“TeamToolbox”

Regulations

[18.03.2021]

These Regulations (hereinafter referred to as the “Regulations”) specify the rules of using the Internet application “TeamToolbox” (hereinafter referred to as the “Application”) and the Services provided to Clients via the Application. Before a Client starts to use the Application, they should familiarise themselves with these Regulations as well as the rules of the Users who use the Application on the Client's behalf, provided therein.

Table of Contents:

I. General information

The supplier of the Application is AgileToolbox spółka z ograniczoną odpowiedzialnością (AgileToolbox sp. z o.o.) with its registered office in Warsaw (01-157) at Eustachego Tyszkiewicza 21, entered into the Register of Entrepreneurs maintained by the District Court for the Capital City of Warsaw in Warsaw, 12th Economic Division of the National Court Register, under the KRS (National Court Register) number: 0000365913, REGON (official business register number): 142578789, NIP (taxpayer’s identification number): 5272637352. Please note that when the phrase "we" is used herein, the reservation shall concern the Delivery of the Application. You can contact us at the following email address: hello@teamtoolbox.io.

II. Definitions

1. **Regulations –** these regulations, made available in the form which makes it possible for the Client to save, reopen and read it in any place at any time (according to the rules described below). Within the scope in which services are provided to the Client electronically, the Regulations shall

be the regulations referred to in Article 8 of the Act of 18 July 2002 on Providing Services Electronically (Journal of Laws of 2002 No. 144, item 1204, as amended). Appendix No. 1, i.e. the Agreement on Entrusting the Task of Data Processing, shall be an integral part of the Regulations as well as Appendix No. 2, i.e. The price-list.

2. **Application Supplier/Service Provider –** the entity specified in Clause I hereof, providing Services to Clients via the Application.
3. **Application –** Internet application, available at http://www.teamtoolbox.io/ and app.teamtoolbox.io delivered by the Application Supplier under the rules specified herein.
4. **Services –** services provided electronically to the Client via the Application by the Application Supplier, making it possible to exchange content, promote team cooperation, and build organisational culture based on the people who know, appreciate and motivate one another.
5. **Client** – natural person, legal person or organisational unit with no legal personality, running business activity and concluding the agreement on using the Services in connection with the business activity run. In order to avoid any doubt, the Service Provided indicates, that the parties to the agreement concluded under these Regulations can be only the persons who are not consumers within the meaning of Article 22(1) of the Civil Code (i.e. who are not natural persons making a legal transaction with the entrepreneur, which is not connected directly to their business or professional activity), or consumers within the meaning of consumer directives (directives the purpose of which is to protect consumers in various fields, such as e.g. consumer sale, distance contracts, unfair market practices etc.), as well as the regulations which implement them into the laws of particular Member States; the above shall not make it impossible for the persons from the Client's organisation only to use the Services (see the User below).
6. **User** – person authorised by the Client to use the Services provided to the Client by the Service Provider, who has the status of the Main Account Administrator, Moderator or Co-user (as decided by the Client).
7. **Main Account Administrator** – the User who:
   - concludes the agreement on providing Services on the Client's behalf, under the rules described herein (authorised to conclude the agreement);
   - is authorised to manage the Services in the scope of the configuration and day-to-day handling of the Account, including in the scope of inviting Users to use the Services on the Client's behalf, as well as to:
   - change the scope of the Services provided, used by the Client;
   - delete the Organisation Account.

   The Main Account Administrator can only have one Account. The function of the Main Account Administrator can be performed by the Client himself/herself.
8. **Moderator** – a Co-user holding the rights in the scope of the configuration and day-to-day handling of the Account, including inviting Co-users (provided he or she has been granted such rights) to use the Services provided as a part of the Application. The Moderator shall not be authorised, however, to delete the Organisation Account (only the Main Account Administrator shall be authorised to do that). The Main Account Administrator or other Moderator (provided they have permission to do that) shall grant the status and rights of the Moderator and shall be allowed to appoint more than one Moderator.
9. **Co-user –** the User who has accepted the invitation of the Main Account Administrator or Moderator to share the Organisation Account and gained access to the Services provided to the Client (on the Client's behalf) via the Application. The Co-user shall not and cannot be a party to the agreement concluded by and between the Client and the Service Provider.
10. **Organisation** – all Users using the Services on the Client's behalf.
11. **Organisation Account –** a collection of resources in the Application, making it possible to use the Services provided by the Supplier to the Client. The Organisation Account shall be created by the Main Account Administrator (who shall – the moment the Organisation Account is created – conclude an agreement on the Client's behalf based on the Regulations). The Organisation Account shall be made available to Co-users by the Main Account Administrator, so that they can use the Services as a part of the User's Account.

12. **User's Account –** an individual collection of resources within the Organisation Account, assigned to a specific User, which makes it possible for the User to use the Services provided by the Supplier to the Client.
13. **Messenger** – space in the User's Account, which makes it possible for Users to contact the Application Supplier directly, intended to report problems and make technical inquiries, connected with providing the Service to the Client (technical support). The Messenger shall not be used to solve problems or disputes between the Client and the User (e.g. regarding employment) or among particular Users – the Application Supplier shall be neither authorised nor obliged to take actions in this scope. For the Main Account Administrator, the Messenger can be used not only for the technical support of the Client, but also to exchange information connected with the provision of Services, including the payments for the Services, the scope of their provision and others.
14. **Price List –** information on the current charges for the Service licence, published on the website of the Service Provider of the Application, which constitutes an integral part of these Regulations (as their Appendix No. 2). A change of the Price List shall always constitute a change of the Regulations. Should the Client's registered office be located outside Poland, the charges shall be reduced by the amount of the VAT tax, and the invoice shall show the reverse charge clause.
15. **Credentials** – individual details, which make it possible for the User to access the Service via the User's Account, including the following:
    a) login – User's individual designation, assigned during the registration process, necessary to use the Service;
    b) password – individual sequence of characters created by the User and known by the User only, used to secure the access the Service.
16. **Knowledge Base –** source of information, which concerns detailed matters describing the functionalities of the Application, available at: www.help.teamoolbox.io. The changes made in the Knowledge Base (e.g. adding a new article) shall not be regarded as a change of these Regulation, unless they concern their provisions and could reduce the safety level of the Services provided. The Client should systematically familiarise themselves with the content of the Knowledge Base, it is suggested to do so before concluding the agreement (the access to the Knowledge Base is public).

III. Technical activities which constitute the procedure of concluding the agreement based on the Regulations

1. The Client shall conclude with the Application Supplier the agreement on providing the Service under the rules described herein. Read the Regulations before you start to use the Services.
2. The procedure of concluding the Agreement shall include the following actions:
    a) registration on the Service Provider's website: www.teamtoolbox.io by clicking the "REGISTER" button, and then providing forename, surname, company name, email address and password (the Service Provider requires that the password should include minimum 8 characters, small and capital letters, digits and special characters, and suggests that it should not be a dictionary entry e.g. "cat" or "dog"). Should the Client be an organisational unit with legal capacity (e.g. a legal person), the person authorised by the Client to conclude the agreement based on the Regulations shall register on the Client's behalf, and the said person shall be the Main Account Administrator (not a party to the agreement); the Main Account Administrator must provide true and current details of themselves and the Client;
    b) clicking the "NEXT" button;
    c) reading the Regulations (including the notification obligation clause – Clause XII below), and making the declarations that the Regulations have been read and accepted, and the declaration on granting the authorisation to act on the Client's behalf (by checking the checkboxes at the end of the document);
    d) clicking the "REGISTER" button, what generates email with the activation link;

e) clicking the "ACTIVATE" button, found in the email with the activation link;

f) clicking the "ACTIVATE" button on the Application website, where you will be redirected by the activation link, which ends the procedure of registering the Organisation Account for the first time.

3. The agreement on providing the Service to the Client by the Service Provider shall be concluded once the procedure of registering the Organisation Account for the first time ends. The procedure of registering the Organisation Account should be completed not later than within 24 hours of performing the action referred to in item 2(d) above.
4. The Regulations shall be made available before the Agreement is concluded, and then in the footer of the Application website. The Regulations shall be also sent to the Main Account Administrator's email address, provided during registration.
5. Should the Client suspect that they have not received the message referred to in item 2(d) above, the Client or the person acting on the Client's behalf should first check the SPAM folder in the interface of their mailbox. If the message went to the SPAM folder, the Client should move it to the Inbox, and then click the "ACTIVATE" button in order to finish the registration process. It may be impossible to click the "ACTIVATE" button when the message is still in the SPAM folder, as the button may be blocked (e.g. by an anti-virus programme). If there are any problems with the registration, the Client should contact the Service Provider. If you do not complete the registration procedure, you will not be able to conclude the agreement.

IV. Technical actions required to create a Co-user

1. In order to add Co-users to the Organisation, you should follow the following instructions. The Client acknowledges that Co-users (excluding the Main Account Administrator concluding the agreement on the Client's behalf according to Clause III above) should not register in the Application on their own and conclude this way the agreement on providing the Services. If a Co-user – other than the Main Account Administrator – completes the registration procedure described in Clause III hereof – they shall not join the Client's Organisation (create the User's Account). It also shall not be possible to combine separately registered accounts of several Organisations, which is why the instructions below should be followed.
2. The Moderator's rights shall be granted by the Main Account Administrator. The Moderator shall gain access to the Account using the Credentials once the rights are granted by the Main Account Administrator. Then, the Main Account Administrator or Moderator shall send an invitation to the Co-users. Further instructions on adding account co-users can be found in the Knowledge Base.
3. A Co-user can register the User's Account not later than within 7 days of the day they receive the invitation, according to item 2(d) above. Once this time limit expires – or the invitation is accepted – the activation link shall be deactivated.
4. While inviting Co-Users to the Organisation, the Main Account Administrator and the Moderator should enter the email addresses to generate the invitation with due diligence; a mistake in an email address and/or invitation sent to a person from outside the Client's Organisation might result in including that person in the Organisation and, consequently, to disclosing the content and personal data from the Application to unauthorised persons, which may violate trade secrets or other legally protected secrets (if applicable to a given Client) or cause the Client – who is the controller of the personal data of the Application Users – to violate personal data protection.
5. Invitations can be sent to any email address (of any domain). However, for safety reasons, it is recommended to send the invitations to join the Organisation to the Co-users to their emails in the company domain (if the Organisation has them), and to register in the Application using the email address in such a domain (address of the Main Account Administrator). If the Service Provider finds that there has been an attempt to invite a Co-user using their email address in a domain different from the domain of the Main Account Administrator (the email address they used registering in the Application), the Application will show the warning that a different domain has been detected. Once the registration is completed, the User can add an avatar and favourite

quote in the User's Account and set the hierarchy of motivators (see the descriptions of modules in Clause V below).

6. For safety reasons, Users should not disclose their credentials to third parties or send the received invitations to join the Organisation Account to other email addresses or other persons (outside the Organisation).

V. Type and scope of the services provided

1. As a part of providing the Services, the Application Supplier undertakes to provide paid access to the functionalities of the Organisation Account in the Application, described herein.
2. The functionalities of the Organisation Account shall comprise the following paid modules (described below in detail):
   a) **KUDO (Kudo Cards)** – makes it possible to send a virtual Kudo card (visible to the whole Organisation) with thanks or praise for the selected User – see items 3–7 below).
   b) **Happiness index** – makes it possible to assess your physical and mental state and your satisfaction with your duties and clients – see items 8–11 below.
   c) **Merit Money + Market** – makes it possible for Users to give points and exchange them for the awards provided by the Client (at the Client's sole discretion) – see items 12–20 below and free modules (subject to item 23 below).
   d) **Feedback** – makes it possible for a User to ask another User for a private opinion. The feedback given to a given User (and the request for the feedback) shall not be visible to other Users, unless the User themselves makes them available.
   e) **People + Teams** – makes it possible to create and view the list of Users in a given Organisation and to organise teams according to any criterion (e.g. a project).
   f) **Motivators** – makes it possible for a User to set a hierarchy of three values, which motivate them within the User's Account (from among the defined motivators such as: acceptance, curiosity, freedom, goals set, honour, expertness, order, strength, relations, status) – visible to other Users.
   g) **Diary –** makes it possible for a User to add an entry – within the User's Account, Team (Teams) or Organisation, including word content (entry subject and content) and added pictures/films, making it possible for other Users to interact (comments, likes for the entry).
   h) **Wall –** makes it possible for a User to add an entry – within the Team or Organisation, including word content (entry subject and content), hashtags (identifying topic related to the entry) and added pictures/videos, making it possible for other Users to interact (comments, likes for the entry).
3. Kudo Cards shall make it possible to do the following:
   a) choose one of six available motifs of cards: "Well done", "Victory", "Thanks for help", "Great Idea!", "Power", "Awesome";
   b) choose the User who will be the addressee of the card by clicking the @ button, and then choose from the list of Users from a given Organisation;
   c) choose a hashtag from among the ones available for a given Organisation or create your own hashtag by clicking the # button, and then to choose or enter the hashtag the User wants to use on their card;
   d) write anything on the card, subject to Clause IX item 2 below;
   e) send the card by clicking the "send" button.
4. The cards can be sent anonymously within the Organisation. In order to do that, the User should select the "anonymous" option before sending the card. Choosing the said option shall not make it impossible to disclose the User's identity to the addressee of the card under the rules resulting from the laws (according to the Client's decision) – the Main Account Administrator shall see the details of the Users sending a card with the "anonymous" option selected.
5. The User acknowledges that the Cards sent shall be visible to other Users within the "Kudo wall". Apart from that, the User shall be able to see the cards they sent in the "Sent" tab, and the cards they received in the "Received" tab.

6. The Application Supplier shall not be the initiator of the data transfer as a part of sending the cards, they shall not choose the recipient of the transfer or choose and modify the information included in that transfer. The Application Supplier shall only make available appropriate technical solutions, which shall make it possible to send the cards under the rules described above, and the Application Supplier shall not be liable for the legality of the actions undertaken by the Client or the User from the Client's Organisation. The Client and User acknowledge that sending the cards which show offensive content, infringe personal rights or are illegal for a different reason (e.g. regarded as SPAM within the meaning of the Act on Providing Services Electronically – in the case of cards sent outside the Organisation) is illegal and can entail legal liability of the Client or the User.
7. The assessment within the Happiness Index module shall be made according to the scale and descriptively.
8. The assessment according to the scale shall be made by answering 3 questions in the scale from 1 to 5 (1 shall be the lowest level of satisfaction and 5 shall be the highest one). The User shall make their assessment by answering demonstration questions (they can be edited by the Main Account Administrator or Moderator with authorisation in this scope):
   - Are you happy in your organisation?
   - Are you happy with your duties?
   - Are you happy with the work with the present client and your situation?

   The descriptive assessment shall be made by answering the open question defined by the Main Account Administrator or Moderator.
9. On the „Happiness Index" tab, which is visible to the whole Organisation, Users can view the average mark from everyday answers to the questions of all Users (according to the scale), divided into monthly or weekly periods.
10. The Users can also check the marks of others – by their forename, surname, email, skills or teams. It shall be also possible to search people by the mark others have given.
11. Within the Market module, a User – once they join the Organisation – shall receive a pool of points specified by the Main Account Administrator, intended to be given to other Users (Points to Distribute). The Points to Distribute shall be only intended to be given to other Users; a User shall not be able to retain them for themselves, and the points which are not distributed shall be lost. The default name of the Points to Distribute shall be "coffee beans" – the Main Account Administrator shall be able to modify the name, look and number of the points granted at their own discretion.
12. Apart from granting the Points to Distribute on joining the Organisation, each User shall receive a pool of points to be distributed with the frequency selected by the Main Account Administrator.
13. Users can give one another the Points to Distribute received as thanks for e.g. tasks completed or help received; however, the criteria for giving the Points to Distribute shall not be determined top-down – the User shall decide on their own who they will give their points to and how many points the person will get.
14. The points received by a User from other Users shall constitute a separate category (Points to Spend) – they do not sum up with the Points to Distribute, and the User shall not be able to change the Points to Distribute, which have not been given to another User, into their own Points to Spend. The default name of the Points to Spend shall be "coffee cups" – the Main Account Administrator shall be able to modify the name, look and the number of the points granted at their own discretion.
15. The points shall be given analogously to sending the Kudo Card. A User shall choose the person who will get the points (choosing them from the list by clicking @) and the number of points (by selecting "+"), and can add a hashtag (#) and write e.g. what the points are given for (items 3(b) to 3(d) above shall be applied accordingly).
16. The Main Account Administrator can give any User any number of Points to Spend and any number of the Points to Distribute. It is not possible to take back the points given.

17. The Points to Spend received from other Users can be exchanged for the awards provided by the Client (at the Client's sole discretion).
18. The Points can be also given for the (individual and group) projects created by the Organisation. A project shall be created by choosing its type, adding its name and description, duration and the number of points required to support the project.
19. The points collected and received within the Market module shall not be the means of payment within the meaning of the Act of 27 July 2002 – Currency Law, or any other applicable laws. They cannot be also exchanged for their cash equivalent.
20. An element of the Services provided (information ordered) shall be also the receipt of the notifications of the User's activeness in the Organisation to the email address provided on joining the Application. A User shall be able to opt out of receiving the notification in the "Notifications" section in the User's Account.
21. The Application Supplier can introduce a payment for the modules listed in items 2(d) to 2(h) above, under the rules specified in Clause VI below.

VI. Versions of the service and payment terms

1. The Service Provider shall provide the Services in the Trial Version (free demo) and Premium Version, i.e. a paid version, which shall require the Client's authorisation (and providing additional details) for cyclical i.e. automatically renewed charging of the Client's account with a given amount through the agency of an outsourcing company (Braintree – company connected with PayPal), based on the rules of providing services specified by this entity. The Client shall be redirected to that payment operator's website, where they shall be able to read the operator's regulations.
2. The Trial Version shall be activated automatically once the registration is completed, according to Clause III item 2 above, and the activation of the Premium Version shall require actions of the Main Account's Administrator, performing on the Client's behalf the activities referred to in item 6 above.
3. The Organisation Account in the Application can be created and used free of charge for the period of 30 days, counting from the day of registering the Organisation Account (Term of the Trial Version). The Term of the Trial Version can be extended by the agreement of the Parties (the Client and the Service Provider).
4. Within the Trial Version, all the modules from the available functionalities of the system (described above in Clause V) shall be activated by default. If within the term of the Trial Version, the Main Account Administrator activates the Premium Version according to item 6 below, the choice of the modules within the Premium Version shall be effective once the term of using the Trial Version ends.
5. Within the Trial Version, the Main Account Administrator can add unlimited number of Users.
6. The Client shall be able to activate the Premium Version for the payment made for each settlement cycle of the term of the Premium Version (payable in arrears). In order to do this, they need to provide payment details via Braintree (external payment operator) and follow the instructions of Braintree to finalise the transaction. The regulations of Braintree can be found at: https://www.braintreepayments.com/pl/legal.
7. Within the Premium Version's price is on the range of selected modules as stated in Appendix no. 2.
8. The settlement period shall be a month, understood as 1 calendar month. The settlement period shall start once the transaction referred to in item 6 above is finalised.
9. The agreement on providing the Services in the Premium Version shall be concluded for an indefinite term, which means that the charge for using the Services in the Premium Version shall be collected when each subsequent settlement period of the term of the Agreement commences.
10. Should any of the paid modules be turned off, e.g. the KUDO module, all the functionalities on the Organisation Account connected with this module shall be inactive.
11. The Application shall also display the information on the number of days remaining until the end of the Trial Version.

12. The Main Account Administrator shall be able to check the following in their account:
    a) dates and amounts of the payments made (history of payments);
    b) dates and amounts of future payments – for subsequent settlement periods.

13. The Client can buy the Premium Version both within the period of using the Trial Version as well as directly after the Trial Version expires. Should the Client decide to switch into the Premium Version before the expiry of 30 days from the date of creating the Organisation Account (within the term of the Trial Version), the Premium Version shall not be activated until the end of that period (until the Trial Version ends; the charge also shall not be collected automatically until the Trial Version ends). After the first unsuccessful attempt to charge the Client's account, the Organisation Account may be blocked. Once the Organisation Account is blocked, the Client can change the payment method or contact the Service Provider. Within this time, another attempt to collect the amount due may be made.
14. After 30 days of the date the Organisation Account is blocked as described in the paragraph above – if the Client's account is not charged or the amount due is not paid another way – the Service Provider may terminate the agreement immediately (sending a declaration to such effect to the email account of the Main Account Administrator), as a consequence of which the Organisation Account shall be deleted.
15. If the Client does not purchase the Premium Version, the agreement on providing services shall be terminated upon the expiry of the term of the Trial Version (30 days). Once this term ends, you shall be logged off from the Application. The Client shall be given the possibility to buy the Premium Version; should the Client fail to purchase it within 30 days of the end of the Trial Period, he shall be no longer able to log into the Application, and the Organisation Account (and the Users' Accounts linked to the Organisation Account) shall be deleted. The Client shall be also able to delete the Account manually.
16. Should the Client opt out of the service within a settlement period, no reimbursement for the unused period of providing services shall be possible. If the Service is blocked immediately due to a significant breach of the terms and conditions of the Regulations or the Polish laws, no charges for the service, which have been already paid by the Client, shall be reimbursed. If more licenses are ordered during the billing period, the fee will be charged only from the new billing period. Accordingly, in the case of limiting the number of users, the fee will be reduced from the new billing period.
17. The Service Provider shall not reimburse the charges collected by the Braintree service for the transactions requiring currency conversion. Subscription shall be settled in EURO only, based on the regulations of Braintree.
18. The invoice for the Service shall be generated by the Application Supplier based on the details which were provided when the Service was ordered, such as the following:
    a) full name of the Organisation and the legal form of the business run;
    b) address;
    c) NIP (taxpayer's identification number);
    d) EU VAT number (in the format which meets the requirements of the transactions made within the intra-Community market).
19. The Main Account Administrator undertakes to provide complete invoice details, in accordance with the actual state. The Main Account Administrator accepts that the invoice will be issued without their signature. The invoice shall be sent to the email address of the Main Account Administrator within 7 working days of the end of a given settlement period.

VII. Technical requirements for the functionality and interoperability of the Application

1. In order to properly use the Services covered by these Regulations, provided via the Application, you should have a device which works properly and has Internet access.

2. The device should have an unmodified, factory installed version of the operating system i.e. Windows (Vista or any subsequent version), Mac OS X (every version from 10.1), Android 6.0 or higher, iOS 11.0 and higher.
3. You should use the Google Chrome browser (Mac or Windows) in the version 78 or any subsequent one. Browsers supported: Firefox, Safari, Opera – however, using them is not recommended as some functionalities of the Application may work incorrectly.
4. In order to work properly, the Application needs JavaScript enabled in the browser. The browser must accept cookies and pop-ups must be enabled.
5. Recommended resolution of the device screen: 1440 x 900 or higher.
6. Supported resolution of the device screen: 1280 x 800 or higher for dektop PCs, for mobile devices 640x360 or higher.
7. The Application Supplier shall not guarantee faultless operation of the Application if the device does not meet the above criteria.

VIII. Licence and copyright

1. The Application uses a computer programme from the Application Supplier.
2. The Client shall be authorised to grant access to the Account to the number of Users specified in accordance with Clause VI item 5 above, and then to use it in the manner specified in these Regulations and the provisions of the Act on Copyright and Related Rights (Journal of Laws of 2016, item 666, as amended) and other commonly binding laws.
3. Both the Application itself and its particular elements, trademarks and other labels and content contained therein, shall be protected under the commonly binding laws, including the Act on Copyright and Related Rights (Journal of Laws of 2016, item 666, as amended), the Act on Industrial Property (Journal of Laws of 2013, item 1410, as amended) and the Act on the Protection of Databases (Journal of Laws of 2001 No. 128, item 1402, as amended).
4. The licence to use the Application, referred to in these Regulations, shall be a non-exclusive and non-transferable licence, granted only in order for the Client to use the Application as a part of the Services covered by these Regulations, with no right to sublicense the Application, distribute it publicly or offer it commercially (hereinafter referred to as the "Licence").
5. The licence shall be limited in time; it shall be granted for the period of using the Application by the Client, according to these Regulations.
6. The Licence shall be granted by the Application Supplier for the computer software found in the Application and other works constituting parts of the Application, with regard to which the Application Supplier is entitled to grant the licence, and the Client must be granted it in order to be able to use the Application. The Licence shall authorise the Client to use the Application within the following fields of use:
   a) multiplying the Application in the memory of the Client’s device and other devices of the Client which meet the technical requirements indicated in Clause VII, and
   b) using the Application for its intended purpose described herein, including storing in the memory of the Client’s device and other devices of the Client which meet the technical requirements indicated in Clause VII, and displaying Application elements on the screen of the Clients device and other devices of the Client which meet the technical requirements indicated in Clause VII.
7. Translating or adjusting the Application, changing its layout or introducing any changes in the Application, including obtaining or changing and modifying the source code, including the reverse engineering of the Application both in full and in part, shall not be covered by the licence granted by the Application Supplier, which shall not exclude those rights of the user of the computer programme which cannot be limited under the law.

IX. Terms and conditions of providing services

1. The Client and any person using the Application on the Client's behalf (by their invitation) must observe these Regulations and refrain from any activity which could disturb its proper operation, including in particular the Client cannot – neither on their own nor with the help of third parties – bypass or brake the security systems of the Application or influence the Application negatively, damaging or overloading it.
2. The Application must not be entered illegal information or information which is contrary to the principles of morality. Entering the pictures which violate the law – among others pornographic in nature – and pictures which are contrary to the principles of morality is prohibited.
3. Moreover, the Application must not be used to contact third parties in a manner which is illegal or contrary to the principles of morality, including in particular it must not be used to send the unsolicited commercial communications within the meaning of the Act on Providing Services Electronically (Journal of Laws 2002 No. 144, item 1204). In particular, the Service Provider shall not be liable for using the Kudo Cards module to send the trade information within the meaning of Article 10 of the Act on Providing Services Electronically (Journal of Laws 2002 No. 144, item 1204).
4. The Client and each person using the Application on the Client's behalf shall be liable for their actions connected with using the Application and for the content (texts, pictures etc.) entered in the Application.
5. Should the Client's use of the Service Provider's Services be at variance with the Regulations or the laws, the Service Provider reserves the right to temporarily block the access to the Account or terminate the agreement on providing the Services without notice of termination.

X. Liability

1. The Application Supplier must provide their services with no defects; should the provision of those services be defective, the Application Supplier shall be liable within the scope of the Service provision, including in particular with regard to physical or legal defects. The Application Supplier's liability shall be limited to the amount of the price for the Services paid by the Client, excluding intentional fault and possible damage caused to a person.
2. The Application Supplier shall be liable towards the Client for the Services provided to the Client via the Application within the scope specified in these Regulations and the laws, which shall not prejudice the liability of the Client of the Application towards Users and third parties connected with the activity of Users, Moderators and the Main Account Administrator based on the commonly binding laws.
3. The Application Supplier shall not be liable for the following:
   a) Users' actions or non-feasance done using the Application;
   b) User's actions or non-feasance towards Users, including in particular connected with ensuring that their personal data are processed in accordance with the law as a part of making it possible for them to use the Application (e.g. within the scope of providing the legal basis for processing their data, meeting the notification obligation and the obligations connected with controlling their personal data by the Client);
   c) content placed by the Client or Users in the Application;
   d) incorrect operation or no operation of the Application resulting from a change in the Application or the operating system of the Client's device, introduced intentionally or accidentally by the Client or other entity acting for the Client in any form and based on any legal or actual relation, who at the same time is not the entity authorised by the Application Supplier to introduce such changes.
4. Apart from other events indicated in these Regulations, the Application Supplier shall not be liable for the following:
   a) inability to use the Application due to circumstances which are not the Service Provider's fault, including in the event of force majeure;

b) intentional or accidental use of the Application by the Client which is at variance with these Regulations or the law;

c) intentional or accidental problems or technical difficulties connected with the operation of the Client's device (both the equipment and the software of the device, including the operating system), which make it difficult or impossible to use the Application or the services offered via the Application;

d) failure or incorrect operation of the Application resulting only from the incorrect use of the Client's device (both the equipment and the software of the device, including the operating system) or incorrect configuration of the software of the said device;

e) intentional or accidental actions (including from a distance) aimed at the Application Supplier or the Client, the equipment of the Application Supplier or the Client (including all devices), or the software and technological environment of the Application Supplier or the Client, done by any third party without the Application Supplier's knowledge or consent.

f) no access to the Internet on the Client's device, limitation of the access or its proper operation;

g) using the Application by the Client on the device which does not meet the technical requirements indicated in Clause IV hereof.

5. Subject to items 6 and 7 below, the Application Supplier shall not be obliged to check the Organisation Account paying special attention to the data and content which are transferred, stored or made available by them.
6. If an official notification or reliable information on the illegal nature of the content entered is received, or on the correspondence sent from the Organisation Account, including User's Account, or activity connected therewith, the Application Supplier shall make it impossible to access these data immediately by deleting them. A reasonable misuse may particularly concern the breach of personal rights, including the right to privacy and protection against unwanted communication, or the breach of the intellectual property rights, patents, trademarks, trade secrets and other rights.
7. The misuse referred to above can be reported to the email address: hello@teamtoolbox.io.
8. The Service Provider shall make efforts to ensure the Client has uninterrupted access to the Application on the level of 97%.
9. The Service Provider shall retain the right (with no reduction of the charge paid by the Client) to make temporary breaks in the operation of the Service for maintenance, repair or updating and developing of the Application, without the need to send announcements in advance. The information on the works performed shall be presented, whenever possible, in the form of announcements made directly to Users (among others on the User's Account, email to Users).
10. If a third party (including a User) lays a claim against the Service Provider for a breach of third party rights or binding laws, or if proceedings (including criminal or administrative proceedings) are initiated in connection with providing the Services via the Application in the scope in which, according to this Agreement, the Client is liable – both towards Users and third parties – the Client shall release the Service Provider from the obligation to satisfy such a claim, and shall cover any duly documented damage sustained by the Service Provider in connection with the said claim, lawsuit or proceedings, adjudged in a legally final and valid court judgement or final administrative decision, including the legally final and valid costs of the proceedings and legal costs as well as the equivalents of damages, penalties imposed (including administrative and legal penalties) or fines, including the ones imposed on the members of the management board or employees of the Client, or the costs of enforcing final administrative decisions by the Service Provider. Should the Service Provider learn of such claims or proceedings, the Service Provide shall inform the Client immediately and make it possible for the Client – in accordance with the law – to enter the proceedings so that the Client can defend their rights.
11. If a third party brings an action against the Service Provider (or makes requests towards the Service Provider another way) for a breach of the rights of that person or third parties or a breach of the binding laws in connection with the actions of the Client or Application Users using the Application on the Client's behalf, the Client undertakes to enter the proceedings pending

immediately as the defendant or – should such entering prove impossible – to make an auxiliary intervention for the Service Provider at any reasonable request of the Service Provider.

XI. Complaint procedure

1. Complaints regarding the operation of the Application and the Services provided via the Application can be reported to the Application Supplier at hello@teamtoolbox.io.
2. For the complaint to be considered as promptly as possible, it should describe the reason for which it is filed as well as the date and time the reason occurred.
3. The Application Supplier shall consider the complaint and inform the Client immediately once it is considered, not later than within 30 days from the day the complaint is received.

XII. Privacy policy and personal data protection

1. The Service Provider shall be the personal data controller of the:
   ➔ Client, who is a natural person running business activity, and
   ➔ the Main Account Administrator – within the scope of the data necessary to enforce their rights specified in these Regulations.
2. The personal data of the Client, i.e. the party to this agreement, and of the Main Account Administrator acting on the Client's behalf, shall be processed first of all to conclude and enforce this agreement. Basis of processing the personal data of the party to the agreement who is a natural person is article 6(1)(b) of GDPR in conjunction with Article 22(2)(a) of GDPR. Legal basis of processing the data of the Main Account Administrator is Article 6(1)(f) of GDPR i.e. legitimate interests pursued by the controller.
3. In connection with the agreement concluded, both at the stage of concluding the agreement (registration in the Application, purchase of the paid services) and the stage of its enforcement (giving notice of its termination when no payment has been made or the paid services are not bought within the time limits provided in the Regulations), the automated decision-making may occur within the meaning of Article 22(1) of GDPR. Such automated decision-making shall be necessary to conclude and enforce the agreement pursuant to Article 22(2)(a) of GDPR. The decisions shall not be based on the special categories of personal data referred to in Article 9(1) of GDPR. If the Client does not agree with the decision made, they shall have the right to contact the controller at the email address provided below.
4. Personal data can be also processed:
   - to pursue, determine or defend the claims connected with the enforcement of the said agreement -> basis of processing: Article 6(1)(f) of GDPR i.e. legitimate interests pursued by the controller;
   - for direct marketing of the Service Provider's goods or services for the term of the agreement -> basis of processing: Article 6(1)(f) of GDPR i.e. legitimate interests pursued by the controller);
   - to ensure the safety of the Application and improve the quality of the Application -> basis of processing: Article 6(1)(f) of GDPR i.e. legitimate interests pursued by the controller);
   - to fulfil the obligations resulting from the laws, including the statutory liabilities -> basis of processing: Article 6[1][c] of GDPR – data controller's obligation;
   - of exercising the rights of the persons whom the data concern, indicated most of all in Chapter III of GDPR -> basis of processing: Article 6[1][c] of GDPR – data controller's obligation;
5. In order to conclude and enforce the agreement, personal data can be collected from the Central Registration and Information on Business, National Court Register and other public registers.
6. The data shall not be made available to anyone, unless it is necessary to enforce this agreement (based on Article 6[1][b] or 6[1][f] of GDPR).

Data recipients:

- Braintree for payment purposes ➔ personal data will transfer data to countries outside the European Economic Area and Switzerland, including the United State. The security and legality of the transfer is ensured by standard contractual clauses. More information:

  https://www.braintreepayments.com/assets/Braintree-PSA-Model-Clauses-March2018.pdf

- Google with the aim of statistical analysis within Google Analitycs service ➔ as part of the service provided, data may be transferred outside the EEA and Switzerland, mainly to the United States. Google participates uses standard contractual clauses. See. more:

  https://support.google.com/analytics/answer/3379636?hl=pl

  https://privacy.google.com/businesses/processorterms/mccs/

- Amazon. In order to host the Application and the database (server location: Ireland), as part of the service provided, data may be transferred to the USA and Switzerland. The data is physically stored in Ireland. According to the entrustment agreement, data may be transferred in exceptional circumstances. Should data be transferred, the basis will be standard contractual clauses of the European Commission:

  https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

  https://www.amazon.com/gp/help/customer/display.html/ref=hp_left_v4_sib?ie=UTF8&nodeId=202135380

- Intercom in order to provide Messenger ➔ personal data may be transferred to the USA and Switzerland as part of the service provided, based on standard contractual clauses.

  More information about transfer:

  https://www.intercom.com/help/pricing-privacy-and-terms/data-protection/how-intercom-complies-with-gdpr

- Isolution sp. z o.o. to support the implementation of the Services (including the development of Application's functionalities).

  You can get more information about data transfers by contacting us.

7. The Client (if the Client is a natural person) or the Main Account Administrator can request:
   access to data, including their copy,
   request that the data be transferred,
   rectified or deleted,
   that their processing be restricted.

   The legitimacy of the request shall be assessed by the Client based on the premises of GDPR.

   A complaint can be also filed with the supervisory authority (President of the Personal Data Protection Office).

8. The entities listed in item 7 shall be also entitled to object (when processing takes place pursuant to Article 6[1][f] of GDPR).

9. Personal data shall be deleted or made anonymous to the maximum extent possible after the expiry of the limitation period of possible claims connected with enforcing this agreement (including statutory liabilities), including in particular the claims resulting from the process of concluding and enforcing this agreement, statutory liabilities. Personal data can be deleted or made anonymous earlier if an effective objection is made.
10. The data shall be provided voluntarily, however, they shall be necessary to achieve the above mentioned purposes.
11. In any matters concerning data protection, contact us at the Service Provider's address or at the email address hello@teamtoolbox.io.
12. In order to avoid any doubt, the parties expressly agree that the Service Provider shall not be the data controller of the categories of people different from the ones specified in items 1 and 2 above, including in particular the Service Provider shall not control the data of the Co-users invited by the Client to use the Application (shall not decide on the purposes and manners of processing their personal data). The Client, who is the controller of the data of the Co-users invited by the Client to the Application (who are most often the Client's employees) shall be liable for ensuring that their data are processed in accordance with the law (including in particular that a proper legal basis is provided and the notification obligations are fulfilled, etc.).
13. In the scope of the Co-users' personal data (indicated in item 11 above), the Client shall entrust the Service Provider with processing the Co-users' personal data – in accordance with Appendix No. 1 hereto.
14. Considering item 12 above, the Service Provider shall be neither authorised nor obliged to respond on the Client's behalf to the requests of Co-users regarding the processing of their personal data by the Client (data controller), including the requests made via the Messenger, unless the Service Provider and the Client agree otherwise.
15. If the Client wants to use a processing entity, including the entity recommended by the Service Provider (e.g. the provider which offers a plugin), the Client shall be liable for ensuring that the law is obeyed in this scope, including in particular for choosing the entity which can guarantee that the right technical and organisational measures are implemented, so that the processing can meet the requirements of this GDPR and protect the rights of the persons whom the data concern, and for concluding an agreement with that entity (if applicable).

XIII. Cookies on the website of the Application

1. The website of the Application can process the following data, which mark the manner in which the persons visiting the website uses it (the so-called operational data):
   a) ID assigned to the person browsing the website;
   b) symbols which identify the end of a telecommunications network or ICT system (type of device, operating system, Internet browser) used by the Internet user;
   c) information on starting and finishing each use of the website and the scope of this use. The operational data listed above shall not be linked with such information as forename and surname, email address and other data, which make it possible to identify easily the person visiting the website.
2. The processing shall not be also used to profile the persons visiting the website.
3. The processing of the above information can be connected – yet does not necessarily have to be connected – with installing cookies or similar technologies in the end device used to display the website (see the information below in this scope). If the cookies mechanism is used, the operational data can include the information described below – collected by those files.
4. The operational data listed above may be the personal data within the meaning of GDPR (General Data Protection Regulation 2016/679) –> if the above mentioned information is qualified as personal data, then the controller's contact data and the information on the data subject's rights have been provided in Clause XII items 4–8 above, which shall be applied accordingly.
5. The processing of the above categories of data shall be necessary to maintain the website and ensure its proper quality, i.e. for the statistical purposes resulting from the legally legitimate

interests pursued by the controller (Article 6(1)(f) of GDPR) –> which makes the following important and necessary:

- analysing the preferences of Internet users and using the results of the analyses to improve the quality of the website;
- log files can be analysed occasionally in order to determine the following: which browsers are used by the persons visiting the website; which tabs, sites or subsites are visited or browsed the most or the least frequently; if there are no errors in the website structure;
- preventing unauthorised access to the website and distribution of malicious codes, stopping 'denial of service' attacks, and preventing damage to computer and electronic communication systems.

6. Based on the above information, statistics can be made, which shall not, however, include any information, which identifies or makes it possible to identify the person visiting the website. The website of the Application shall only use the cookies necessary for its proper operation, including for analysing and monitoring the traffic on the website (among others Google Analytics). For this purpose, the website shall also use the so-called operational data.
7. Through cookies, the website of the Application can store or get access to the information which is already stored in the device used to display it:
   - for the purpose and only in the scope necessary to display it. For this purpose, the website can use session cookies, which shall be installed so that the website can be displayed properly, and only until the end of a browser session (i.e. for the period for which the website is displayed in a browser).
   - Upon the consent of the person visiting the website, the so called cookies of third parties (partners) i.e. Google Analitics can be installed so that the preferences of Internet users can be analysed and the results of these analyses can be used to improve the quality of the website; the following data can be collected and analysed: number of users and sessions, duration of sessions, operating systems, models of devices, geographical data, starting / opening the application for the first time, application updates, shopping in the application –> more information: https://support.google.com/analytics/answer/6318039?hl=pl. Based on that, the following statistical reports are made or can be made: https://support.google.com/analytics/answer/2799357?hl=pl.
8. Such information as forename, surname or email address shall not be collected by the operator of this website via the Google Analytics tool. They shall not be compared with other information in order to identify the person visiting the website.
9. The consent to use cookies shall be granted in the settings of the browser on the User's device (Article 173(2) of the Telecommunications Law).
10. The installation of cookies can be disabled or limited in the browser.
11. The Internet browser of a User will usually allow to store cookies in the Users end device be default. The User can change the settings in this scope.
12. An Internet browser also makes it possible to delete cookies. It is also possible to block cookies automatically. Detailed information on this subject can be found in the Help section or documentation of the browser used.
13. The information stored and accessing this information shall not cause configuration changes in the User's telecommunications end device and the software installed in the said device.
14. The operational data listed above shall be stored for 2 years from the date they are obtained.

XIV. Termination of the agreement, deleting the account

1. The Main Account Administrator, acting on the Client's behalf, can give up the Account (terminate the agreement on providing the Service) at any time, subject to other provisions of the Regulations.

2. The Main Account Administrator or Co-user, who is the Client's employee, acknowledge that the Client shall be entitled to block the access to the User's Account and delete it at any time, and the User cannot expect that the access to the User's Account is restored without the Client's consent (this shall not include restoring the data deleted from the Account).
3. If the Account is closed by the Main Account Administrator, the Organisation Account shall be deleted permanently and the access to all the information and content found in the Application shall be deleted. The process of deleting the Account shall be irreversible and shall require the following steps:
   a) the "Administration" tab has the "Delete organisation" tab (available to the Main Account Administrator only);
   b) deleting the Organisation Account, the Main Account Administrator shall confirm this action by providing the password to the Account;
   c) completing the actions performed by the Main Account Administrator.
4. After 14 days of completing the process of deleting the Organisation Account in the manner described above, the Account and all the data collected in the Account (including the data provided by the Users within their Accounts) shall be deleted. Before the end of an indicated period, the Client can request that the Organisation Account be restored, sending an email to the address: hello@teamtoolbox.io.
5. Before the Main Account Administrator decides to close the Account, they should (if they consider it appropriate) inform the Co-users on their own that the Account is to be closed and the information and content found in the Application will be lost permanently.
6. Deleting the Organisation Account shall not release the Client from the obligation to pay the Service Provider for the Services provided until the moment the Account was closed.
7. Once the Account is deleted permanently, the Service cannot be used again and the content and information in the profiles of the Users of the deleted Account cannot be restored.
8. Independently of the possibility to delete the Organisation Account by the Client or the Service Provided, a Co-user can end the Co-user's activity in the Application through the agency of the Main Account Administrator or Moderator (via their email addresses visible in the Application or in any other manner chosen). The Main Account Administrator or Moderator can also delete a User without their request (e.g. when the User stops to be a member of a given Organisation or in other circumstances deemed appropriate by the Client).
9. Once the Co-user's Account is deleted, the Co-user shall be logged out from the application and shall not be able to log in again.
10. Once the User's Account is deleted (as decided by the Client), the information concerning the User shall be made anonymous. Due to the need to retain statistical validity, the information and content of the messages which cannot be linked with the User's data shall remain in the User's Account. The Service Provider can make the data completely anonymous when the User's Account is deleted, although the activity of the Main Account Administrator or Moderator (Kudo Cards) may be required. If the Client has doubts whether all the data in the User's Account have been made anonymous, the Client can request the Service Provider for verification at hello@teamtoolbox.io.

XV. Final provisions

1. The Application Supplier reserves their right to change these Regulations for the following important reasons only:
   a) if a change of the Regulations is necessary due to a change of the commonly binding laws;
   b) if a change of the Regulations is necessary due to a change of the price of the Service;
   c) fulfilling the obligation resulting from a legally final and valid court ruling or decision of administrative bodies;
   d) changes introduced for safety reasons, including intended to make it impossible to use the services specified herein in a manner which is at variance with the laws or these Regulations;

e) introducing changes in the operation of the Application or the services provided via the Application, including the ones connected with technical or technological progress, which include the changes in the Application Supplier’s systems.

2. An increase in the safety level shall not constitute a change of the regulations and shall not require prior notification.
3. The Regulations including the changes introduced in accordance with the preceding paragraph shall be made available to the Client 14 days in advance to the Main Account Administrator’s address provided during the registration in the Application. The Client shall be able to terminate the agreement within 14 days if they do not accept the new version of the Regulations.
4. The agreement between the Client and the Application Supplier shall be concluded for a definite term (Trial Version), and for an indefinite term in the case of the Premium Version. The agreement can be terminated if the Client violates the provisions of these Regulations or the binding laws.
5. The agreement between the Client and the Application Supplier concluded for the indefinite term can be also terminated by the Application Supplier with the notice period of 30 days counted from the end of a calendar month, and by the Client – by deleting the account according to Clause XIV above.
6. To the matters not regulated herein the relevant laws commonly binding within the Republic of Poland shall be applied.
7. The agreement between the Client and the Application Supplier can be concluded based on these Regulations in the Polish language only.
8. The Regulations shall be binding from October 29th, 2020.

Appendix No. 1 to the TeamToolbox Regulations

AGREEMENT ON ENTRUSTING THE TASK OF PROCESSING PERSONAL DATA

(hereinafter referred to as the "Agreement")

Concluded by and between the Client (hereinafter also referred to as the Data Controller) and the Service Provider (hereinafter also referred to as the Processor) – hereinafter jointly referred to as the Parties.

I. Subject of the Agreement

1. The subject of this Agreement shall be entrusting the Processor with the personal data specified in detain in Appendix No. 2 to the Agreement by the Data Controller.
2. The terms used herein should be understood in accordance with the definitions found in GDPR. The definitions provided in the regulations of **"TeamToolbox”** (hereinafter referred to as the Regulations) should be also considered, including in particular with regard to the notion of the Client, Service Provider, Messenger, Main Account Administrator, etc.
3. This Agreement shall constitute the agreement within the meaning of Article 28 of GDPR.

II. Parties’ representations

1. This agreement shall constitute a part of the agreement concluded by and between the Parties based on the Regulations ("Main Agreement").
2. In connection with the Services provided by the Processor to the Data Controller, in order to enforce the Main Agreement, the Processor shall occasionally process the personal data described in Appendix No. 2 to the Agreement on the Data Controller’s behalf.
3. The Client declares that the Client is the controller of the personal data described in detail in Appendix No. 2 below. In the event of joint control, the Client must act only in the scope of the agreement concluded under Article 26 of GDPR.
4. The Data Controller declares that the personal data referred to in item 3 above have been or will be collected in accordance with the relevant, commonly binding laws, and that the Processor may be entrusted with the task of processing them. The Controller acknowledges that the Controller shall be solely liable for providing the legal basis of processing the personal data entrusted under this Agreement (and the Main Agreement) according to the laws and meeting other requirements which result from GDPR in this scope.
5. The Processor declares that on the day of concluding this Agreement the Processor meets the requirements which allow to process the personal data entrusted according to GDPR, and will provide sufficient guarantees of implementing proper technical and organisational measures, so that the processing of the data entrusted can meets the requirements of GDPR and protects the rights of the persons whom the data concern.

III. Purpose, subject and nature of processing

1. The Processor undertakes to use the entrusted personal data to enforce the Main Agreement and in accordance with the terms of this Agreement, GDPR and the ones issued based on the secondary legislation and other commonly binding laws regarding personal data processing.
2. Appendix No. 2 to the Agreement describes the following: nature and type of personal data, and the categories of the persons, whom the data concern („Processing Specification”). The Processor can process the personal data only in the scope specified in this Appendix. The Regulations show the scope and context in which the Service Provider can process

personal data – in connection with enforcing the Main Agreement – as the independent data controller within the meaning of GDPR.

3. The personal data entrusted shall be processed by the Processor in a continuous manner for the period specified in Clause VII item 1.

4. The Service Provider cannot put together (combine, compare, etc.) the personal data entrusted and the personal data processed by the Service Provider as the data controller or by other data controllers.

IV. Data safety

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

2. The Processor undertakes to keep secret all the information connected with entrusting them with the personal data as well as the entrusted personal data both during their processing and indefinitely once their processing ends. Demonstration protection measures are specified in this scope in the Appendix No. 4 below. An increase in the safety level compared with the measures listed in Appendix No. 4 shall not constitute a change of this Agreement. The manner of implementing the requirement indicated in Article 32 of GDPR takes into account the nature of processing and the information available to the Processor specified in the Appendices 1 to 2 below.

3. The Processor must systematically and regularly test, measure and assess the effectiveness of the above protection measures and, if needed, implement immediately new measures or perfect the ones which have already been implemented.

4. The Processor shall process the entrusted personal data at the Data Controller's documented request only, which shall include this Agreement, requests sent by the Main Account Administrator via the Messenger and the requests sent by the Main Account Administrator to the address: hello@teamtooblox.io. The request can be also made in a different document form or written form within the meaning of the Civil Code.

5. The Processor undertakes to process the entrusted personal data with due diligence.

6. The Processor undertakes that the only persons authorised by them to process the personal data will be the persons who process the entrusted data to enforce this Agreement.

7. The personal data referred to in this Agreement on processing shall be treated as confidential information. The persons authorised to process personal data shall be obliged to keep confidential the entrusted data both within the term of their employment with the Processor and after the employment ends.

8. Taking into account the nature of the processing and the information available to the Processor, the Processor shall help the Data Controller with reporting data protection breaches to the supervisory authority, and informing the person whom the data concern of the personal data protection breach, as well as with the data protection impact assessment and prior consultation. Should a breach of personal data protection be found, the Processor shall report it without undue delay to the Data Controller to the email address of the Main Account Administrator or via the Messenger – at the discretion of the Processor. Should the Main Account Administrator lose control of the email account, they should inform the Service Provider of this fact in a different way (other than by email). Should the Data Controller need help with notifying the persons whom the data concern of the data protection breach (Article 34 of GDPR), the Processor – at the Data Controller's request – shall immediately email the users such information and display a message in the Application. After the incident, the Data Controller shall specify the circle of the entities who should be sent such information as well as the content of the message on the personal data breach.

V. Parties' cooperation

1. Taking into account the nature of the processing, the Processor undertakes, whenever possible – within 7 days of receiving the notification – to help the Data Controller using proper technical and organisational measures to fulfil the obligation to respond to the requests of the person whom the data concern in the scope of exercising that person's rights resulting from the commonly binding laws. The technical manner of fulfilling this obligation is specified more precisely in Appendix No. 3. The Data Controller can make their request via the Messenger or to the email address provided in Clause IV item 4.
2. In order to exclude doubts, the Parties unanimously confirm that the Processor shall be neither authorised nor obliged to respond – on the Data Controller's behalf – to the requests of the persons whose data are processed, including the requests made to the Processor via the Messenger. The persons making the request shall be provided with such information and informed that the request should be addressed to the Data Controller directly.
3. During the time the personal data are processed, the Parties undertake to cooperate in the process of processing the personal data entrusted, including to inform each other of any circumstances which affect or may affect the fulfilment of their obligations, and the Processor undertakes to comply with the Data Controller's instructions and recommendations regarding the personal data entrusted.
4. The Processor shall be liable for using the personal data at variance with this Agreement, including in particular for making available the personal data, which have been entrusted for processing, to unauthorised persons.
5. The Processor shall provide the Controller with any information necessary to prove that the obligations specified in this Agreement have been fulfilled.
6. The Controller shall be entitled to conduct audits in the scope of the Processor's compliance with the rules of processing the personal data the Processor have been entrusted with, specified herein. The Processor must contribute to making inspection or audit, possible, including the inspection of the Data Controller or the Auditor authorised by the Data Controller, and repair the irregularities found during the inspection. The right of inspection shall be exercised within the Processor's working hours, once the Processor is notified of the planned inspection at least 7 days in advance. The costs of the audit shall be covered by the Data Controller, subject to the remuneration of the Processor's employees or partners (i.e. the costs of their participation in the audit). In one calendar year, the Client can carry out maximum one audit, which shall last no longer than 2 working days, unless the Client justifies adequately the need to perform the audit, indicating a possible breach of the Agreement by the Service Provider.

VI. Entrusting data for further processing

1. The Processor undertakes not to use the services of another processor without the controller's prior general consent in writing. The Data Controller hereby consents to entrusting data for further processing to the entities listed in Appendix No. 5 to the Agreement and accepts the bases of further processing specified therein. The Processor shall inform the Data Controller by email to the Main Account Administrator's address of any intended changes, which concern adding or replacing other processors, making it possible for the controller to object to such changes. The objection made electronically by the Main Account Administrator to the email hello@teamtooblox.io shall be treated as the termination of the Main Agreement in compliance with the notice period.
2. The entrusted data can be transferred to a third country at the Data Controller's documented request only, unless the Processor is obliged to do so by the Union law or the law of the Member State the Processor is governed by. In such event, before the processing starts, the Processor shall inform the Controller of this legal obligation, unless the law forbids to provide such

information due to important public interest. The Data Controller hereby agrees that the data be transferred to a third country – to the entities listed in Appendix No. 5 to the Agreement – and accepts the bases of such transfer specified therein.

3. If the Processor uses the services of a further processor to perform specific processing actions on the Controller's behalf, the Processor must impose on the further processor in an agreement at least the same data protection obligations as the ones provided herein, including in particular the obligation to provide sufficient guarantees of implementing proper technical and organisational measures, so that the processing can meet the requirements of GDPR.
4. The Processor shall be fully liable towards the Controller for the failure to fulfil the subcontractor's obligations of data protection.

VII. Term and termination of the Agreement

1. This Agreement shall be concluded for the term of the Main Agreement.
2. The Data Controller can terminate this Agreement immediately if the Processor:
   a) processes the data in a manner which is at variance with this Agreement;
   b) failed to repair the irregularities found during an inspection;
   c) entrusted another entity with the task of processing the data without the Controller's consent.
3. Once the Agreement ends, within 10 working days, the Service Provider shall – as decided by the Client's in an email sent by the Main Account Administrator – delete or return all personal data to the Client (in the manner agreed by the Parties) and delete all their existing copies, unless the Union law or the law of the Member State require to store the personal data. The cost of returning the personal data shall be covered by the Service Provider, unless the cost exceeds 50% of the monthly licence. In such case, the costs shall be covered by the Client; within 10 working days of receiving the Service Provider's information on the amount of the costs, the Client shall decide if they still want the personal data to be returned.

VIII. Final provisions

1. The Parties shall not be entitled to additional remuneration in connection with entrusting the task of processing personal data, unless indicated otherwise by this Agreement or the Main Agreement.
2. The provisions of the Civil Code, the Act on the Protection of Personal Data of 10 May 2018, and the provisions of GDPR shall be applied to the matters which have not been regulated.
3. The competent Court for resolving the disputes resulting from this Agreement shall be the Court with the jurisdiction of the Processor's registered office. The Polish law shall be the applicable law.
4. The agreement was made in two counterparts – one for each of the Parties.
5. The appendices to the Agreement shall constitute its integral part. List of appendices:
   - *Appendix No. 1 to the Agreement on Entrusting the Task of Data Processing –> General description of the service*
   - *Appendix No. 2 to the Agreement on Entrusting the Task of Data Processing –> Specification of entrusting the task*
   - *Appendix No. 3 to the Agreement on Entrusting the Task of Data Processing –> Help with exercising rights*
   - *Appendix No. 4 to the Agreement on Entrusting the Task of Data Processing –> List of technical and organisational measures intended to meet the requirement specified in Article 32 of GDPR*
   - *Appendix No. 5 to the Agreement on Entrusting the Task of Data Processing –> Sub-processing*

6. The Agreement shall be changed according to the procedure specified in the Main Agreement, subject to the cases when – according to this Agreement or the Main Agreement – the change in the parameters of service provision, including data processing, does not constitute a change of the Agreement.

Appendix No. 1 to the Agreement on Entrusting the Task of Data Processing –> General description of the service

item no.	**Issue**	**Answers**
1.	Name of service/system/application.	TeamToolbox Application (hereinafter referred to as the Application) supplied under the terms specified in the regulations of "TeamToolbox” (Regulations).
2.	Designation of the entity providing the solution (name and registered office of the Service Provider).	AgileToolbox spółka z ograniczoną odpowiedzialnością (AgileToolbox sp. z o.o.) with its registered office in Warsaw (01-157) at Eustachego Tyszkiewicza 21, entered into the Register of Entrepreneurs maintained by the District Court for the Capital City of Warsaw in Warsaw, 12th Economic Division of the National Court Register, under the KRS (National Court Register) number: 0000365913, REGON (official business register number): 142578789, NIP (taxpayer’s identification number): 5272637352.
3.	Description of the technology used as a part of entrusting data.	Web application (SaaS model).
4.	Role of the Client concluding the Main Agreement based on the Regulations.	Data controller within the meaning of GDPR, subject to item 6 below.
5.	Role of the Service Provider.	The Processor within the meaning of Article 28 of GDPR, subject to item 6 below.
6.	Exclusions from the scope of entrusting the task.	In order to exclude doubts, it should be indicated that the scope of entrusting data to the Service Provider shall not cover the personal data processed by the Service Provider as the data controller pursuant to Clause XII of the Regulations.

Appendix No. 2 to the Agreement on Entrusting the Task of Data Processing –> Specification of entrusting the task

Item No.	**Designation of significant elements of entrusting the task**	**Specification**
	Designation of the categories of the entities whom the question concerns	**The Users who have been given access (including qualified users)**
1.	What is the nature of the processing (will the data be processed occasionally, systematically or in a complex manner)?	Systematically (the Main Agreement concluded for an indefinite term)
2.	What is the purpose of processing the data?	To enforce the Main Agreement.
3.	Will the data entrusted be processed in one Member State only or does the Service Provider have organisational units in more than one Member State?	Service Provider's registered office: Eustachego Tyszkiewicza 21, 01-157 Warsaw, Poland
4.	Will the data be processed within the European Economic Area only?	No, in the USA in the scope of the Intercom Messenger Service and the Amazon Web Services (AWS) (us-east-1). (see the table below)
5.	The locations where the data will be processed (country / city / street / apartment number).	Service Provider's registered office: Eustachego Tyszkiewicza 21, 01-157 Warsaw, Poland See. also the locations of the entities to which the data is subprocessed (table in Annex 5 below).
6.	Will the data be entrusted for further processing?	Yes
7.	What operations on the personal data will be carried out by the Service Provider?	Storing, deleting. In the case of the Messenger – also browsing. Note! The Service Provider shall not collect or supplement the data on the Client's behalf. As a part of the functionalities presented in the Regulations, the Client (or

	Demonstration operations on the data: collecting, recording, organising, putting in order, storing, adapting, etc.	the Client’s employees/partners) shall be also able to carry out other operations on the personal data on their own, such correcting, modifying, editing, etc.
8.	What is the scope of the data processed by the Service Provider on behalf of the Client (as the Processor)? (e.g. forename, surname, etc.).	Email address/login and password (data used to verify identity); Data provided (e.g. picture, forename, surname) and "created” by the users on their own by using the Application. Operational data: IP address, data of the application logs, statistical data, user’s browser, user’s country, Internet services provider of the user, type of user’s device, version of the user’s browser, archival data. A User can supplement their profile with the following: avatar, favourite quote, skills and type of motivation.
9.	Will special categories of personal data be processed?	The Service Provider shall not process those data categories intentionally. However, they can be "created" by users, in which case they shall be also entrusted to the Service Provider. The Client should specify (in their internal rules) and communicate to users the categories of data the users should not make available in the application.
10.	Is the application dedicated to children (persons under the age of 18)?	The Application is not dedicated to children, although the final decision in this scope shall be made by the Client (who shall choose the persons allowed to use the application on the Client’s behalf). A child cannot be the Client (party to the agreement).
11.	Was the obligation of the so called privacy by design and privacy by default (Article 25 of GDPR) considered when the tool intended for data processing was designed? Is there documentation in this scope?	Yes. At the stage of design, the Application was analysed paying special attention to rights or freedoms.

Appendix No. 3 to the Agreement on Entrusting the Task of Data Processing –> Help with exercising rights

item no.	Requirement	Technical/organisational measures intended to help the controller
1.	Having correspondence with the entity whose data are processed (receiving requests, responding to requests, providing the information requested, including verification of the identity of the requesting entity) (Article 12 of GDPR).	The Client shall specify and communicate on their own the manner in which the requests referred to in GDPR can be made to the Client by the persons whose data are processed. Should the Service Provider's help be needed to comply with a request, the Client shall hand over such request in the manner specified above in the Agreement on Entrusting the Task of Data Processing. The Service Provider shall not have correspondence on behalf of the Client – Data Controller. The Service Provider shall not make decisions on the Client's behalf in the scope of exercising the rights of the persons whose data are processed (including in particular in the scope of whether and how the rights of the persons whom the data concern should be exercised). The Service Provider shall inform the person making a request to the Service Provider of the need to address it to the Client directly. The only requests accepted by the Service Provider shall be the requests connected with the technical operation of the Application (e.g. error reports). In case of doubts regarding the nature of a request, the Service Provider shall hand the request over to the Client (those types of requests made by Users – without the Main Account Administrator – shall be included in the task of entrusting).
2.	Meeting the notification obligations indicated in Articles 13–14 of GDPR, information clauses (especially if the Service Provider collects personal data from data subjects).	The Client should fulfil the notification obligation on their own outside the Application itself.
3.	Right of access to data in the scope of providing copies of the data (Article 15 of GDPR).	At the Client's request, the Service Provider shall generate a copy of the data as a part of enforcing the Agreement.
4.	Right to rectification	Handled by the Service Provider (at the Client's request made in accordance with the Agreement).
5.	Right to data erasure, including the right to erase the data which have been made public, if applicable (Article 17 of GDPR).	Once the User's Account is deleted (as decided by the Client in accordance with the Regulations), the information concerning them shall be made anonymous. Due to the need to retain statistical validity, the information and content of the messages which cannot be linked with the User's data shall remain in the User's Account. The Service Provider can make the data completely anonymous when the User's Account is deleted, although the activity of the Main Account Administrator or Moderator (Kudo Cards) may be required. If the Client has doubts whether all the data in the User's Account have been made anonymous, the Client can request the Service Provider for verification at hello@teamtoolbox.io.

6.	Right to restriction of processing (Article 18 of GDPR)	Handled by the Service Provider (at the Client’s request made in accordance with the Agreement).
7.	Obligation to notify data recipients, including sub-processors, of the rectification or erasure of personal data or restriction of processing to (Article 19 of GDPR).	Fulfilled by the Service Provider by automated communication with subcontractors.
8.	Right to data portability (Article 20 of GDPR).	Handled by the Service Provider (at the Client’s request made in accordance with the Agreement).
9.	Right to object (Article 21 of GDPR).	Technically, it shall be completed the same as data erasure.
10.	The right not to be subject to a decision based solely on automated processing, including profiling (Article 21 of GDPR).	Not applicable, unless the Client decides – based on the assessment of the Application functionalities – that the automated decision-making within the meaning of Article 22 of GDPR occurs.
11.	Will the consents of data subjects be collected as a part of the task of entrusting data? If so, will the Service Provider help the Personal Data Controller fulfil the obligations indicated in Articles 7–8 of GDPR and what will be the scope of such help? (collecting and documenting the consents)?	Should the Client deem it necessary to collect specific consents, they should do this outside the Application.

Appendix No. 4 to the Agreement on Entrusting the Task of Data Processing –> List of technical and organisational measures intended to meet the requirement specified in Article 32 of GDPR

item no.	Requirement	Technical measures	Organisational measures
1.	Measures intended to ensure the confidentiality, availability and integrity of personal data.	The measures of physical protection of data: • The collection of personal data shall be stored in a room secured with ordinary door (not reinforced, not fire door). • The collection of personal data shall be stored in a room in which windows are secured with grating, blinds or safety and security window film. • The rooms, where the collection of personal data is processed, shall be equipped with burglar alarm system. • The access to the rooms, where the collection of personal data is processed, shall be controlled by the monitoring system using CCTV cameras. • The access to the rooms, where the collection of personal data is processed, shall be supervised by the security when the employees working in the rooms are not there. • The collection of personal data in the paper form shall be stored in a locked, metal cabinet. • Backup/archival copies of the collection of personal data shall be stored in a locked, metal cabinet. • The room, where the collections of personal data are processed, shall be secured against the effects of fire by the fire system and/or free-standing fire extinguisher. • Once no longer useful, the documents containing personal data shall be destroyed mechanically using shredders. Equipment measures of the computer and telecommunications infrastructure: • The collection of personal data shall be processed using a portable computer. • The following has been used: UPS-type devices, electricity generator and/or separate electric grid, which protect the computer system intended to process personal data against the effects of power failure. • The access to the personal data collection processed on a separate computer station / portable computer has been secured against unauthorised start-up with a BIOS password. • The access to the operating system of the computer which processes personal data has been secured with an authentication process using a user ID and password. • The measures which make it impossible to make unauthorised copies of personal data processed using IT systems have been applied.	Trainings of employees Agreements on Entrusting the Task of Data Processing Data protection policies implemented The Service Provider undertakes to test, measure and assess regularly the effectiveness of the technical and organisational measures intended to guarantee the safety of processing.

		• System mechanisms forcing a periodic change of passwords have been used. • The system which registers access to the system / personal data collection has been used. • The means of cryptographic data protection have been used for the personal data transferred by teletransmission. • The access to the means of teletransmission have been secured with authentication mechanisms. • A disk array has been used to protect personal data against the effects of the failures of the disk storage. • Protective measures have been used against such malware as e.g. bugs, viruses, Trojan horses, or rootkits. • The Firewall system has been used to protect the access to the computer network. • The IDS/IPS system has been used to protect the access to the computer network.	

Appendix No. 5 to the Agreement on Entrusting the Task of Data Processing –> Sub-processing

Item no.	Designation of entity	Sub-processor's registered office	Locations of data processing (country / city / street, apartment number)	Will data be transferred outside the European Economic Area as a part of using a subcontractor?	Have the Service Provider concluded a sub-processing agreement with the sub-processor, which guarantees that the requirements of GDPR are met? Is the enforcement of those requirements monitored?	List of entities whose data can be further sub-entrust	Link to processing agreement
1.	Amazon (Amazon Web Services)	Seattle (USA)	Amazon Web Services, Inc. - United States; Affiliated companies Amazon Web Services - the whole world.	The data is physically stored in Ireland. According to the entrustment agreement, data may be transferred in exceptional circumstances. Should data be transferred, the basis will be standard contractual clauses of the European Commission: https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf	such an obligation results from the data entrustment agreement.	see: https://aws.amazon.com/privacy/ and https://www.amazon.com/gp/help/customer/display.html?nodeId=468496	https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf
2.	Isolution sp. z o.o.	Poland	Warsaw	not applicable	not applicable	not applicable	in the registered office
3.	Intercom	San Francisco (USA)	United States (San Francisco, Chicago), Ireland (Dublin), Australia (Sydney), United Kingdom	Yes, data will be transferred outside the EEA and Switzerland based on standard contractual clauses. For details on transfer, see: https://www.intercom.com/help/pri	Intercom undertakes to conclude a processing agreement with other processors.	see: https://www.intercom.com/terms-and-policies#security-third-parties	Entrustment agreement Intercom register to access.

			(London)	cing-privacy-and-terms/data-protection/how-intercom-complies-with-gdprdetails: https://www.intercom.com/help/pricing-privacy-and-terms/data-protection/how-intercom-complies-with-gdpr			

Appendix No. 2 to the TeamToolbox Regulations

THE PRICE-LIST

Number of Users	Price for each module per 1 user / monthly	Price if a total of 7 modules are selected / monthly
For each user account as part of the premium version	HI: 2 EURO (8 PLN) SKILLS: 2 EURO (8 PLN) KUDO: 2 EURO (8 PLN) Market: 2 EURO (8 PLN) (WALL, TODO, Chat): 2 EURO (8 PLN) Feedback: 1 EURO (4 PLN)	7 EURO / (28 PLN)