SUMMIT MANAGEMENT SERVICES

Customer Privacy Notice

Last update : 13/08/2025

Our privacy commitment includes:

- Ensuring the security and confidentiality of your personal data.
- Never selling your personal information.
- Allowing you to manage and review your marketing preferences at any time.

1. About us

The Summit Management Services sp. z o.o. company (hereinafter “Summit”) is responsible for providing products or services and will oversee the processing of your personal data associated with those offerings. This Summit Management Services sp. z o.o. entity is identified as the “controller” of your personal data.

The Regulation (EU) 2016/679 of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter “GDPR”) stipulates that personal data must be processed lawfully, fairly, and in a transparent manner. Therefore, this privacy policy (hereinafter the “Policy”) aims to provide you with clear and simple information regarding the processing of your personal data during your navigation and operations conducted on our website.

2. Reasons for reviewing this notice

We gather your personal data through:

- our website / app at www.summit.io or app.summit.io

When referring to “personal data”, we are describing information that:

- We know about you (for example, we know such as activity associated with your Summit account for checking investments).

- Can potentially identify you personally (such as a combination of your name and postal address).

This notice clarifies the details of what information we collect, how it is utilised, and your rights concerning your personal data.

These notices:

- Provide detailed information on how Summit collects, uses, and safeguards your personal data when you utilise specific Summit products or services.
- Will be accessible to you via the Summit app when you start using relevant Summit products or services.
- Are available for review at any time on the Summit website (see here).

We may issue privacy notices and explanations in languages besides English. In cases where there are differences between translations and the English version, the English version takes precedence.

If you have questions about how we handle your personal data, you can reach us at dpo@summit.io.

3. Data controller

In the course of your activities on the summit.io site/app, we collect and use personal data related to you, natural persons.

For all data processing activities, Summit Management Services sp. z o.o. (operating under the trade name Summit), registered under number 528172198 with TIN 7831900833 and located at Władysława Andersa 3, Floor 11, PL-61-894, Poznań, Poland, determines the means and purposes of the processing. Thus, we act as the Data Controller, as defined by personal data regulations, including Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

4. What personal data do we collect and how?

By using our website or subscribing to our services, you provide us with certain information about yourself, some of which can identify you ("Personal Data"). This occurs when you browse our site, fill out online forms, or simply become a customer.

The nature and quality of the Personal Data collected about you vary depending on your interactions with Summit, the main types being:

Type of personal data	Details
Information you give us	We collect information you provide when you: ➔ fill in any forms ➔ correspond with us ➔ respond to any of our surveys ➔ register to use the Summit app ➔ open an account or use any of our services ➔ take part in online discussions or promotions ➔ speak with a member of our social media or customer support teams (either on the phone or through the Summit app) ➔ enter a competition or share information with us on social media ➔ contact us for other reasons. We will collect the following information: ➔ your name, address, nationality / citizenship, and date of birth ➔ your email address, phone number and details of the device you use (for example, your phone, computer or tablet, browser, operating system, IP address, location via IP) ➔ your Discord username ➔ your registration information ➔ details of your bank account, including the account number, sort code and IBAN ➔ copies of your identification documents (for example, your passport) and any other information you provide to prove you are eligible to use our services ➔ your country of residence, tax residency information, and tax identification number ➔ information you provide when you apply for services, including details about your, or your spouse's, income and financial obligations ➔ information you provide when you sign up, including details about your employment and salary ➔ Records of our discussions, if you contact us or we contact you (including records of phone calls) ➔ Your image in photo or video form, and facial scan data extracted from your photo or video (known as 'biometric data'), to verify your identity during onboarding as part of our Know-Your-Customer (KYC)

	checks, to authenticate you as an authorised user of our services, or to detect and prevent fraud ➔ Information about other people (such as a joint account holder, your spouse or family) when we ask you to give us this information to enable us to comply with our obligations under KYC, anti-money laundering and other laws and to assist with fraud monitoring ➔ In some cases, particularly for clients who do not have an address in their name and are residing with third parties, we may request information about the individuals who are hosting you. This information includes their identity card and a certificate of residence. We collect this information to ensure compliance with legal requirements and to enhance our fraud prevention measures. ➔ Additional requirements for US residents: For clients who are US residents or US persons for tax purposes, we may collect additional documentation to comply with US regulatory obligations, including but not limited to: - US tax identification numbers (SSN/TIN) - IRS Forms W-2, 1099, and other relevant tax documents - US federal tax returns (Forms 1040 and schedules) - Documentation evidencing US tax compliance This enhanced collection is required under the Foreign Account Tax Compliance Act (FATCA), anti-money laundering regulations (FinCEN), and Office of Foreign Assets Control (OFAC) compliance requirements that apply to financial institutions serving US persons. If you give us personal data about other people, or you ask us to share their personal data with third parties, you confirm that you have brought this notice to their attention beforehand.
Information collected from your use of our products and services	Whenever you use our website or app, we collect the following information: ➔ Technical information, including the internet protocol (IP) address used to connect your computer to the internet, your login information, the browser type and version, the time zone setting, device language, the operating system and platform, the type of device you use, whether your device uses a virtual private network (VPN), a unique device identifier (for example, your mobile operating system and the type of mobile browser you use) ➔ Information about your visit, including the links you've clicked on, through and from our website or app

	(including date and time), services you viewed or searched for, page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling and clicks), and methods used to browse away from the page ➔ Information on transactions and your use of Summit products (for example, Purchase and Sell of SMK, subscription details about Summit Research, etc.), including the date, time, amount, currencies, exchange rate, beneficiary details, IP address of Seller and Buyer, Seller's and Buyer's name and registration information, messages sent or received, details of device used to arrange the payment and the payment method used.
Information from social media	➔ Occasionally, we'll use publicly available information about you from selected social media websites or apps to carry out enhanced due diligence checks. Publicly available information from social media websites or apps may also be provided to us when we conduct general searches on you (for example, to comply with our anti-money laundering or sanctions screening obligations).
Information from publicly available sources	➔ We collect information and contact details from publicly available sources, such as media stories, online registers or directories, and websites for enhanced due diligence checks, security searches, and KYC purposes.

5. Why do we collect your personal data and how?

We collect your Personal Data for specific purposes and on various legal grounds.

In the context of contract execution or pre-contractual measures, your Data is processed for the following purposes:

- Order management
- Contract management
- Customer account management
- Handling complaints and after-sales service
- Managing contests
- Processing job applications

Based on your consent, your Data is processed for the following purposes:

- Managing cookies requiring your consent

Under Summit's legitimate interests, your Data is processed for the following purposes:

- Establishing product and service improvement statistics
- Conducting satisfaction surveys and polls
- Managing pre-litigation and litigation
- Managing newsletters sent to customers
- Conducting commercial and marketing operations
- External communications

Under legal and regulatory obligations applicable to Summit, your Data is processed for the following purposes:

- Fraud prevention
- Customer account verification
- Combating money laundering and terrorism financing
- General and subsidiary accounting requirements

6. Do we share your personal data?

Your data is intended for the authorised employees of Summit responsible for managing and executing contracts and legal obligations, depending on the purposes of the collection and within the limits of their respective roles.

They may be transmitted, for certain tasks related to the purposes, and within the limits of their missions and authorisations, to the following recipients:

Service providers and subcontractors that we use to perform a set of operations and tasks on our behalf, including:

- ClickUp
- SumSub
- Scorechain
- ComplyAdvantage
- Fireblocks
- HubSpot
- Synaps

- PassFort
- Onfido
- AirCall
- Discord
- Google Workspace
- PandaDoc
- Calendly
- ActiveCampaign
- Postmark
- Bugnsag
- LogRocket
- HotJar
- Firebase
- Stripe
- Shopify
- Twilio
- Placekit
- Google Analytics
- Agorapulse

- Commercial partners only when you have expressly consented via a checkbox on our data collection forms;
- Duly authorised public authorities (judicial, regulatory, etc.), within the framework of our legal and regulatory obligations;
- Regulated professionals (lawyers, bailiffs, etc.) who may intervene in the implementation of guarantees, recovery, or litigation;

When your data is communicated to our service providers and subcontractors, they are also asked not to use the data for purposes other than those initially intended. We do everything possible to ensure that these third parties maintain the confidentiality and security of your data.

In any case, only the necessary data is provided. We make every effort to ensure the secure communication or transmission of your data.

We do not sell your data.

7. Is your personal data transferred to third countries?

Summit strives to keep within the European Economic Area (EEA).

However, it is possible that the data we collect when you use our platform or as part of our services may be transferred to other countries. This may occur, for example, if some of our service providers are located outside the European Economic Area.

In the event of such a transfer, we ensure that it is carried out:

- To a country providing an adequate level of protection, i.e., a level of protection equivalent to what European regulations require;
- Within the framework of standard contractual clauses;
- Within the framework of binding corporate rules.

8. How long do we keep your personal data?

We retain your personal data only for the time necessary to achieve the purpose for which we hold this data, in order to meet your needs or fulfill our legal obligations.

Retention periods vary based on several factors, such as:

- The needs of Summit's activities;
- Contractual requirements;
- Legal obligations;
- Recommendations from regulatory authorities.

The retention periods for your data are as follows:

Purposes	Retention periods
Order management	10 years
Contract management	For the duration of the business relationship
Customer account management	5 years from the account closure
Claims and after-sales service management	5 years from the end of the contractual relationship
Application management	From the decision not to retain the candidate. Then 2 years after the last contact with the non-retained candidate
Prospecting through contests	Until consent is withdrawn or 3 years from the last contact with the organisation

Carrying out commercial and marketing prospecting operations	1 year during the prospecting period, then 3 years from the last contact
Newsletter management	3 years from the last contact
Management of cookies requiring your consent	13 months
Establishment of statistics for product and service improvement	13 months
Conducting satisfaction surveys and polls	Personal data related to clients cannot be kept beyond the duration strictly necessary for managing the business relationship
Customer account verification	5 years from the end of the contractual relationship
Fraud prevention	5 years from the closure of the fraud case
Combating tax fraud and fulfilling our tax reporting and compliance obligations	6 years from the end of any contractual relationship
Anti-money laundering and counter-terrorism financing	5 years from the end of the relationship with the concerned individual
Maintenance of general and subsidiary accounting	10 years

9. How do we ensure the security of your personal data?

Summit is committed to protecting the personal data we collect or process against loss, destruction, alteration, unauthorised access, or disclosure.

Therefore, we implement all appropriate technical and organisational measures, according to the nature of the data and the risks involved in their processing. These measures aim to preserve the security and confidentiality of your personal data. They may include practices such as limited access to personal data by authorised individuals based on their roles, pseudonymisation, or encryption.

Additionally, our practices, policies, and/or physical and/or logical security measures (secure access, authentication procedures, backups, software, etc.) are regularly reviewed and updated if necessary.

10. What are your rights?

The GDPR provides the data subjects with rights that you can exercise. These include:

1. Right to information: The right to have clear, precise, and complete information about the use of personal data by Summit.
2. Right of access: The right to obtain a copy of the personal data held by the Data Controller about the requester.
3. Right to rectification: The right to have personal data corrected if it is inaccurate or outdated and/or to complete it if it is incomplete.
4. Right to erasure / right to be forgotten: The right, under certain conditions, to have data erased or deleted, unless Summit has a legitimate interest in retaining it.
5. Right to object: The right to object to the processing of personal data by Summit for reasons related to the requester's particular situation (under conditions).
6. Right to withdraw consent: The right to withdraw consent at any time when the processing is based on consent.
7. Right to restriction of processing: The right, under certain conditions, to request that the processing of personal data be temporarily suspended.
8. Right to data portability: The right to request that personal data be transmitted in a reusable format that allows it to be used in another database.
9. Right not to be subject to automated decision-making: The right for the requester to refuse fully automated decision-making and/or to exercise additional safeguards offered in this regard.
10. Right to define post-mortem directives: The right for the requester to define directives regarding the fate of personal data after their death.

Additional rights may be granted by local regulations to data subjects.

To this end, Summit has implemented a procedure for managing data subjects' rights in accordance with the requirements of applicable legislation. This procedure establishes:

- The standards to be respected to ensure transparent information for data subjects
- The legal requirements that must be met
- The authorised means to submit a request for each right, depending on the category of data subjects
- The operational processes to handle these requests in accordance with the aforementioned requirements
- The parties involved in these processes, their roles, and responsibilities.

To exercise your rights, you can contact the Data Protection Officer (DPO) at: dpo@summit.io.

When you submit a request to exercise a right, you are asked to specify the scope of the request as much as possible, the type of right exercised, the personal data processing concerned, and any other useful elements to facilitate the review of your request. Additionally, in case of reasonable doubt, you may be asked to prove your identity.

11. Cookies and tracking technologies

We use cookies to analyse how you interact with our website. Please refer to our Cookies Policy for more information about cookies. Additionally, we utilise pixels or web beacons in the direct marketing emails we send to you. These pixels track whether our emails were delivered and opened, and if links within the emails were clicked. They also allow us to collect information such as your IP address, browser, email client type, and other similar details. This information is used to measure the performance of our email campaigns and for analytics purposes.

12. Updating this Policy

This Policy may be regularly updated to take into account changes in regulations related to personal data.