for mobile phones, and then change those settings for The Global Risks Alliance (GRA), some or all of the apps on the particular device. Users must be aware that disabling push notifications may negatively affect the utility of The Global Risks Alliance (GRA).

Push notifications based on the User's geographic location

The Global Risks Alliance (GRA) may use the User's geographic location to send push notifications for the purposes outlined in this privacy policy.

Users may in most cases opt-out of receiving push notifications by visiting their device settings, such as the notification settings for mobile phones, and then changing those settings for some or all of the apps on the particular device.

Users must be aware that disabling push notifications may negatively affect the utility of The Global Risks Alliance (GRA).

Push notifications for direct marketing

The Global Risks Alliance (GRA) may send push notifications to the User for the purpose of direct marketing (to propose services and products provided by third parties or unrelated to the product or service provided by The Global Risks Alliance (GRA)).

Users may in most cases opt-out of receiving push notifications by visiting their device settings, such as the notification settings for mobile phones, and then changing those settings for The Global Risks Alliance (GRA) or all of the apps on the particular device.

Users must be aware that disabling push notifications may negatively affect the utility of The Global Risks Alliance (GRA).

Besides applicable device settings, the User may also make use of the rights described under User rights in the relevant section of this privacy policy.

Selling goods and services online

The Personal Data collected are used to provide the User with services or to sell goods, including payment and possible delivery. The Personal Data collected to complete the payment may include the credit card, the bank account used for the transfer, or any other means of payment envisaged. The kind of Data collected by The Global Risks Alliance (GRA) depends on the payment system used.

User identification via a universally unique identifier (UUID)

The Global Risks Alliance (GRA) may track Users by storing a so-called universally unique identifier (or short UUID) for analytics purposes or for storing Users' preferences. This identifier is generated upon installation of this Application, it persists between Application launches and updates, but it is lost when the User deletes the Application. A reinstall generates a new UUID.

Preference Cookies

Preference Cookies store the User preferences detected on The Global Risks Alliance (GRA) in the local domain such as, for example, their timezone and region.

Pseudonymous use

When registering for The Global Risks Alliance (GRA), Users have the option to indicate a nickname or pseudonym. In this case, Users' Personal Data shall not be published or made publicly available. Any activity performed by Users on The Global Risks Alliance (GRA) shall appear in connection with the indicated nickname or pseudonym. However, Users acknowledge and accept that their activity on The Global Risks Alliance (GRA), including content, information or any other material possibly uploaded or shared on a voluntary and intentional basis may directly or indirectly reveal their identity.

Browser Fingerprinting

Browser Fingerprinting creates an identifier based on a device's unique combination of characteristics (e.g. IP address, HTTP header, browser properties etc.), that allows to distinguish the User from other Users, thereby enabling to track the User's browsing behavior across the web. Browser Fingerprinting does not have an expiration date and cannot be deleted.

Equal protection of User Data

The Global Risks Alliance (GRA) shares User Data only with third parties carefully selected to ensure that they provide the same or equal protection of User Data as stated in this privacy policy and requested by applicable data protection laws. Further information on data processing and privacy practices by third parties can be found in their respective privacy policies.

localStorage

localStorage allows The Global Risks Alliance (GRA) to store and access data right in the User's browser with no expiration date.

Rights for registered California Users under the age of 18

California's "Online Eraser" law, part of California's Business and Professions Code Sections 22580-22582, requires operators of certain websites and online services targeting minors to allow registered Users who are under the age of 18 and residents of California to request removal of content they post.

If a registered User fits that description and posted content on The Global Risks Alliance (GRA), they may request removal of such content by contacting the Owner or its privacy policy coordinator at the contact details provided in this document.

In response to this request, the Owner may make content posted by the registered User invisible to other registered Users and the public (rather than deleting it entirely), in which case the content may remain on the Owner's servers. It may also be publicly available elsewhere if a third party copied and reposted this content.

sessionStorage

sessionStorage allows The Global Risks Alliance (GRA) to store and access data right in the User's browser. Data in sessionStorage is deleted automatically when the session ends (in other words, when the browser tab is closed).

Unique device identification

The Global Risks Alliance (GRA) may track Users by storing a unique identifier of their device, for analytics purposes or for storing Users' preferences.

Access the address book

The Global Risks Alliance (GRA) may request access to your address book.

Cookie Policy

The Global Risks Alliance (GRA) uses Trackers. To learn more, Users may consult the Cookie Policy.

Further Information for Users in the European Union

Legal basis of processing

The Owner may process Personal Data relating to Users if one of the following applies:

- Users have given their consent for one or more specific purposes.
- provision of Data is necessary for the performance of an agreement with the User and/or for any pre-contractual obligations thereof;
- processing is necessary for compliance with a legal obligation to which the Owner is subject;
- processing is related to a task that is carried out in the public interest or in the exercise of official authority vested in the Owner;
- processing is necessary for the purposes of the legitimate interests pursued by the Owner or by a third party.

In any case, the Owner will gladly help to clarify the specific legal basis that applies to the processing, and in particular whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract.

Further information about retention time

Unless specified otherwise in this document, Personal Data shall be processed and stored for as long as required by the purpose they have been collected for and may be retained for longer due to applicable legal obligation or based on the Users’ consent.

Therefore:

- Personal Data collected for purposes related to the performance of a contract between the Owner and the User shall be retained until such contract has been fully performed.
- Personal Data collected for the purposes of the Owner’s legitimate interests shall be retained as long as needed to fulfill such purposes. Users may find specific information regarding the legitimate interests pursued by the Owner within the relevant sections of this document or by contacting the Owner.

The Owner may be allowed to retain Personal Data for a longer period whenever the User has given consent to such processing, as long as such consent is not withdrawn. Furthermore, the Owner may be obliged to retain Personal Data for a longer period whenever required to fulfil a legal obligation or upon order of an authority.

Once the retention period expires, Personal Data shall be deleted. Therefore, the right of access, the right to erasure, the right to rectification and the right to data portability cannot be enforced after expiration of the retention period.

The rights of Users based on the General Data Protection Regulation (GDPR)

Users may exercise certain rights regarding their Data processed by the Owner.

In particular, Users have the right to do the following, to the extent permitted by law:

- **Withdraw their consent at any time.** Users have the right to withdraw consent where they have previously given their consent to the processing of their Personal Data.
- **Object to processing of their Data.** Users have the right to object to the processing of their Data if the processing is carried out on a legal basis other than consent.
- **Access their Data.** Users have the right to learn if Data is being processed by the Owner, obtain disclosure regarding certain aspects of the processing and obtain a copy of the Data undergoing processing.
- **Verify and seek rectification.** Users have the right to verify the accuracy of their Data and ask for it to be updated or corrected.
- **Restrict the processing of their Data.** Users have the right to restrict the processing of their Data. In this case, the Owner will not process their Data for any purpose other than storing it.
- **Have their Personal Data deleted or otherwise removed.** Users have the right to obtain the erasure of their Data from the Owner.
- **Receive their Data and have it transferred to another controller.** Users have the right to receive their Data in a structured, commonly used and machine readable format and, if technically feasible, to have it transmitted to another controller without any hindrance.
- **Lodge a complaint.** Users have the right to bring a claim before their competent data protection authority.

Users are also entitled to learn about the legal basis for Data transfers abroad including to any international organization governed by public international law or set up by two or more countries, such as the UN, and about the security measures taken by the Owner to safeguard their Data.

Details about the right to object to processing

Where Personal Data is processed for a public interest, in the exercise of an official authority vested in the Owner or for the purposes of the legitimate interests pursued by the Owner, Users may object to such processing by providing a ground related to their particular situation to justify the objection.

Users must know that, however, should their Personal Data be processed for direct marketing purposes, they can object to that processing at any time, free of charge and without providing any justification. Where the User objects to processing for direct marketing purposes, the Personal Data will no longer be processed for such purposes. To learn whether the Owner is processing Personal Data for direct marketing purposes, Users may refer to the relevant sections of this document.

How to exercise these rights

Any requests to exercise User rights can be directed to the Owner through the contact details provided in this document. Such requests are free of charge and will be answered by the Owner as early as possible and always within one month, providing Users with the information required by law. Any rectification or erasure of Personal Data or restriction of processing will be communicated by the Owner to each recipient, if any, to whom the Personal Data has been disclosed unless this proves impossible or involves disproportionate effort. At the Users' request, the Owner will inform them about those recipients.

Transfer of Personal Data outside of the European Union

Data transfer abroad based on consent

If this is the condition for Data transfer, Personal Data of Users shall be transferred from the EU to third countries only if the User has explicitly consented to such transfer, after having been informed of the possible risks due to the absence of an adequacy decision and appropriate safeguards. In such cases, the Owner shall inform Users appropriately and collect their explicit consent via The Global Risks Alliance (GRA).

Data transfer abroad based on standard contractual clauses

If this is the condition for Data transfer, the transfer of Personal Data from the EU to third countries is carried out by the Owner according to "standard contractual clauses" provided by the European Commission. This means that Data recipients have committed to process Personal Data in compliance with the data protection standards set forth by EU data protection legislation. For further information, Users are requested to contact the Owner through the contact details provided in the present document.

Data transfer to countries that guarantee European standards

If this is the condition for Data transfer, the transfer of Personal Data from the EU to third countries is carried out according to an adequacy decision of the European Commission. The European Commission adopts adequacy decisions for specific countries whenever it considers that country to possess and provide Personal Data protection standards comparable to those set forth by EU data protection legislation. Users can find an updated list of all adequacy decisions issued on the European Commission's website.

Other legal basis for Data transfer abroad

If no other condition for Data transfer applies, Personal Data shall be transferred from the EU to third countries only if at least one of the following is met:

the transfer is necessary for the performance of a contract between the User and the Owner or of pre-contractual measures taken at the User's request; the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the User between the Owner and another natural or legal person; the transfer is necessary for important reasons of public interest; the transfer is necessary for establishment, exercise or defence of legal claims; the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; the data transferred is sourced from a public register created under the law of the country that the data originates from; subject to further conditions, the Owner has a compelling legitimate interest to perform a one-off transfer of Personal Data.

In such cases, the Owner shall inform the User about the condition the transfer is based on via The Global Risks Alliance (GRA).

Transfer of Personal Data outside of the United Kingdom

Data transfer abroad based on consent (UK)

If this is the condition for Data transfer, Personal Data of Users shall be transferred from the UK to third countries only if the User has explicitly consented to such transfer, after having been informed of the possible risks due to the absence of an adequacy decision and appropriate safeguards.

In such cases, the Owner shall inform Users appropriately and collect their explicit consent via The Global Risks Alliance (GRA).

Data transfer abroad based on standard contractual clauses (UK)

If this is the condition for Data transfer, the transfer of Personal Data from the UK to third countries is carried out by the Owner according to "standard contractual clauses" provided by the European Commission.

This means that Data recipients have committed to process Personal Data in compliance with the data protection standards set forth by EU data protection legislation, which are recognized as valid also under UK law. For further information, Users are requested to contact the Owner through the contact details provided in the present document.

Data transfers according to a UK adequacy regulation

If this is the condition for Data transfer, the transfer of Personal Data from the UK to third countries may take place according to a so called "adequacy regulation" of the UK Government.

The UK Government adopts adequacy regulations for specific countries or territories whenever such countries or territories guarantee Personal Data protection standards comparable to those set forth by UK data protection legislation. Users can find an updated list of all adequacy regulations on the website of the Information Commissioner's Office (ICO).

Other legal basis for Data transfer abroad (UK)

If no other condition for Data transfer applies, Personal Data shall be transferred from the UK to third countries only if at least one of the following is met:

the transfer is necessary for the performance of a contract between the User and the Owner or of pre-contractual measures taken at the User's request; the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the User between the Owner and another natural or legal person; the transfer is necessary for important reasons of public interest; the transfer is necessary for establishment, exercise or defence of legal claims; the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; the data transferred is sourced from a public register created under UK law; subject to further conditions, the Owner has a compelling legitimate interest to perform a one-off transfer of Personal Data.

In such cases, the Owner shall inform the User about the condition the transfer is based on via The Global Risks Alliance (GRA).

Further information for Users in Switzerland

This section applies to Users in Switzerland, and, for such Users, supersedes any other possibly divergent or conflicting information contained in the privacy policy.

Further details regarding the categories of Data processed, the purposes of processing, the categories of recipients of the personal data, if any, the retention period and further information about Personal Data can be found in **the section titled "Detailed information on the processing of Personal Data" within this document**.

The rights of Users according to the Swiss Federal Act on Data Protection

Users may exercise certain rights regarding their Data within the limits of law, including the following:

- right of access to Personal Data;
- right to object to the processing of their Personal Data (which also allows Users to demand that processing of Personal Data be restricted, Personal Data be deleted or destroyed, specific disclosures of Personal Data to third parties be prohibited);
- right to receive their Personal Data and have it transferred to another controller (data portability);
- right to ask for incorrect Personal Data to be corrected.

How to exercise these rights

Any requests to exercise User rights can be directed to the Owner through the contact details provided in this document. Such requests are free of charge and will be answered by the Owner as early as possible, providing Users with the information required by law.

Further information for Users in Brazil

This section of the document integrates with and supplements the information contained in the rest of the privacy policy and is provided by the entity running The Global Risks Alliance (GRA) and, if the case may be, its parent, subsidiaries and affiliates (for the purposes of this section referred to collectively as “we”, “us”, “our”).
This section applies to all Users in Brazil (Users are referred to below, simply as “you”, “your”, “yours”), according to the "Lei Geral de Proteção de Dados" (the "LGPD"), and for such Users, it supersedes any other possibly divergent or conflicting information contained in the privacy policy.
This part of the document uses the term “personal information“ as it is defined in the **LGPD**.

The grounds on which we process your personal information

We can process your personal information solely if we have a legal basis for such processing. Legal bases are as follows:

- your consent to the relevant processing activities;
- compliance with a legal or regulatory obligation that lies with us;
- the carrying out of public policies provided in laws or regulations or based on contracts, agreements and similar legal instruments;
- studies conducted by research entities, preferably carried out on anonymized personal information;
- the carrying out of a contract and its preliminary procedures, in cases where you are a party to said contract;
- the exercising of our rights in judicial, administrative or arbitration procedures;
- protection or physical safety of yourself or a third party;
- the protection of health – in procedures carried out by health entities or professionals;
- our legitimate interests, provided that your fundamental rights and liberties do not prevail over such interests; and
- credit protection.

To find out more about the legal bases, you can contact us at any time using the contact details provided in this document.

Categories of personal information processed

To find out what categories of your personal information are processed, you can read the section titled “Detailed information on the processing of Personal Data” within this document.

Why we process your personal information

To find out why we process your personal information, you can read the sections titled “Detailed information on the processing of Personal Data” and “The purposes of processing” within this document.

Your Brazilian privacy rights, how to file a request and our response to your requests

Your Brazilian privacy rights

You have the right to:

- obtain confirmation of the existence of processing activities on your personal information;
- access to your personal information;
- have incomplete, inaccurate or outdated personal information rectified;
- obtain the anonymization, blocking or elimination of your unnecessary or excessive personal information, or of information that is not being processed in compliance with the LGPD;
- obtain information on the possibility to provide or deny your consent and the consequences thereof;
- obtain information about the third parties with whom we share your personal information;

- obtain, upon your express request, the portability of your personal information (except for anonymized information) to another service or product provider, provided that our commercial and industrial secrets are safeguarded;
- obtain the deletion of your personal information being processed if the processing was based upon your consent, unless one or more exceptions provided for in art. 16 of the LGPD apply;
- revoke your consent at any time;
- lodge a complaint related to your personal information with the ANPD (the National Data Protection Authority) or with consumer protection bodies;
- oppose a processing activity in cases where the processing is not carried out in compliance with the provisions of the law;
- request clear and adequate information regarding the criteria and procedures used for an automated decision; and
- request the review of decisions made solely on the basis of the automated processing of your personal information, which affect your interests. These include decisions to define your personal, professional, consumer and credit profile, or aspects of your personality.

You will never be discriminated against, or otherwise suffer any sort of detriment, if you exercise your rights.

How to file your request

You can file your express request to exercise your rights free from any charge, at any time, by using the contact details provided in this document, or via your legal representative.

How and when we will respond to your request

We will strive to promptly respond to your requests.
In any case, should it be impossible for us to do so, we'll make sure to communicate to you the factual or legal reasons that prevent us from immediately, or otherwise ever, complying with your requests. In cases where we are not processing your personal information, we will indicate to you the physical or legal person to whom you should address your requests, if we are in the position to do so.

In the event that you file an **access** or personal information **processing confirmation** request, please make sure that you specify whether you'd like your personal information to be delivered in electronic or printed form.
You will also need to let us know whether you want us to answer your request immediately, in which case we will answer in a simplified fashion, or if you need a complete disclosure instead.
In the latter case, we'll respond within 15 days from the time of your request, providing you with all the information on the origin of your personal information, confirmation on whether or not records exist, any criteria used for the processing and the purposes of the processing, while safeguarding our commercial and industrial secrets.

In the event that you file a **rectification, deletion, anonymization or personal information blocking** request, we will make sure to immediately communicate your request to other parties with whom we have shared your personal information in order to enable such third parties to also comply with your request — except in cases where such communication is proven impossible or involves disproportionate effort on our side.

Transfer of personal information outside of Brazil permitted by the law

We are allowed to transfer your personal information outside of the Brazilian territory in the following cases:

- when the transfer is necessary for international legal cooperation between public intelligence, investigation and prosecution bodies, according to the legal means provided by the international law;
- when the transfer is necessary to protect your life or physical security or those of a third party;
- when the transfer is authorized by the ANPD;
- when the transfer results from a commitment undertaken in an international cooperation agreement;
- when the transfer is necessary for the execution of a public policy or legal attribution of public service;
- when the transfer is necessary for compliance with a legal or regulatory obligation, the carrying out of a contract or preliminary procedures related to a contract, or the regular exercise of rights in judicial, administrative or arbitration procedures.

Additional information for Users in Brazil

Transfer of personal information outside of Brazil based on contracts and other legal means

We can transfer your personal information outside of the Brazilian territory provided that we are able to ensure that any further processing of your personal information will be in compliance with the principles and the rules established by the LGPD, and your rights are safeguarded.

To do so, we may use one of the following legal means:

specific contractual clauses for each given transfer. This means that we will enter into an agreement with the recipient of your personal information to make sure that such transfers meet the requirements explained above. Such an agreement shall be subject

to the ANPD's prior verification; standard contractual clauses. These clauses set terms and conditions for the transfer of personal information and are adopted by the ANPD; global corporate clauses. These clauses set terms and conditions for the transfer of personal information within an organisation and, before they come into force, are subject to the ANPD's prior verification; seals of approval, certificates and codes of conduct regularly issued by the ANPD. These legal instruments allow us to transfer your personal information provided that we abide by their rules. They are subject to the previous approval of the ANPD.

Transfer of personal information outside of Brazil based on your consent

We can transfer your personal information outside of the Brazilian territory if you consent to such transfer. When we ask for your consent, we'll make sure to provide all the information that you need to make an educated decision and to understand the implications and consequences of providing or denying your consent. Such information will be given in clear and plain language and in such a way that you'll be able to clearly distinguish these requests from other consent requests that we may possibly ask. **You may withdraw your consent at any time**.

Transfer of personal information outside of Brazil to countries that guarantee the same protection standards as LGPD

We can transfer your personal information outside of the Brazilian territory, if the destination country, or the international organization which receives the personal information, provides an adequate level of protection of the personal information according to the ANPD. The ANPD authorizes such transfers whenever it considers that country to possess and provide personal information protection standards comparable to those set forth by the LGPD, having taken into account the following:

the general and sectoral rules of the legislation in force in the country of destination or in the international organization; the nature of the personal information subject to the transfer; the compliance with the general principles on the protection of the personal information and on the rights of the individuals as set forth in the LGPD; the adoption of suitable security measures; the existence of judicial and institutional guarantees for the respect of personal information protection rights; and any other pertinent circumstance related to the relevant transfer.

Further information for Users in the United States

This part of the document integrates with and supplements the information contained in the rest of the privacy policy and is provided by the business running The Global Risks Alliance (GRA) and, if the case may be, its parent, subsidiaries and affiliates (for the purposes of this section referred to collectively as "we", "us", "our").
The information contained in this section applies to all Users (Users are referred to below, simply as "you", "your", "yours"), who are residents in the following states: **California, Virginia, Colorado, Connecticut, Utah, Texas, Oregon, Nevada, Delaware, Iowa, New Hampshire, New Jersey, Nebraska, Tennessee, Minnesota, Maryland, Indiana, Kentucky, Rhode Island and Montana.**
For such Users, this information supersedes any other possibly divergent or conflicting provisions contained in the privacy policy.
This part of the document uses the term Personal Information (and Sensitive Personal Information).

Notice at collection

The following Notice at collection provides you with timely notice about the **categories of Personal Information collected or disclosed in the past 12 months** so that you can exercise meaningful control over our use of that Information.
While such categorization of Personal Information is mainly based on California privacy laws, it can also be helpful for anyone who is not a California resident to get a general idea of what types of Personal Information are collected.

Identifiers

Sold or Shared

Targeted Advertising

Personal Data processed: First name; Last name; Gender; Date of birth + 111

Personal Information collected or disclosed:

- first name
- last name
- gender
- date of birth
- phone number
- company name
- profession
- physical address
- fax number
- country
- state

- county
- email address
- ZIP/Postal code
- various types of Data
- city
- field of activity
- User ID
- number of employees
- website
- Trackers
- Usage Data
- unique device identifiers for advertising (Google Advertiser ID or IDFA, for example)
- Universally unique identifier (UUID)
- various types of Data as specified in the privacy policy of the service
- general activity data
- food related activity
- Full access
- Read only access
- Read metadata
- Modify
- Insert and import
- Compose
- Basic settings management
- Sensitive settings management
- budget
- academic background
- billing address
- geographic position
- picture
- profile picture
- screenshots
- workplace
- Data communicated while using the service
- purchase history
- shipping address
- device information
- Data communicated in order to use the Service
- Calendar permission
- Contacts permission
- Camera permission
- Approximate location permission (continuous)
- Approximate location permission (non-continuous)
- Microphone permission
- Phone permission
- Sensors permission
- SMS permission
- Storage permission
- Reminders permission
- HomeKit permission
- Motion sensors permission
- Bluetooth sharing permission
- Social media accounts permission
- Microphone permission, without recording
- NFC Reader permission
- Media Library permission (Music)
- Photo Library permission
- Siri permission
- Apple's speech recognition servers permission
- TV Provider permission
- Google Assistant permission
- Google Home permission
- Call permission
- Camera permission, without saving or recording
- Write-only Photo Library permission
- answers to questions
- name
- social media accounts
- language

- user content
- contact info
- house number
- prefix
- data relating to the point of sale
- Twitter handle
- order ID
- province
- latitude (of city)
- longitude (of city)
- metro area
- geography/region
- IP address
- app information
- device logs
- operating systems
- browser information
- launches
- number of sessions
- session duration
- scroll-to-page interactions
- mouse movements
- scroll position
- keypress events
- motion sensor events
- touch events
- video views
- clicks
- browsing history
- search history
- session statistics
- page views
- interaction events
- page events
- custom events
- Application opens

Sensitive Personal Information collected or disclosed VAT Number, Tax ID, username, body measurements & indexes, movement activity, sleeping activity, heart rate and other vital data, blood type, payment info, Precise location permission (continuous), Precise location permission (non-continuous), Biometric Data access permission, Health Data read permission, Health Data update permission , marital status, password, Social Security number (SSN)

Purposes:

- Contacting the User
- Analytics
- Content commenting
- Data transfer outside the EU
- Displaying content from external platforms
- Further information about Personal Data
- Handling activity data
- Handling payments
- Hosting and backend infrastructure
- Platform services and hosting
- Registration and authentication
- Registration and authentication provided directly by The Global Risks Alliance (GRA)
- Social features
- Handling activities related to productivity
- Data transfer outside of the UK
- Device permissions for Personal Data access
- Managing contacts and sending messages
- Managing data collection and online surveys
- Building and running The Global Risks Alliance (GRA)
- Traffic optimization and distribution
- Spam and bots protection

Retention period: for the time necessary to fulfill the purpose

Sold or Shared: Yes

Targeted Advertising: Yes

Third-parties: Google LLC, Automattic Inc., GitHub Inc., Adobe Systems Incorporated, PayPal Inc., Stripe, Inc., Apple Inc., Twitch Interactive, Inc., The Global Risks Alliance (GRA), Intuit Inc.

Service providers or contractors: The Global Risks Alliance (GRA)

Commercial information

Sold or Shared

Targeted Advertising

Personal Data processed: First name; Last name; Gender; Date of birth + 42

Personal Information collected or disclosed:

- first name
- last name
- gender
- date of birth
- phone number
- company name
- profession
- physical address
- fax number
- country
- state
- county
- email address
- ZIP/Postal code
- various types of Data
- city
- field of activity
- User ID
- number of employees
- website
- Trackers
- Usage Data
- budget
- academic background
- billing address
- geographic position
- picture
- profile picture
- screenshots
- workplace
- Data communicated while using the service
- various types of Data as specified in the privacy policy of the service
- purchase history
- shipping address
- answers to questions
- name
- social media accounts
- language
- user content
- contact info
- house number
- prefix
- data relating to the point of sale
- Twitter handle
- order ID
- device information

Sensitive Personal Information collected or disclosed VAT Number, Tax ID, payment info, username, marital status, password, Social Security number (SSN)

Purposes:

- Contacting the User
- Handling payments
- Registration and authentication provided directly by The Global Risks Alliance (GRA)
- Social features
- Handling activities related to productivity
- Managing contacts and sending messages
- Managing data collection and online surveys
- Registration and authentication
- Platform services and hosting
- Building and running The Global Risks Alliance (GRA)

Retention period: for the time necessary to fulfill the purpose

Sold or Shared: Yes

Targeted Advertising: Yes

Third-parties: Google LLC, Apple Inc., Intuit Inc., The Global Risks Alliance (GRA)

Service providers or contractors: The Global Risks Alliance (GRA)

Internet or other electronic network activity information

Sold or Shared

Targeted Advertising

Personal Data processed: First name; Last name; Gender; Date of birth + 111

Personal Information collected or disclosed:

- first name
- last name
- gender
- date of birth
- phone number
- company name
- profession
- physical address
- fax number
- country
- state
- county
- email address
- ZIP/Postal code
- various types of Data
- city
- field of activity
- User ID
- number of employees
- website
- Trackers
- Usage Data
- unique device identifiers for advertising (Google Advertiser ID or IDFA, for example)
- Universally unique identifier (UUID)
- Full access
- Read only access
- Read metadata
- Modify
- Insert and import
- Compose
- Basic settings management
- Sensitive settings management
- various types of Data as specified in the privacy policy of the service
- budget
- academic background
- billing address
- answers to questions
- clicks

- keypress events
- motion sensor events
- mouse movements
- scroll position
- touch events
- Data communicated while using the service
- geographic position
- profile picture
- screenshots
- workplace
- purchase history
- shipping address
- number of Users
- session statistics
- device information
- Data communicated in order to use the Service
- IP address
- Calendar permission
- Contacts permission
- Camera permission
- Approximate location permission (continuous)
- Approximate location permission (non-continuous)
- Microphone permission
- Phone permission
- Sensors permission
- SMS permission
- Storage permission
- Reminders permission
- HomeKit permission
- Motion sensors permission
- Bluetooth sharing permission
- Social media accounts permission
- Microphone permission, without recording
- NFC Reader permission
- Media Library permission (Music)
- Photo Library permission
- Siri permission
- Apple's speech recognition servers permission
- TV Provider permission
- Google Assistant permission
- Google Home permission
- Call permission
- Camera permission, without saving or recording
- Write-only Photo Library permission
- name
- social media accounts
- language
- user content
- contact info
- picture
- house number
- prefix
- data relating to the point of sale
- Twitter handle
- order ID
- referral URL
- page views
- province
- latitude (of city)
- longitude (of city)
- metro area
- geography/region
- app information
- device logs
- operating systems
- browser information
- launches
- number of sessions

- session duration
- scroll-to-page interactions
- video views
- browsing history
- search history
- interaction events
- page events
- custom events
- Application opens

Sensitive Personal Information collected or disclosed VAT Number, Tax ID, username, payment info, Precise location permission (continuous), Precise location permission (non-continuous), Biometric Data access permission, Health Data read permission, Health Data update permission , marital status, password, Social Security number (SSN)

Purposes:

- Contacting the User
- Displaying content from external platforms
- Analytics
- Content commenting
- Infrastructure monitoring
- Interaction with external social networks and platforms
- Registration and authentication
- Registration and authentication provided directly by The Global Risks Alliance (GRA)
- Remarketing and behavioral targeting
- Spam and bots protection
- Tag management
- Further information about Personal Data
- Handling activities related to productivity
- Handling payments
- Collection of privacy-related preferences
- Device permissions for Personal Data access
- Managing contacts and sending messages
- Managing data collection and online surveys
- Platform services and hosting
- Building and running The Global Risks Alliance (GRA)
- Advertising

Retention period: for the time necessary to fulfill the purpose

Sold or Shared: Yes

Targeted Advertising: Yes

Third-parties: Google LLC, Automattic Inc., YANDEX, LLC, GitHub Inc., Meta Platforms, Inc., Vimeo, LLC, Pingdom AB, PayPal Inc., reddit inc., Pinterest, Inc., Italiaonline S.p.A., Adobe Systems Incorporated, Apple Inc., iubenda srl, SoundCloud Limited, Intuit Inc., The Global Risks Alliance (GRA), Fonticons, Inc. , Jetpack Digital LLC

Service providers or contractors: The Global Risks Alliance (GRA)

Employment related information

Sold or Shared

Targeted Advertising

Personal Data processed: First name; Last name; Gender; Date of birth + 40

Personal Information collected or disclosed:

- first name
- last name
- gender
- date of birth
- phone number
- company name
- profession
- physical address
- fax number

- country
- state
- county
- email address
- ZIP/Postal code
- various types of Data
- city
- field of activity
- User ID
- number of employees
- website
- Trackers
- Usage Data
- budget
- academic background
- billing address
- geographic position
- picture
- profile picture
- screenshots
- workplace
- Data communicated while using the service
- answers to questions
- name
- social media accounts
- language
- user content
- contact info
- shipping address
- house number
- prefix
- data relating to the point of sale
- Twitter handle
- purchase history
- device information

Sensitive Personal Information collected or disclosed VAT Number, Tax ID, username, payment info, marital status, password, Social Security number (SSN)

Purposes:

- Contacting the User
- Registration and authentication provided directly by The Global Risks Alliance (GRA)
- Social features
- Handling activities related to productivity
- Managing data collection and online surveys
- Registration and authentication
- Building and running The Global Risks Alliance (GRA)

Retention period: for the time necessary to fulfill the purpose

Sold or Shared: Yes

Targeted Advertising: Yes

Third-parties: Google LLC, The Global Risks Alliance (GRA)

Service providers or contractors: The Global Risks Alliance (GRA)

Biometric information

Sold or Shared

Targeted Advertising

Personal Data processed: General activity data; Food related activity ; Gender; Date of birth + 27

Personal Information collected or disclosed:

- general activity data
- food related activity
- gender
- date of birth
- Calendar permission
- Contacts permission
- Camera permission
- Approximate location permission (continuous)
- Approximate location permission (non-continuous)
- Microphone permission
- Phone permission
- Sensors permission
- SMS permission
- Storage permission
- Reminders permission
- HomeKit permission
- Motion sensors permission
- Bluetooth sharing permission
- Social media accounts permission
- Microphone permission, without recording
- NFC Reader permission
- Media Library permission (Music)
- Photo Library permission
- Siri permission
- Apple's speech recognition servers permission
- TV Provider permission
- Google Assistant permission
- Google Home permission
- Call permission
- Camera permission, without saving or recording
- Write-only Photo Library permission

Sensitive Personal Information collected or disclosed body measurements & indexes, movement activity, sleeping activity, heart rate and other vital data, blood type, Precise location permission (continuous), Precise location permission (non-continuous), Biometric Data access permission, Health Data read permission, Health Data update permission

Purposes:

- Handling activity data
- Device permissions for Personal Data access

Retention period: for the time necessary to fulfill the purpose

Sold or Shared: Yes

Targeted Advertising: Yes

Geolocation data

Sold or Shared

Targeted Advertising

Personal Data processed: General activity data; Food related activity ; Gender; Date of birth + 93

Personal Information collected or disclosed:

- general activity data
- food related activity
- gender
- date of birth
- geographic position
- first name
- last name
- physical address
- phone number
- email address
- profession
- company name

- country
- state
- county
- picture
- city
- Trackers
- Usage Data
- profile picture
- screenshots
- workplace
- Data communicated while using the service
- Calendar permission
- Contacts permission
- Camera permission
- Approximate location permission (continuous)
- Approximate location permission (non-continuous)
- Microphone permission
- Phone permission
- Sensors permission
- SMS permission
- Storage permission
- Reminders permission
- HomeKit permission
- Motion sensors permission
- Bluetooth sharing permission
- Social media accounts permission
- Microphone permission, without recording
- NFC Reader permission
- Media Library permission (Music)
- Photo Library permission
- Siri permission
- Apple's speech recognition servers permission
- TV Provider permission
- Google Assistant permission
- Google Home permission
- Call permission
- Camera permission, without saving or recording
- Write-only Photo Library permission
- fax number
- ZIP/Postal code
- various types of Data
- field of activity
- number of employees
- User ID
- website
- billing address
- shipping address
- house number
- prefix
- data relating to the point of sale
- language
- Twitter handle
- budget
- contact info
- purchase history
- device information
- province
- latitude (of city)
- longitude (of city)
- metro area
- geography/region
- IP address
- app information
- device logs
- operating systems
- browser information
- launches
- number of sessions

- session duration
- scroll-to-page interactions
- mouse movements
- scroll position
- keypress events
- motion sensor events
- touch events
- video views
- clicks
- browsing history
- search history
- session statistics
- page views
- interaction events
- page events
- custom events
- Application opens

Sensitive Personal Information collected or disclosed body measurements & indexes, movement activity, sleeping activity, heart rate and other vital data, blood type, username, VAT Number, Precise location permission (continuous), Precise location permission (non-continuous), Biometric Data access permission, Health Data read permission, Health Data update permission , password, Tax ID, Social Security number (SSN), marital status, payment info

Purposes:

- Handling activity data
- Location-based interactions
- Social features
- Handling activities related to productivity
- Device permissions for Personal Data access
- Registration and authentication
- Building and running The Global Risks Alliance (GRA)
- Spam and bots protection

Retention period: for the time necessary to fulfill the purpose

Sold or Shared: Yes

Targeted Advertising: Yes

Third-parties: Google LLC, The Global Risks Alliance (GRA)

Service providers or contractors: The Global Risks Alliance (GRA)

Inferences drawn from other personal information

Sold or Shared

Targeted Advertising

Personal Data processed: General activity data; Food related activity ; Gender; Date of birth + 79

Personal Information collected or disclosed:

- general activity data
- food related activity
- gender
- date of birth
- Full access
- Read only access
- Read metadata
- Modify
- Insert and import
- Compose
- Basic settings management
- Sensitive settings management
- Trackers
- physical address
- company name

- country
- county
- city
- budget
- academic background
- billing address
- Usage Data
- answers to questions
- clicks
- keypress events
- motion sensor events
- mouse movements
- scroll position
- touch events
- name
- social media accounts
- phone number
- profession
- workplace
- first name
- last name
- email address
- language
- profile picture
- user content
- contact info
- geographic position
- state
- fax number
- ZIP/Postal code
- picture
- various types of Data
- field of activity
- number of employees
- User ID
- website
- shipping address
- house number
- prefix
- data relating to the point of sale
- Twitter handle
- purchase history
- device information
- Data communicated while using the service
- screenshots
- province
- latitude (of city)
- longitude (of city)
- metro area
- geography/region
- IP address
- app information
- device logs
- operating systems
- browser information
- launches
- number of sessions
- session duration
- scroll-to-page interactions
- video views
- browsing history
- search history
- session statistics
- page views
- interaction events
- page events
- custom events
- Application opens

Sensitive Personal Information collected or disclosed body measurements & indexes, movement activity, sleeping activity, heart rate and other vital data, blood type, payment info, marital status, username, password, VAT Number, Tax ID, Social Security number (SSN)

Purposes:

- Handling activity data
- Registration and authentication
- Registration and authentication provided directly by The Global Risks Alliance (GRA)
- Spam and bots protection
- Managing data collection and online surveys
- Building and running The Global Risks Alliance (GRA)

Retention period: for the time necessary to fulfill the purpose

Sold or Shared: Yes

Targeted Advertising: Yes

Third-parties: Google LLC, The Global Risks Alliance (GRA)

Service providers or contractors: The Global Risks Alliance (GRA)

Audio, electronic, visual, thermal, olfactory, or similar information

Sold or Shared

Targeted Advertising

Personal Data processed: First name; Last name; Physical address; Gender + 66

Personal Information collected or disclosed:

- first name
- last name
- physical address
- gender
- date of birth
- phone number
- email address
- geographic position
- profession
- company name
- country
- state
- county
- picture
- city
- Trackers
- Usage Data
- profile picture
- screenshots
- workplace
- Data communicated while using the service
- Calendar permission
- Contacts permission
- Camera permission
- Approximate location permission (continuous)
- Approximate location permission (non-continuous)
- Microphone permission
- Phone permission
- Sensors permission
- SMS permission
- Storage permission
- Reminders permission
- HomeKit permission
- Motion sensors permission
- Bluetooth sharing permission
- Social media accounts permission

- Microphone permission, without recording
- NFC Reader permission
- Media Library permission (Music)
- Photo Library permission
- Siri permission
- Apple's speech recognition servers permission
- TV Provider permission
- Google Assistant permission
- Google Home permission
- Call permission
- Camera permission, without saving or recording
- Write-only Photo Library permission
- answers to questions
- name
- social media accounts
- billing address
- language
- user content
- contact info
- fax number
- ZIP/Postal code
- various types of Data
- field of activity
- number of employees
- User ID
- website
- shipping address
- house number
- prefix
- data relating to the point of sale
- Twitter handle
- budget
- purchase history
- device information

Sensitive Personal Information collected or disclosed username, VAT Number, Precise location permission (continuous), Precise location permission (non-continuous), Biometric Data access permission, Health Data read permission, Health Data update permission , payment info, marital status, password, Tax ID, Social Security number (SSN)

Purposes:

- Social features
- Handling activities related to productivity
- Device permissions for Personal Data access
- Managing data collection and online surveys
- Registration and authentication
- Building and running The Global Risks Alliance (GRA)

Retention period: for the time necessary to fulfill the purpose

Sold or Shared: Yes

Targeted Advertising: Yes

Third-parties: Google LLC, The Global Risks Alliance (GRA)

Service providers or contractors: The Global Risks Alliance (GRA)

ℹ️ You can read the definitions of these concepts inside the "Definitions and legal references section" of the privacy policy.

To know more about your rights in particular to opt out of certain processing activities and to limit the use of your sensitive personal information ("Limit the Use of My Sensitive Personal Information") you can refer to the "Your privacy rights under US state laws" section of our privacy policy.

For more details on the collection of Personal Information, please read the section "Detailed information on the processing of Personal Data" of our privacy policy.

We won't process your Information for unexpected purposes, or for purposes that are not reasonably necessary to and compatible with the purposes originally disclosed, without your consent.

What are the sources of the Personal Information we collect?

We collect the above-mentioned categories of Personal Information, either directly or indirectly, from you when you use The Global Risks Alliance (GRA).

For example, you directly provide your Personal Information when you submit requests via any forms on The Global Risks Alliance (GRA). You also provide Personal Information indirectly when you navigate The Global Risks Alliance (GRA), as Personal Information about you is automatically observed and collected.

Finally, we may collect your Personal Information from third parties that work with us in connection with the Service or with the functioning of The Global Risks Alliance (GRA) and features thereof.

Your privacy rights under US state laws

You may exercise certain rights regarding your Personal Information. In particular, to the extent permitted by applicable law, you have:

- **the right to access Personal Information: the right to know.** You have the right to request that we confirm whether or not we are processing your Personal Information. You also have the right to access such Personal Information;
- **the right to correct inaccurate Personal Information.** You have the right to request that we correct any inaccurate Personal Information we maintain about you;
- **the right to request the deletion of your Personal Information.** You have the right to request that we delete any of your Personal Information;
- **the right to obtain a copy of your Personal Information.** We will provide your Personal Information in a portable and usable format that allows you to transfer data easily to another entity – provided that this is technically feasible;
- **the right to opt out from the Sale of your Personal Information;** We will not discriminate against you for exercising your privacy rights.
- **the right to non-discrimination.**

Additional rights for Users residing in California

In addition to the rights listed above common to all Users in the United States, as a User residing in California, you have:

- **The right to opt out of the Sharing of your Personal Information** for cross-context behavioral advertising;
- **The right to request to limit our use or disclosure of your Sensitive Personal Information** to only that which is necessary to perform the services or provide the goods, as is reasonably expected by an average consumer. Please note that certain exceptions outlined in the law may apply, such as, when the collection and processing of Sensitive Personal Information is necessary to verify or maintain the quality or safety of our service.

Additional rights for Users residing in Virginia, Colorado, Connecticut, Texas, Oregon, Nevada, Delaware, Iowa, New Hampshire, New Jersey, Nebraska, Tennessee, Minnesota, Maryland, Indiana, Kentucky, Rhode Island and Montana

In addition to the rights listed above common to all Users in the United States, as a User residing in Virginia, Colorado, Connecticut, Texas, Oregon, Nevada, Delaware, Iowa, New Hampshire, New Jersey, Nebraska, Tennessee, Minnesota, Maryland, Indiana, Kentucky, Rhode Island and Montana you have

- **The right to opt out of** the processing of your personal information for **Targeted Advertising or profiling** in furtherance of decisions that produce legal or similarly significant effects concerning you;
- **The right to freely give, deny or withdraw your consent for the processing of your Sensitive Personal Information.** Please note that certain exceptions outlined in the law may apply, such as, but not limited to, when the collection and processing of Sensitive Personal Information is necessary for the provision of a product or service specifically requested by the consumer. In Maryland, your Sensitive Personal Information will be collected or processed only if strictly necessary to provide or maintain a specific product or service requested by you.

In Minnesota and Maryland Users also have the right to obtain a list of the specific third parties to which the controller has disclosed the consumer's personal data

* Note that in some states like Minnesota you have the following specific rights connected to profiling:

- The right to question the results of the profiling;
- The right to be informed of the reason that the profiling resulted in the decision; if feasible
- The right to be informed of what actions the consumer might have taken to secure a different decision and the actions that the consumer might take to secure a different decision in the future;
- The right to review personal data used in the profiling;
- If inaccurate, the right to have the data corrected and the profiling decision reevaluated based on the corrected data;

Additional rights for users residing in Utah and Iowa

In addition to the rights listed above common to all Users in the United States, as a User residing in Utah and Iowa, you have:

- **The right to opt out of** the processing of your Personal Information for **Targeted Advertising**;
- **The right to opt out of the processing of your Sensitive Personal Information.** Please note that certain exceptions outlined in the law may apply, such as, but not limited to, when the collection and processing of Sensitive Personal Information is necessary for the provision of a product or service specifically requested by the consumer.

How to exercise your privacy rights under US state laws

To exercise the rights described above, you need to submit your request to us by contacting us via the contact details provided in this document.

For us to respond to your request, we must know who you are. We will not respond to any request if we are unable to verify your identity and therefore confirm the Personal Information in our possession relates to you. You are not required to create an account with us to submit your request. We will use any Personal Information collected from you in connection with the verification of your request solely for verification and shall not further disclose the Personal Information, retain it longer than necessary for purposes of verification, or use it for unrelated purposes.

If you are an adult, you can make a request on behalf of a child under your parental authority.

How to exercise your rights to opt out

In addition to what is stated above, to exercise your right to opt-out of Sale or Sharing and Targeted Advertising you can also use the privacy choices link provided on The Global Risks Alliance (GRA).

If you want to submit requests to opt out of Sale or Sharing and Targeted Advertising activities via a user-enabled **global privacy control**, such as for example the Global Privacy Control (“GPC”), you are free to do so and we will abide by such request in a frictionless manner.

How and when we are expected to handle your request

We will respond to your request without undue delay, but in all cases within the timeframe required by applicable law. Should we need more time, we will explain to you the reasons why, and how much more time we need.

Should we deny your request, we will explain to you the reasons behind our denial (where envisaged by applicable law you may then contact the relevant authority to submit a complaint).

We do not charge a fee to process or respond to your request unless such request is manifestly unfounded or excessive and in all other cases where it is permitted by the applicable law. In such cases, we may charge a reasonable fee or refuse to act on the request. In either case, we will communicate our choices and explain the reasons behind them.

Additional information for Users in the United States

Collection of Personal Information about California consumers aged 13 to 16

We collect Personal Information of consumers between the age of 13 and 16 and won't Sell or Share their Personal Information unless those consumers have opted in.

Collection of Personal Information about California consumers below the age of 13

We collect Personal Information of consumers below the age of 13 and won't Sell or Share their Personal Information unless their parents or guardians have opted in on behalf of those minors.

Profiling of Users in Virginia, Colorado, Connecticut, Utah, Texas, Oregon, Delaware, New Hampshire, New Jersey, Nebraska, Tennessee, Minnesota and Montana

We perform automated processing of your Personal Information to evaluate, analyze, or predict personal aspects related to, for example, your economic situation, health, personal preferences, interests, reliability, behavior, location, or movements. Such profiling activity is done in furtherance of decisions that may result in the provision or denial of, for example, financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, healthcare services, or access to essential goods or services.

You always have the right to opt out from this kind of profiling activity. To fully exercise this right to opt out you can contact us at any time, using the contact details provided in this document. To find out more about your rights and how to exercise them, you can consult the“Your privacy rights under US state laws” section of this document.

Additional information about Data collection and processing

Legal action

The User's Personal Data may be used for legal purposes by the Owner in Court or in the stages leading to possible legal action arising from improper use of The Global Risks Alliance (GRA) or the related Services.
The User declares to be aware that the Owner may be required to reveal personal data upon request of public authorities.

Additional information about User's Personal Data

In addition to the information contained in this privacy policy, The Global Risks Alliance (GRA) may provide the User with additional and contextual information concerning particular Services or the collection and processing of Personal Data upon request.

System logs and maintenance

For operation and maintenance purposes, The Global Risks Alliance (GRA) and any third-party services may collect files that record interaction with The Global Risks Alliance (GRA) (System logs) or use other Personal Data (such as the IP Address) for this purpose.

Information not contained in this policy

More details concerning the collection or processing of Personal Data may be requested from the Owner at any time. Please see the contact information at the beginning of this document.

Changes to this privacy policy

The Owner reserves the right to make changes to this privacy policy at any time by notifying its Users on this page and possibly within The Global Risks Alliance (GRA) and/or - as far as technically and legally feasible - sending a notice to Users via any contact information available to the Owner. It is strongly recommended to check this page often, referring to the date of the last modification listed at the bottom.

Should the changes affect processing activities performed on the basis of the User’s consent, the Owner shall collect new consent from the User, where required.

Definitions and legal references

Personal Data (or Data) / Personal Information (or Information)

Any information that directly, indirectly, or in connection with other information — including a personal identification number — allows for the identification or identifiability of a natural person.

Sensitive Personal Information

Sensitive Personal Information means any Personal Information that is not publicly available and reveals information considered sensitive according to the applicable privacy law.

Usage Data

Information collected automatically through The Global Risks Alliance (GRA) (or third-party services employed in The Global Risks Alliance (GRA)), which can include: the IP addresses or domain names of the computers utilized by the Users who use The Global Risks Alliance (GRA), the URI addresses (Uniform Resource Identifier), the time of the request, the method utilized to submit the request to the server, the size of the file received in response, the numerical code indicating the status of the server's answer (successful outcome, error, etc.), the country of origin, the features of the browser and the operating system utilized by the User, the various time details per visit (e.g., the time spent on each page within the Application) and the details about the path followed within the Application with special reference to the sequence of pages visited, and other parameters about the device operating system and/or the User's IT environment.

User

The individual using The Global Risks Alliance (GRA) who, unless otherwise specified, coincides with the Data Subject.

Data Subject

The natural person to whom the Personal Data refers.

Data Processor (or Processor)

The natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller, as described in this privacy policy.

Data Controller (or Owner)

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data, including the security measures concerning the operation and use of The Global Risks Alliance (GRA). The Data Controller, unless otherwise specified, is the Owner of The Global Risks Alliance (GRA).

The Global Risks Alliance (GRA) (or this Application)

The means by which the Personal Data of the User is collected and processed.

Service

The service provided by The Global Risks Alliance (GRA) as described in the relative terms (if available) and on this site/application.

Sale

Sale means any exchange of Personal Information by the Owner to **a third party, for monetary or other valuable consideration**, as defined by the applicable privacy US state law. Please note that the exchange of Personal Information with a service provider pursuant to a written contract that meets the requirements set by the applicable law, does not constitute a Sale of your Personal Information.

Sharing

Sharing means any sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's Personal Information by the business to a **third party for cross-context behavioral advertising**, whether for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged, as defined by the California privacy laws. Please note that the exchange of Personal Information with a service provider pursuant to a written contract that meets the requirements set by the California privacy laws, does not constitute sharing of your Personal Information.

Targeted advertising

Targeted advertising means displaying advertisements to a consumer where the advertisement is selected based on Personal Information obtained from that consumer’s activities over time and across nonaffiliated websites or online applications to predict such consumer’s preferences or interests, as defined by the applicable privacy US state law.

European Union (or EU)

Unless otherwise specified, all references made within this document to the European Union include all current member states to the European Union and the European Economic Area.

Cookie

Cookies are Trackers consisting of small sets of data stored in the User's browser.

Tracker

Tracker indicates any technology - e.g Cookies, unique identifiers, web beacons, embedded scripts, e-tags and fingerprinting - that enables the tracking of Users, for example by accessing or storing information on the User’s device.

Full access

Full access to the account, including permanent deletion of threads and messages.

Read only access

Read all resources and their metadata—no write operations.

Read metadata

Read resources metadata including labels, history records, and email message headers, but not the message body or attachments.

Modify

All read/write operations except immediate, permanent deletion of threads and messages, bypassing Trash.

Insert and import

Insert and import messages only.

Compose

Create, read, update, and delete drafts. Send messages and drafts.

Basic settings management

Manage basic mail settings.

Sensitive settings management

Manage sensitive mail settings, including forwarding rules and aliases.

Legal information

This policy has been prepared based on provisions of multiple legislations.

This policy relates solely to The Global Risks Alliance (GRA), if not stated otherwise within this document.

How can we help?

What you can do

Your data

- Ask us to know and access the information we hold on you
- Ask us to correct information we hold on you
- Ask us to be forgotten (delete the information we hold on you)
- Ask to port your data to another service

In case of issues

While we strive to create a positive user experience, we understand that issues may occasionally arise between us and our users. If this is the case, please feel free to contact us.

Contact us

Footer

The Global Risks Alliance (GRA)

The Global Risks Alliance

Owner contact email: contact@theglobalriskalliance.com

Downloadable documents

- Privacy Policy
  Latest update: May 08, 2026
- Cookie Policy
  Latest update: May 08, 2026
- Terms and Conditions
  Latest update: May 08, 2026

iubenda hosts this content and only collects the Personal Data strictly necessary for it to be provided.