Privacy Statement

Privacy Statement

I. INTRODUCTION OF DATA CONTROLLER

In order to ensure the legality of its internal data protection processes and the rights of the data subjects, **BOTS Slovakia s.r.o.** (hereinafter: Data Controller) formulates the following privacy statement.

Name of Data Controller:

BOTS Slovakia s.r.o.

Trade registry nr.:

53601033

Registered seat:

Karpatské námestie 10A 831 06 Bratislava - mestská časť Rača

Electronic address: privacy@revenyou.io

Representative:

Colin Groos and Michael Antonius Stokman

Data Protection Officer (DPO):

Bovard Kft. (info@bovard.hu)

The personal data of the data subjects are managed in accordance with the requirements of all effective laws, but primarily in accordance with the requirements of the following laws:

- Act No. 18/2018 Coll. Act on the Protection of Personal Data and on Amendments to Certain Acts (hereinafter: Protection of Personal Data Act),
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal

data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter: GDPR).

The Data Controller keeps personal data confidential and employs technical and organizational measures relating to the storage of processing of said data in order to ensure its safety.

*****

II. PRELIMINARY OBSERVATIONS

Definitions

The conceptual framework of this privacy statement is identical to that described in Article 4 of the GDPR, and in some points supplemented by the interpretative provisions of Section 1 of the Protection of Personal Data Act.

When the privacy statement mentions data or data processing/controlling it refers to personal data and the processing/controlling of personal data.

The source of personal data

The source of the personal data for the processing purposes set out in this privacy notice is primarily the data subject. In order to enable some features (such as opening the account and conducting the customer due diligence), the BOTS Platform may require the data subject to give access to the images stored in the device of the data subject, and/or to use the camera of the device of the data subject. If, for a particular purpose, the Data Controller obtains personal data from other sources, it will provide specific information in relation to that purpose.

Recipients of the personal data provided

Personal data shall only be processed by employees of the Data Controller whose job duties include the processing of personal data.

A list of the data processors used by the Data Controller is included in Chapter IV.

If, for a particular purpose, there may be other recipients of personal data, the Data Controller will provide specific information in relation to that purpose.

Automated decision-making and profiling

None of the processing purposes set out in this privacy statement involves automated decision-making and profiling as defined in Article 22 of the GDPR.

Consequences of failure to provide personal data

The provision of personal data for the processing purposes set out in this privacy statement is in general a necessary condition for the provision of the Data Controller's service through the BOTS App/Platform. Where the provision of personal data for certain purposes is possible on a voluntary basis, the Data Controller will provide specific information thereon.

*****

III. THE CHARACTERISTICS OF EACH DATA PROCESSING PURPOSE

The Data Controller is providing an automated digital service in the form of an integrated platform service (hereinafter: "BOTS Platform") where it connects the client (hereinafter: "Client" or "data subject") with certain parties, including cryptocurrency exchange (and wallet) service providers, and automated trading strategies that are computer programs designed and provided by independent developers (hereinafter: "BOT Creators") that automatically buy and sell cryptocurrencies based on a set trading strategy and indicators (hereinafter: "Bots").

BOTS Platform is available for the Clients through a mobile application (hereinafter: "BOTS

App") following the creation of a personalized account. In connection with accessing the

BOTS App, creating an account, carrying out a customer due diligence process, using the BOTS Platform, depositing and withdrawing funds, and other related activities, the processing of Clients' personal data by the Data Controller is essential.

The purpose of this privacy statement is to inform Clients in advance of the characteristics of the data processing operations carried out by the Data Controller in connection with the provision of services related to the BOTS platform.

*****

I. Access to BOTS App

To ensure secure access to the BOTS App, a security code must be provided by the Clients for each access. The security code is sent by the Data Controller automatically via SMS to

the phone number provided by the Client in the BOTS App login interface. Clients with an existing account can change the access method in the security settings to a passcode generated by them or to the device's Touch/Face ID.

Purpose of the data processing

The purpose of the processing is to ensure secure access to the application for the Clients.

Processed personal data

The Data Controller processes the telephone number provided by the Client and the security code that has been sent.

In case Clients with an existing account change the access method in the security settings to a passcode, the passcode generated by them is also processed by the Data Controller. However, in case of changing to Touch/Face ID access, these data remain stored on the device, to which the Data Controller has no access, therefore no further data is being processed by the Data Controller.

Legal basis of data processing

The legal basis for the processing of personal data is Article 6(1)(a) of the GDPR, i.e. the data subject's consent.

Time period of processing personal data

Until consent is withdrawn, but no later than until the account is deleted by the Client.

*****

II. Account opening

BOTS Platform and the services provided by the Data Controller are available to Clients following the creation of a personalized account (hereinafter: "BOTS Account").

Purpose of the data processing

The purpose of the data processing is to open a personalized account for Clients to gain access the BOTS Platform.

Processed personal data

In order to open a personalized account, the Data Controller processes personal data necessary to identify and contact the Client.

Legal basis of data processing

The legal basis for the account opening purpose is Article 6(1)(b) of the GDPR as the data are processed for the performance of a contract between the Client and the Data Controller.

Time period of processing personal data

Until the account is deleted by the Client, but no later than 5 years after the last account

login.

*****

Customer due diligence

In order to maintain the integrity and security of the BOTS Platform and prevent the misuse of the platform for the purpose of money laundering, terrorist financing, fraud or other financial crimes and, as well as to comply with the applicable international and national legal standards, the Data Controller applies specific Anti-Money Laundering (AML) and Know Your Customer (KYC) Due Diligence measures (hereinafter: “Customer due diligence or CDD”).

Customer due diligence measures apply in the following circumstances:

- when establishing a business relationship (i.e. opening a BOTS account) and periodically thereafter, as specified in the Data Controller’s internal anti-money laundering policy (hereinafter: “AML Policy”);
- when carrying out an occasional transaction through the BOTS Platform that is considered a potential risk based on the Data Controller’s AML Policy in accordance with the applicable international and national legal standards;
- when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;
- when there are doubts about the veracity or adequacy of previously obtained customer identification data.

Customer due diligence measures shall comprise:

- identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;
- identifying the beneficial owner and taking reasonable measures to verify that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer;
- assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
- conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the obliged entity's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date.

The Customer due diligence is carried out through the BOTS account of the Client. In addition to regular Customer due diligence, enhanced Customer due diligence shall also be carried out in cases where a potential risk is detected based on the Data Controller's AML Policy.

Purpose of the data processing

The purpose of the data processing is to carry out customer due diligence in accordance with the Data Controller's AML Policy and in compliance with the applicable international and national legal standards. **Processed personal data.**

Natural persons:

- personal data necessary to identify the Client,
- personal data necessary to contact the Client,
- personal data necessary to verify the identity of the Client,
- personal data necessary to determine the business and risk profile of the Client and to mitigate money laundering, terrorist financing or other financial crime risks related to the Client and the Client's financial activities.

Legal entities:

- personal data necessary to identify the representative(s) of the entity,
- personal data necessary to identify the natural person beneficial owners of the entity (hereinafter: "UBO(s)"),

- personal data necessary to verify the identity of the representative(s) / UBO(s),
- personal data necessary to verify existence of the right of representation of the representative(s),
- personal data of the UBO(s) necessary to determine the business and risk profile of the Client and to mitigate money laundering, terrorist financing or other financial crime risks related to the Client and the Client's financial activities.

The Data Controller will provide specific information on the exact scope of the data processed in the context of each customer due diligence process, given that this will depend on whether regular or enhanced customer due diligence is to be carried out in accordance with the AML Policy.

Legal basis of data processing

The legal basis for the processing of personal data in relation to the Customer due diligence process is Article 6(1)(f) of the GDPR (legitimate interest).

It is the legitimate interest of the Data Controller to apply CDD in certain circumstances in accordance with the Data Controller's AML Policy and in compliance with the applicable international and national legal standards in order to

- maintain the integrity and safety of the BOTS Platform,
- prevent the misuse of the BOTS Platform for the purpose of money laundering, terrorist financing, fraud or other financial crimes,
- comply with potentially applicable international and national legal standards (e.g. Directive (EU) 2015/849 – the 5th anti-money laundering Directive and the recommendations of the FATF [FATF- AML/CFT]),
- prepare the BOTS Platform to comply with requirements that will become applicable once the BOTS Group is granted its registration/license applications (ES, NL).

Playing an active role in fighting financial crimes, such as money laundering, terrorist financing, corruption, bribery, fraud, human trafficking, smuggling, or tax evasion, protects not only the interests of the Data Controller, but also the interests of the entire BOTS Platform, the Clients, and also serves the public interest.

Time period of processing personal data

All personal data related to the Customer due diligence process, including the copy of the documents and information which are necessary to comply with the Customer due diligence requirements are processed by the Data Controller for a period of five years after the end of the business relationship with the Client.

*****

Services provided by the Data Controller in connection with the use of the BOTS Platform

Intermediary services in connection with the exchange of Clients' fiat money to crypto and vice versa, and deposit and withdrawal orders

The Data Controller is providing an intermediary service to Clients which includes services to facilitate the exchange of Clients' fiat money to the respective cryptocurrency and vice versa and the execution of the deposit and withdrawal orders of funds from their BOTS Account.

The exchange of Clients' fiat money to the respective base cryptocurrency of the bot(s) the Client intends to use, and the exchange of Clients' crypto assets to fiat money, can be arranged via:

- as per the authorization to be granted by the Clients to the Data Controller, the Data Controller is able to facilitate the exchange of Clients' fiat money to the respective cryptocurrency on behalf of and for the benefit of the Clients
- through the Pay.nl platform, operated by TinTel BV (Jan Campertlaan 10 3201 AX, Spijkenisse, Netherlands) or
- via Holland Crypto (Gedempte oude gracht 45-47, 2011 GL Haarlem, Netherlands)

Withdrawal orders are executed through a financial service provider, JANUAR ApS, a company incorporated in Denmark, registered at Gothersgade 14, 4. sal, 1123 Copenhagen K, Denmark.

Purpose of the data processing

The purpose of the processing is to provide an intermediary service for Clients to facilitate the exchange of their fiat money to the respective cryptocurrency and vice versa and to execute the deposit and withdrawal orders of funds from the Client BOTS Account.

Processed personal data

The Data Controller processes the following personal data:

- personal data necessary to identify the Client,
- the amount of cryptocurrency exchanged and available for use on the BOTS platform,
- deposit and withdrawal history,
- IBAN number and other personal data specified by the financial service provider on a case-by-case basis when executing withdrawal orders.

Legal basis of data processing

The legal basis for processing is Article 6(1)(b) of the GDPR as the data are processed for the performance of a contract between the Client and the Data Controller.

The source of personal data

In connection with the exchange, the aforementioned service providers JANUAR ApS., TinTel BV. and Holland Crypto provide the Data Controller with data on the Client's fiat-cryptocurrency transfer history (i.e. the amount of cryptocurrency exchanged and available for use on the BOTS platform) or the amount of fiat money transferred from the Client's bank account to the BOTS Platform.

In connection with the execution of the withdrawal orders, JANUAR ApS. provides the Data Controller with data on the Client's withdrawal history (i.e. the amount of funds withdrawn).

Recipients of the personal data provided

The above-mentioned intermediary services involve the transfer of the following personal data to the relevant services providers, who act as independent data controllers when processing Clients' personal data:

In case Clients authorize the Data Controller to facilitate the exchange, the following personal data is transferred by the Data Controller to TinTel B.V through the Pay.nl platform:

- Full name of the Client,
- ID document,
- IP-Address

to Holland Crypto:

- personal data necessary to identify the Client,
- personal data necessary to contact the Client,
- personal data necessary to verify the identity of the Client,
- personal data necessary to determine the business and risk profile of the Client and to mitigate money laundering, terrorist financing or other financial crime risks related to the Client and the Client's financial activities.

In connection with the execution of the withdrawal orders the following data is transferred to

JANUAR ApS.:

- personal data necessary to identify the Client,
- IBAN number

The full scope of the data transferred to JANUAR ApS. in connection with the withdrawal orders is determined on a case-by-case basis by JANUAR ApS., over which the Data Controller has no discretion.

Time period of processing personal data

The Data Controller shall process the personal data until the expiry of the general limitation period set out in the Act on Protection against Legalization of Proceeds from Crime and Protection against Financing of Terrorism and on Amendments to Certain Acts, i.e. 5 years after the performance of the contract.

*****

Executing BOT Assignment orders of the Clients, recording data related to Clients' use of the BOTS Platform

By opening the account and accepting the GTC's of the Data Controller, the Client is granting the Data Controller the assignment to

- arrange the use of the bots the Client chooses to utilize at the cryptocurrency exchanges, and
- carry out administrative management actions related to the use of the bots (hereinafter "BOT assignment order(s)").

The granting of a BOT assignment order takes place when a Client indicates through the

BOTS Platform that they would like to ‘start a bot’, ‘add more funds to a bot’, or ‘stop a bot’.

The Data Controller keeps a digital record of all Bot assignment orders that have been granted by its Clients through the chosen bots.

The Data Controller also keeps a digital record and makes available to Clients, via the BOTS App, the Client’s investment strategy and the value of their investment through the BOTS Platform via their account which contains, wherever possible, a real-time digital display of the amount that each Client has invested through the BOTS Platform and their respective return, as well as further information about the bots available on the Bots Platform.

Purpose of the data processing

The purpose of the processing is to execute BOT Assignment orders of the Clients, and record data related to Clients’ use of the BOTS Platform.

Processed personal data

The Data Controller processes the following personal data:

- personal data necessary to identify the Client,
- IP address (regarding the track&trace of internal deposits),
- personal data related to the BOT assignment orders and the Clients’ use of the BOTS Platform.

Legal basis of data processing

The legal basis for processing is Article 6(1)(b) of the GDPR as the data are processed for the performance of a contract between the Client and the Data Controller.

Time period of processing personal data

The Data Controller shall process the personal data until the expiry of the general limitation period set out in the Act on Protection against Legalization of Proceeds from Crime and Protection against Financing of Terrorism and on Amendments to Certain Acts, i.e. 5 years after the performance of the contract.

Spinoza Caute Fund

In order to enable Clients to participate in the Spinoza Caute fund and provide related Client administration services, certain personal data may be shared with and processed by external parties which include but are not limited to:

Elite Fund Management B.V., (hereinafter "EFM") with statutory seat in Alkmaar, the Netherlands, registered address at Beursplein 5 (2A.07), 1012 JW Amsterdam, the Netherlands: EFM is acting as fund manager of the Spinoza Caute Fund and may provide different services such as portfolio management, compliance and risk management, administration regarding Spinoza Caute Fund.

IQEQ Financial Services B.V. (hereinafter: "IQEQ") with a statutory seat in Amsterdam, the Netherlands, registered address at Hoogoorddreef 15, 1101 BA Amsterdam, the Netherlands: provides different support services such as financial administration and administration of participants in the Spinoza Caute Fund.

Purpose of the data processing

EFM and IQEQ may process personal data to enable Clients to participate in the Spinoza Caute Fund and perform required actions relating thereto and/or provide services relating thereto (together: “Client Administration of Spinoza Caute”). Client Administration of Spinoza Caute may include but is not limited to: personal data for Client onboarding/identification and verification, Client risk classification, PEP screenings, ongoing client monitoring, transaction monitoring, processing Client deposits, processing instructions from Clients, processing /administrating client mutations, providing confirmations and/or overviews to clients, data necessary to mitigate risks money laundering, terrorist financing or other financial crime risks and all other services directly or indirectly relating to the before mentioned services/activities/duties. EFM and IQEQ may (sub-)delegate tasks and/or services.

Processed personal data

All personal data required for the Administration of Spinoza Caute as explained above, including but not limited to:

- Name, address, telephone number and email-address
- Data on ID (Identification Document, such as passport)
- Bankaccount number
- Instructions/confirmations/mutations from the Client (buy, sell, deposits, other)
- In case of a legal entity: all data on the register of the chamber of commerce and all personal data necessary to identify the natural person beneficial owners of the entity

Legal basis of data processing

Personal data are processed to comply with the contract with the client and/or comply with legal/regulatory obligations.

Time period of processing personal data

Personal Data will be processed until the expiry of the general limitation period, i.e. 5 years after the performance of the contract.

*****

Other data processing activities

1) Communication

Clients or other people interested in the service provided by the Data Controller (hereinafter collectively referred to as data subjects) can contact the Data Controller by sending a direct email, using the chat help on the website (https://www.bots.io/) or in the BOTS App or even by phone or by post, whether it's a request for information, a technical question, or any other subject.

The Data Controller, in connection with its services, also provides Clients the possibility to create a user account on the support website available at https://support.bots.io/ (hereinafter referred to as the "website"), where questions and requests related to the use of the service can be addressed directly to the Data Controller.

The creation of a user account requires prior registration. Registration can be initiated on the website by providing the necessary personal data. The system will automatically send a welcome email to verify the email address. At the first login, the Client will be required to enter a password, which shall be kept confidential at all times. In the event that, following the correct provision of the email address and password during the log-in process, the Client's login data has been disclosed to an unauthorised third party due to the fault of the Client, the Data Controller shall not be liable for any damage or harm resulting therefrom. Once the registration is completed, the user account is set up and the Client is free to edit it at any time and make personalised settings.

Access to the user account after registration:

- by entering the email address and password, or
- by using the Client's existing Facebook, Twitter, Google or Microsoft account.

In the case of logging in with a Facebook, Apple or Google account, the provider of that account will, depending on the account settings of the data subject, transfer the personal data necessary to identify the data subject to the Data Controller. For more information on logging in to other applications and services with each account and on the account setup

options, data subjects can find more information on the respective service provider's website:

Google:
https://support.google.com/accounts/answer/112802?hl=hu&co=GENIE.Platform%3DDesktop&oco=1

Facebook:
https://www.facebook.com/help/2230503797265156?helpref=faq_content

Twitter:
https://help.twitter.com/en/managing-your-account/connect-or-revoke-access-to-third-party-apps

Microsoft:
https://support.microsoft.com/en-us/account-billing/sign-in-to-your-accounts-using-the-microsoft-authenticator-app-582bdc07-4566-4c97-a7aa-56058122714c

The purpose of data processing

Purpose of data processing: communication, response to enquiries from the data subjects. The Data Controller uses all the data provided by the data subjects during the contact process solely for the purpose of the communication and the administration in the matters included in the message.

The purpose of the processing of personal data related to the creation of a user account is to provide a platform for Clients to directly address requests and questions related to the service provided by the Data Controller, while at the same time providing a personalised treatment of the requests submitted.

Processed personal data

Name, email address, alternatively phone number or postal address, as well as any other information provided by the data subjects during the communication with the Data Controller.

Mandatory data to be provided for registration of a user account are also the name and e-mail address of the Clients, however after registration, the Clients can voluntarily provide additional personal data in their user account and can access the activities carried out in the user account.

Legal basis of data processing

Where the request comes from a Client in relation to the service provided by the Data Controller, the legal basis for the processing of personal data is point (b) of Article 6(1) of the GDPR.

Otherwise, point (f) of Article 6(1) of the GDPR (legitimate interest) also provides the Data Controller a legal basis for data processing. It is a legitimate interest of the Data Controller, in case it is contacted in a matter, to process the personal data that are necessary for responding and resolving the given issue.

It is also a legitimate interest of the Data Controller to operate a support website where

Clients can directly address requests and questions regarding the service provided by the Data Controller and at the same time to manage the submitted request in a personalised manner.

The source of personal data

If the data subject logs in to the user account with an existing Facebook, Twitter, Google or

Microsoft account, certain personal data will be transferred to the Data Controller by Facebook Ireland Ltd, Twitter, Inc., Google Ireland Ltd. and Microsoft Ireland Operations Ltd.

The Data Controller has no control over the scope of the data transferred.

Time period of processing personal data

In the event of any kind of contract (agreement) is concluded between the Data Controller and the data subject, the Data Controller will process the personal data obtained in the course of the communication in relation to the contract in question.

If no contract is concluded between the Data Controller and the data subject following the pre-contractual processing, or if the communication is not related to a contract and the communication cannot have any future legal effect, the Data Controller will process the personal data obtained during the communication until the communication is finally terminated.

As for the user account, the data subject may delete the user account at any time. In such a case, the personal data related to the registration will no longer be processed by the Data Controller for this purpose. However, irrespective of the cancellation of the registration, data related to the handling of requests and questions submitted through the user account will be processed by the Data Controller in accordance with the provisions set forth in this point.

*****

Complaint handling

The Data Controller shall provide Clients with the opportunity to lodge complaints regarding the services of the Data Controller in accordance with consumer protection regulations.

Complaints are handled in accordance with the provisions of the AAct No. 108/2024 Coll. Act on Consumer Protection and on Amendments to Certain Acts (hereinafter referred to as the „Consumer Protection Act").

In the event of a verbal complaint, if the Client does not agree with the immediate handling of the complaint, or if an immediate investigation of the complaint is not possible, the Data Controller shall immediately take a record of the complaint and its opinion on the complaint.

The purpose of data processing

The purpose of data processing is the handling of complaints submitted by Clients in accordance with the provisions of the Consumer Protection Act.

Processed personal data

Pursuant to the Consumer Protection Act, in the event of a Client complaint:

- the name and address of the costumer,
- the place, date and form of submitting the complaint,
- the detailed description of the costumer's complaint, and the list of documents and evidence presented by the costumer,
- the Data Controller's statement of its opinion concerning the costumer's complaint, if the complaint can be investigated immediately
- the signature of the person preparing the report and the signature of the costumer, except if the oral complaint was submitted over the telephone or via another electronic communications service,
- the place and date of the report,
- the individual identification number of the complaint if the oral complaint was submitted over the telephone or via another electronic communications service.

Where the complaint or request is made by electronic means or by telephone, the Data Controller shall store the email address of the data subject in the case of the former and the telephone number of the data subject in the case of the latter, as specified in this notice.

Legal basis of data processing

The legal basis for data processing is the fulfilment of a legal obligation pursuant to Article 6 (1) (c) of the Regulation, which in this case means the fulfilment of the requirements of the Consumer Protection Act.

Time period of processing personal data

The Data Controller is obliged to keep the documents related to the complaint for 3 years in accordance with the Consumer Protection Act.

*****

Direct marketing (e-mail, SMS)

The Data Controller provides existing and potential Clients with information on news, updates, available new products, and services related to its services by electronic means in the form of an e-mail or SMS communication, depending on the subscription of the data subject.

The purpose of data processing

The purpose of data processing is to inform current and potential Clients about news, updates, new products, and services available, related to the services provided by the Data Controller.

Processed personal data

In the case of subscription to an SMS DM communication, the Data Controller processes the name and telephone number of the data subject, and in the case of subscription to an e-mail DM communication, the Data Controller processes the name and e-mail address of the data subject.

The sending of e-mail DM communication is carried out through the Braze CRM system, which allows the Data Controller to have access to the following data of the sent letters:

– the type of e-mail sent and the time of sending (day, hour, minute).

Legal basis of data processing

The processing of personal data is based on Article 6(1)(a) of the GDPR, i.e. on the data subject's consent.

Time period of processing personal data

Until consent is withdrawn. The data subject can unsubscribe from the newsletter at any time by clicking on the unsubscribe link in the newsletter automatically, or by sending an unsubscribe request to privacy@revenyou.io Consequences of failure to provide personal data The provision of personal data is voluntary.

*****

Customer experience surveys

The Data Controller carries out customer experience surveys by means of telephone enquiries, email and online surveys among the Clients for business development purposes, i.e., in order to evaluate customer satisfaction regarding its products and services. During the survey, Clients can voluntarily answer various questions and can make personal suggestions and comments on the products and services provided by the Data Controller.

The purpose of data processing

The purpose of data processing is to contact the Clients to carry out customer experience surveys for business development purposes, i.e., to gather personal feedback on the Data Controller's products and services.

Processed personal data

The name, telephone number and/or email address of the Client, as well as the answers given during customer experience surveys and any suggestions or comments made by the Clients.

Legal basis of data processing

The processing of personal data is based on Article 6(1)(a) of the GDPR, i.e. on the data subject's consent.

Time period of processing personal data

The Data Controller processes the personal data for the purposes set out in this point until the evaluation of the personal suggestions and comments made during the survey or until the final result of the customer experience survey is obtained, but no longer than 6 months.

Nevertheless, the data subject may withdraw the consent at any time by sending a request to the following address. privacy@revenyou.io. Consequences of failure to provide personal data The provision of personal data is voluntary.

*****

Maintenance and development of the BOTS App

As the developer and provider of the BOTS App, the Data Controller continuously analyses data generated by the use of the BOTS App to ensure continued development, enhancement of user experience and efficient operation.

The purpose of data processing

The purpose of data processing is to ensure continued development, enhancement of user experience and efficient operation.

Processed personal data

The relevant data generated by the use of the BOTS App.

Legal basis of data processing

It is the Data Controller's legitimate interest as the developer and provider of the BOTS App to ensure continued development, enhancement of user experience and efficient operation of the BOTS App, therefore the legal basis for data processing is Article 6(1)(f) of the GDPR.

Time period of processing personal data

The Data Controller processes personal data as long as it's necessary for the maintenance and development of the BOTS App.

*****

Competitions

The Data Controller organizes different types of competitions for its clients or other people interested in the service provided by the Data Controller (hereinafter collectively referred to as competitors). Competitors may participate in the competitions in accordance with the terms and conditions of the specific competitions (when applicable). Competitors may win different prices in relation to the competitions organized by the Data Controller.

The purpose of data processing

The purpose of data processing is to organize the competitions and contact the competitors who have won different prizes in relation to the competitions.

Processed personal data

The name, address, telephone number, and/or email address of the competitors, as well as the answers given during the competitions or comments made by the competitors.

Legal basis of data processing

The processing of personal data is based on Article 6(1)(a) of the GDPR, i.e. on the data subject's consent.

Time period of processing personal data

The Data Controller processes the personal data for the purposes set out at this point until the competition has been completed and answers, as well as comments made during the competition, have been processed or until the final result of the competition is obtained, but no longer than 6 months.

Nevertheless, the data subject may withdraw the consent at any time by sending a request to the following address. privacy@revenyou.io. Consequences of failure to provide personal data The provision of personal data is voluntary.

*****

THE DATA PROCESSORS ENGAGED BY THE CONTROLLER

The Data Controller uses the services of the following service providers:

- **BOTS Support Services B.V.** (Gedempte Oude Gracht 45 47, 2011GL Haarlem, Netherlands) – Contributes to the operation of the IT infrastructure of the Data Controller and provides different types of support services, such as HR, recruitment, marketing, customer support, IT support, IT development and other professional consulting background services to the Data Controller.
- **ComplyCube** (Crown House, 27 Old Gloucester St, London, UK, WC1N 3AX) – the developer and provider of the CDD software used by the Data Controller.
- **Certainly ApS** (Søtorvet 5, 1. th, 1371 Copenhagen, Denmark) – the developer and operator of the chatbot service used by the Data Controller.

- **Zendesk, Inc.** (989 Market Street, San Francisco, California 94103, United States of America) the developer or operator of the Zendesk customer service software used by the Data Controller.
- **Ask Nicely Holdings, Inc.** (1615 SE 3rd Avenue, Floor 3, Portland, Oregon 97214, United States of America) – the developer or operator of the AskNicely customer service software used by the Data Controller.
- **Braze, Inc.** (330 West 34th Street, 18th Floor New York, NY 10001, United States of America) the developer or operator of the Braze CRM software used by the Data Controller.
- **Daisycon B.V.** (P.J. Oudweg 5 1314 CH, Almere, FLEVOLAND Netherlands) – provides marketing services to the Data Controller.
- **SK AUDIT Kft.** (2837 Vértesszőlős, Templom utca 26., Hungary) – Performs accounting services for the Data Controller.
- **5CA International B.V.** (Stationsstraat 154, 3511 EK Utrecht, the Netherlands) – Provides Customer support services to the Data Controller.
- **Vonage** (Basisweg 10 1043AP Amsterdam, the Netherlands) – provides telecommunication services in relation to receiving the SMS required to obtain access to BOTS App.

The data processors may process the personal data of the data subject only for the purpose specified by the Data Controller and determined in the contract, in accordance with the instructions of the Data Controller, they have no independent decision-making right regarding data processing. The data processors have undertaken to maintain confidentiality and provided contractual guarantee for the protection of personal data obtained during the performance of their duties.

*****

TRANSFER OF PERSONAL DATA TO A THIRD COUNTRY

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country shall take place only if, subject to the other provisions of the GDPR, the conditions laid down in Chapter V of the GDPR are complied with by the Data Controller.

In case of engagement of the following data processors, personal data may be processed in a third country. In this case, data transfers take place on the basis of standard contractual clauses adopted by the European Commission, in which the data processors undertake to comply with the guarantees set out in Chapter V of the Regulation.

The standard contractual clauses concluded with the data processors are available at the following link:

- Zendesk, Inc.: https://www.zendesk.com/company/data-processing-form/
- Ask Nicely Holdings, Inc.: https://www.asknicely.com/data-processing-addendum
- Braze, Inc.: https://www.braze.com/company/legal/scc
  https://www.braze.com/company/legal/dpa

*****

THE RIGHTS OF THE DATA SUBJECT

Right to be informed

The data subject has the right to be informed with regard to the data processing, which right is observed by the Data controller by providing this privacy statement.

Data processing based on consent

In case the legal basis of any data processing is the consent of the data subject, they have to right to withdraw their consent to the data processing at any time. However, it is important to note that withdrawing the consent involves only the data whose processing has no other legal basis. In case there are no other legal bases, we delete the personal data finally and irrevocably after the consent is revoked.

The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

Right of access by the data subject

The data subject shall have the right to obtain from the Data controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;
- where possible, the planned period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the data subject is informed about their right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;

- where the personal data are not collected directly from the data subject, any available information as to their source;
- the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

If a request is made to rectify (modify) personal data then the data subject needs to prove the authenticity of the data to be modified. Additionally, the data subject must verify that the person requesting rectification is authorised to do so. This is the only way for the data controller to verify the authenticity of the new data before modifying it.

Please report any changes in your personal data to the Data controller as soon as possible, facilitating the legality of data processing and the enforcement of your rights.

Right to erasure ('right to be forgotten')

The data subject shall have the right to obtain from the Data controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws consent on which the processing is based, and where there is no other legal ground for the processing;
- the data subject objects to the processing and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing of personal data for direct marketing purposes;
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- the personal data have been collected in relation to the offer of information society services.

Right to restriction of processing

The data subject shall have the right to obtain from the Data controller restriction of processing where one of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

Right to object

If the legal basis for processing personal data is the legitimate interest of the Data controller (point (f) of Article 6(1) of the GDPR), or the processing is necessary for the performance of a task carried out in the exercise of official authority vested in the controller (point (e) of Article 6(1) of the GDPR), the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, including profiling based on the relevant provisions.

If the personal data of the data subject are processed for direct marketing purposes (i.e.: sending marketing e-mails), the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. If the data subject objects to the processing of their personal data for direct marketing purposes then such data can no longer be processed for that purpose.

Balancing test of legitimate interest

If the basis of processing personal data is in the legal interest of the data controller or third person as described in Article 6. Paragraph (1) Point f) of GDPR law, then according to (47) Preamble Article, and Article 5, Paragraph (2), the Data controller carries out a ’Balancing test of legitimate interest’ which can be obtained at privacy@revenyou.io email address.

Right to data portability

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to the Data controller, in a structured, commonly used and

machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

- the processing is based on consent of the data subject or on a contract according to Article 6 Paragraph (1) Point b) of the GDPR; and
- the processing is carried out by automated means.

PROCEDURES FOR ENFORCING THE RIGHTS OF DATA SUBJECTS

The above rights can be exercised by data subject by sending an electronic mail to this e-mail address: privacy@revenyou.io, or regular mail to the seat of the Data controller or in person at the seat of the Data controller. The data subject shall be informed about the measure taken in response to the request within 30 days. If we are unable to fulfil the request, we inform the data subject about the reasons of the rejection and the administrative and judicial redress rights of the data subject.

The rights of the deceased may be enforced within five (5) years by an authorized person who possesses administrative provisions, or a statement towards the data processor included in a public document or full probative private document. If multiple such statements exist at the same data processor, then the statement made the latest will prevail. If the subject has made no such legal statement, then a close relative - as defined in respective legislation - is still able to enforce certain rights of the deceased within five (5) years of death. These rights are defined in Article 16 (right to rectification) and Article 21 (right to object), as well as – if the data processing was unlawful during the life of the subject, or the purpose of data processing has ceased with the death of the subject – Articles 17 (right to erasure) and 18 (right to restriction of processing) of the GDPR. The close relative who exercises their right first will be entitled to enforce rights of the subject as set forth in this Paragraph.

THE RIGHT TO LODGE A COMPLAINT AND TO AN EFFECTIVE JUDICIAL REMEDY

In order to exercise their right to judicial remedy, the data subjects may seek legal action against the Data controller if the data subject considers that the Data controller or a data processor acting on behalf of or under the instructions of the Data controller is processing the personal data in breach of the provisions of laws on the processing of personal data or of binding legal acts of the European Union. According to Article 79 (2) of the GDPR proceedings against the data controller shall be brought before the courts of the Member

State where the data controller has an establishment, i.e., before the Bratislava-Capital Regional Court (Slovakia). The court shall deal with the case as a matter of priority. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has habitual residence.

Without prejudice to judicial remedy, according to Article 77 (1) of the GDPR every data subject shall have the right to lodge a complaint with the supervisory authority, in particular in the Member State of data subject's habitual residence, place of work or place of the alleged infringement (i.e. in Slovakia), alleging that the processing of personal data by the Data Controller has resulted in a violation of rights or an imminent threat thereof, or that the Data Controller is restricting the exercise of rights related to the processing of personal data or is refusing to exercise such rights.

The claim can be filed at the Hungarian supervisory authority at one of the below addresses:

Office for Personal Data Protection of the Slovak Republic

Address: May 1st Square 18, 811 06 Bratislava, Slovak Republic

E-mail: zodpovednaosoba@pdp.gov.sk

URL: https://dataprotection.gov.sk/