Terms of Service, Privacy Policy, DPA

Terms of Service

Please read these Terms of Service, the Privacy Policy and the Data Processing Agreement. Together these three (3) documents constitute agreement ("**Agreement**") that applies to all Users of Our Service. This Agreement is between Survicate S.A. with its registered office in Warsaw (postal code 02 – 786) at ul. Zamiany 8 LU2, entered into the register of entrepreneurs of the National Court Register kept by the District Court for the capital city of Warsaw in Warsaw, 13th Commercial Division of the National Court Register under KRS number: 0001021023, NIP number: 9512390641, fully paid-up share capital: PLN 300,000.00, contact e-mail address: support@survicate.com ("**Survicate**", "**Service Provider**", "**We**", "**Our**" or "**Us**") and an adult person (having legal capacity) who is entitled to set up a company Account and does so in connection with the activity or profession performed and the rights held in the company - is not a consumer within the meaning of the law, for personal, family, non-business use ("**Authorized Person**", "**User**", "**You**" or "**Your**"). When we write "You", "Your" is to be understood in relation to each "User" and "Authorized Person" too. The Agreement sets out Your and Our rights and obligations. By signing up to Survicate's Service, You agree that You have read, understood and are bound by the Agreement.

The Terms of Service come into force on **28/02/2025.**

1. Definitions

1.1. **Account** – an account created on the Website which is necessary to use the Services. Only registered Users have access to the Account. The following data are necessary to log on to the Account: active e-mail address and the Password. The Account is used free of charge. By creating an Account on the Website, You declare that You are authorized to represent the company and use company data, and You provide truthful data.

1.2. **Account Data** – anything that You share with us, including personal data and Confidential Information in connection with Services provided.

1.3. **Account access service** – the service provided by Us through the Internet and with the use of the Website which consists in the access to the Account, management of the Account details, possibility of purchasing and activating the Services, as well as the possibility of downloading the data by the User in the form of a CSV file.

1.4. **Agreement** – agreement on provision of the Services on the terms and conditions set out in the Terms of Service, concluded electronically between the User and Us. The Agreement is concluded upon registration of the Account and terminated upon deletion of the Account. The contract for Subscription is concluded at the time of purchase of the Subscription and terminated at the end of the Service.

1.5. **Authorized Person –** a natural person who has been invited by the User to take advantage of the Services as part of the User Account. The User may grant to the Authorized Person access to all Services available on the Website or only to selected areas and functionalities. With respect to the rights granted by the User to the Authorized Person, the Authorized Person is the User's plenipotentiary for using the Services. The provisions of the Terms of Service, Rules and Regulations which apply to the User shall be applied to the Authorized Person accordingly. The User may assign different roles to Authorized Person, e.g. organization owner, admin, a user, or a guest. An Authorized Person can simultaneously be a member of another organization (User) or be an independent User.

1.6. **Confidential Information** - any information disclosed by either party to the other party under this Agreement, either directly or indirectly, in writing, electronic or orally (including, without limitation, documents, Personal Information, software). Confidential Information may also include information disclosed to a disclosing party by third parties. Confidential Information shall not, however, include any information which (i) was publicly known and made generally available in the public domain prior to the time of disclosure by the disclosing party; (ii) becomes publicly known and made generally available after disclosure by the disclosing party to the receiving party through no action or inaction of the receiving party; (iii) is already rightfully in the possession of the receiving party at the time of disclosure by the disclosing party as shown by the receiving party's files and records immediately prior to the time of disclosure; (iv) is obtained by the receiving party from a third party without a breach of such third party's obligations of confidentiality; or (v) is required by law to be disclosed by the receiving party, and discloses only so much of the Confidential Information as is required. The fact of establishing cooperation between the Parties, including the use of the Services by the User, is not considered Confidential Information.

1.7. **Entrepreneur** – a natural person, a legal person or an organizational unit without the status of a legal person which has legal capacity, and which, in its own name, conducts economic or professional activity within the meaning of the Civil Code.

1.8. **GDPR –** Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

1.9. **Package** – a set of Services offered by the Service Provider with the parameters and limits set out in the Price List or a separate agreement, thanks to which the User is able to use the Service for the fee set out therein.

1.10. **Password** – a series of alphanumeric or/and special characters necessary to conduct authorization in the process of gaining access to the Account.

1.11. **Price List** – the schedule made available by the Service Provider at URL address: https://survicate.com/pricing, which sets out the cost for which the

Service is provided by Us to You, as well as detailed functionalities and technical parameters of the Packages.

1.12. **Registration –** made in order to create the Account on the Website by entering the e-mail address in a relevant registration form. It is a process of acquiring the User rights, which is approved both by the Service Provider and the User. The registration form may be made available through the Website and/or through other access channels authorized by Us.

1.13. **Service –** the service provided by the Service Provider through the Internet and with the use of the Website which consists in the access to functionalities as part of the Package chosen and access to the ICT system where the User may store data.

1.14. **Services –** shall be understood as both the Account access service and the Survicate Service.

1.15. **Subscription –** access to the Package for a definite period, i.e. the period for which the User makes payment in advance and extends automatically if You don't unsubscribe. The scope of the Package's functionality as part of the Subscription has been set out in the Price List or separate agreement.

1.16. **Subscription Period** – the period indicated in the Price List or separate agreement for which the User made the payment and/or has undertaken to make the payment in the amount set out in the Price List. The Subscription Period ends on the date which corresponds to the date on which the Subscription Period started, lasts one month, quarter or one year, and ends on:

  1.16.1. in case of month subscription - the same last day of a next given month. If the customer purchased a subscription on the 31st, and in the next month there is no such day, the billing period will end on the last day of the month, i.e. on April 30 or February 28, respectively

  1.16.2. in case of quarter subscription - the same day of a third month counting from the subscription begin month. If the customer purchased a subscription on the 31st, and in the next quarter month there is no such day, the billing period will end on the last day of the month, i.e. on April 30 or February 28, respectively

  1.16.3. in case of a year subscription - on the date corresponding to the same date in the following calendar year

1.17. **Software** - software belonging to the Service Provider through which Services are provided to Users, i.e. Website.

1.18. **Term of the Agreement** – the period during which the User and Survicate remain bound by the Agreement, i.e. the period from the moment at which the Account was created to the termination of the Agreement.

1.19. **User** – a natural, a legal person or an organizational unit which uses the Service on the basis of the Agreement. The person who creates the Account for a User being a legal person or an organizational unit shall be obliged to obtain relevant authorization in advance. Entrepreneurs may be the User, using the Service in connection with the conducted activity or profession, the provision of services or the performance of work.

1.20. **Website –** the system of Service Provider's websites, including the limited access area, through which the User may manage the Services available in it. The Website is available at URL address: https://panel.survicate.com.

2. The Service

2.1.   Under the Agreement, the User gains access to the Account (this is free). The Website helps the User manage the Account, as well as purchase or activate other Services available in Price List.

2.2.   During the Term of the Agreement, the User may order the Survicate Service in the Package selected.

2.3.   The Service may be activated by the User as early as the stage of Registration on the Website, and at any Term of the Agreement in accordance with the Terms of Service.

2.4.   The cost of use of the Survicate Service has been provided in the Price List.

2.5.   The User has a possibility of analyzing on the Website the answers and effectiveness of the surveys created thanks to detailed reports.

2.6.   You can also:

(a) browse profiles of the respondents and analyze their behavior on websites where the survey has been placed,

(b) analyze activity of the respondents of the websites when a survey is active, answers, as well as the reaction to a call for action.

2.7.   Depending on the Package chosen, the Service may have limitations with respect to access to certain functionalities and/or differences in limits for use of certain events. The detailed information on that and the description of the Service can be found in the Price List.

2.8.   During the Term of the Agreement, the Service Provider may offer to Users additional paid and/or free services on the terms and conditions set out in separate rules and regulations as well as price lists.

3. Your rights and obligations

3.1.   The Service Provider shall offer the User support connected with the Services available on the Website.

3.2.   The User shall have the right to manage the Services through the Account and the right to view the personal data he has gathered. There is a possibility of changing the email address or other personal data, including payment data, after login in.

3.3.   The User undertakes:

(a) to verify, in advance, whether the technical requirements that need to be met in order to use the Website, including the Services, are complied,

(b) to update data, including personal data,

(c) not to use the Website to phish other Internet users, through malware or fraudulent acquisition of access data or other information,

(d) not to use the Website to collect card data, login and password data, official id numbers like national insurance numbers, passports number or other data that may lead to taking over the identity of a person or causing damage to them,

(e) inform respondents about the legal basis of the collected personal data and other legal obligations arising from the processing of personal data,

(f) not to take any actions which fail to comply with the generally applicable legal regulations (in particular, it is forbidden to disseminate content which contain child pornography, human trafficking, violence and hate speech, which breach copyright and/or other intellectual property rights of third parties, as well as contravene rules of social coexistence, show

extremely drastic scenes or may be considered to be vulgar or offensive lib),

(g) not to supply through the Services illegal content/data (in particular, pornographic and racist ones), which are generally considered to be vulgar, offensive and/or obscene, or which may offend feelings of other people, including religious and political ones, or any other content/data which violate legal regulations,

(h) not to use the Services to sell goods and/or services which are contrary to legal regulations,

(i) not to post misleading information regarding the authenticity and origin of goods and/or services,

(j) not to use the Website and the Services in a manner which is contrary to applicable legal regulations or rules of decency (indecent gambling, prostitution, excessive promotion of stimulants, illicit arms trade) as well as which infringe on personal rights of third parties and/or Service Provider's justified interests; Survicate is entitled to refuse to provide services if it is determined that the subject of the User's activity may affect Survicate's image and the mere presence of the Survicate tool on the User's side may prove harmful to Survicate,

(k) not to send unsolicited commercial information through the Website,

(l) not to interfere in the Website's and Service's source code,

(m) not to post through the Survicate Service hyperlinks to infected websites or websites whose content is contrary to law or rules of decency,

(n) not to take any actions which may hinder and/or disrupt the Website's and Services' operation, in particular by intentionally placing a malicious code or infected files,

(o) to use the Services within the applicable legal limits and for their intended purpose,

(p) not to access the Accounts of third parties (e.g. by cracking Passwords of other Users),

(q) not to generate excessive or disproportionate traffic on the connections or other elements of the infrastructure relied upon to provide the Service,

(r) keep his Password strictly confidential and not to make it available in any manner to third parties,

(s) not to make available to third parties his Account, as well as Account access data,

(t) not to use the Services for malicious purposes, e.g. exploiting the ignorance or naivety of respondents as well as manipulating information, misleading, using small fonts, no information on risks etc.

3.4. As part of the Service, it is forbidden to use any software / scripts unauthorized by the Service Provider, in particular those which disrupt and/or in any manner make the use of the Services automatic, such as viruses, bots, other harmful software, etc.

3.5. You shall be obliged to use correct personal data and e-mail address or other data. The Service Provider reserves the right to request the User to confirm the correctness of his data by a copy of relevant documents (like company register excerpt, power of attorney).

3.6. The rights and obligations of the User may not be transferred to other Users and/or third parties. This means that the User should not transfer, sell, or dispose of their Account for the benefit of any other entity, unless otherwise agreed upon. The Service Provider shall be the sole entity authorized to render the Services for the benefit of the User.

4. Our rights and obligations

4.1.   The Survicate does not moderate the content of the User Account.

4.2.   We may ask the Users for opinions and their level of satisfaction with the Services and customer support. We assess the quality of the service provided based on the data controller's legitimate interest and verify whether the contract we provide is or has been provided at the appropriate level and your expectations have been met.

4.3.   The Service Provider:

(a) may examine the manner in which the Services are used, in particular through collection anonymous information which allow improving them in terms of functionalities and technical aspects,

(b) has the right to examine the manner in which the Website, including the Services, is used, as well as create reports statistical analysis and use them in commercial activities (only anonymous data without any personal data of respondents or Your data),

(c) may use the logos of the Users using the Website, including the Services, on the Survicate's websites or promotional material, offers, etc. in order to indicate that they are or were Survicate's clients,

(d) may change, at its sole discretion, the properties and functionalities of the Services and/or the software used, provided that the level of quality of the Services rendered for the benefit of the User is not adversely affected,

(e) reserves the right to render the entire Website and/or the Service or portions thereof, temporarily unavailable due to technical reasons, especially when performing maintenance or introducing changes to the Website or the Services. The Service Provider shall take every effort to limit, to the extent practicable, the arduous nature of such unavailability of the Website and/or the Services for the User,

(f) undertakes to take every effort to ensure that the Services are rendered in a due manner, on a permanent and continuous basis,

(g) may suspend provision of the Service (during active Subscription) if the User has breached the provisions of Terms of Service. Prior to the suspension of the Services, the User shall be requested, sufficiently well in advance, to provide explanation, and should he fail to provide it or provide an unsatisfactory answer, the Services shall be suspended within 24 hours. Information about the reason and date of removal will be visible as a form of e-mail notification/system notification visible after logging in. We reserve that we may disable the use of the Services faster and leave only logging in to the Account. The User has the right to make a complaint. Any compensations shall be looked into in accordance with the complaint procedure and legal regulations. We reserve that if We receive a phishing report indicating You used Services to conduct phishing, we have the right to delete Your Account ourselves within 24 hours and terminate the Agreement immediately.

5. Technical requirements

In order to gain access to the Services, it is necessary to:

(a) accept the Terms of Service, Privacy Policy and Data Processing Agreement,

(b) successfully complete the Registration on the Website,

(c) use a device with one of the following Internet browsers with cookies enabled and access to the Internet with the minimum speed of 1 Mbit/s.

6. Account Registration and access

6.1.   To use the Service, You need to create an Account by providing Survicate with all required information and accepting the Agreement. You agree to provide to Us with complete and accurate information upon registration.

6.2.   If You use Our Website and Software on behalf of a legal entity (such as Your employer or a client), You represent and warrant that You have the authority to bind that legal entity. If You no longer have this authority, then You shall inform Us and the legal entity shall provide Survicate with a new authorized representative. We shall not be held liable should a person without the necessary authorization enter into this Agreement for and on behalf of a legal entity. Survicate assumes that the owner Account has access to the email address. Any changes will take place after acceptance to this email address. Survicate is in no way responsible for the situation if the email address assigned to the Account is not in the possession of the Account owner. In the event of such a situation, please contact technical support.

6.3.   We have the right to access Your Account if there is a breach of the law, legitimate interest related to solutions regarding the services provided or if You consent to access to data in order to resolve a support request. We make every effort to ensure that Your data does not change in any way, but it may happen that it will be necessary to modify the data - if it is necessary for the purpose of solving the application, we will inform you about it and ask for your consent. If modification or deletion of data is necessary under the notice and take down procedure, we will inform You about the actions we have taken.

6.4.   You are responsible for the security of your data (Account Data). We recommend using Two-factor authentication (2FA) to your account. If You notice that someone has hacked into your Account or has taken control over it, please inform Us immediately at **security@survicate.com**. We reserve that we are not responsible for actions or omissions committed using your Account and we have the right to block your Account in the event of a security breach on your part. In this case, only you bear full responsibility for actions or omissions using your Account and Survicate is not responsible in any way for lost profits or incurred losses.

6.5.   If there is a dispute or doubts about Account access or User content ownership, we reserve the right to determine ownership (or login data) based on our reasonable judgment in our sole discretion, whether or not an independent investigation has been conducted.

7. Subscription and Payments

7.1.   You shall make upfront payment for using the Service in the Package chosen. Payments are rightfully owed to Us, notwithstanding a lack of actual use of Subscription Services (i.e., Subscription paid without further use of Services).

7.2.   The Services shall be provided in accordance with the time limitations indicated in the Price List.

7.3.   The Service Provider may grant a discount to the User on the standard fees for provision of the Service on the terms and conditions set out in the Price

List and/or separate regulations or agreement. The discount amount may, in particular, depend on the duration of the Subscription Period in the case of a given User.

7.4. The Service Provider activates the Service once the payment is made. In well-justified cases, We may activate the Service prior to the User's payment. It is possible, however, only on the basis of an individual agreement between the parties to the Agreement.

7.5. Subscription is for a definite period. The User shall be informed at least 30 days prior to the expiry of the Subscription Period about the fact that Subscription shall automatically renew on monthly or annual periods, depending on the term contracted, unless You, at any time during Subscription period, decide to cancel their renewal through Account. If you've indicated your desire not to renew your Subscription, except in the event of an entire Account cancellation, the paid Subscription will remain active for the entirety of the contracted term. After this term, your Account will be downgraded to a free plan or its current equivalent.

7.6. During the Subscription Period, the User may, at any time, change the Package into a Package with higher parameters. Please get in touch with us: support@survicate.com or use the Website. A change of the Package into a higher one shall become effective within 48 hours of the payment - the payment shall be charged upon updating of the Package, and the remaining period in the transition month shall be adjusted on a pro-rata basis, whereas the Subscription Period shall remain unchanged. Upon ordering the Service, You declare the intention to receive VAT invoices. The VAT invoice shall be issued by electronic means, without the recipient's signature. The invoice shall be sent through the Service Provider's e-mail address: payments@survicate.com or a separate page. By accepting Terms of Services, you consent to the delivery of the invoice in this very form.

7.7. You can pay with:
(a) bank transfer - depending on pricing business plan,
(b) credit card with PayPal (Europe) S.à r.l. et Cie, S.C.A., a limited liability partnership registered as R.C.S. Luxembourg B 118 349, with its office at 22-24 Boulevard Royal, L-2449, Luxembourg. The terms and conditions of using the website referred to in this definition, as well as the rules for processing payments through the entity referred to in the preceding sentence have been set out in separate regulations available at URL address: https://www.braintreepayments.com/legal,

7.8. You shall provide Survicate or its third-party payment processor, with accurate and complete billing information including full name, address, state, zip code, and valid payment method information. By submitting such payment information, you automatically authorize Survicate to charge all Subscription fees incurred through your Account to any such payment instruments. All amounts paid are non-refundable. You further agree to be responsible for all taxes associated with the Service, along with any transaction fees and currency conversions added by your financial institution and intermediaries.

7.9. You can choose the frequency of payment for the Service and this is a recurring payment (consent for charging the credit card with recurring payments) in accordance with the Price List. The recurring payment is renewable. You may withdraw this consent for the recurring payment by sending an e-mail to the address support@survicate.com (You may be

requested to log on to the Account in order to confirm the instruction submitted), effective as of the end of the Subscription Period.

7.10. You may manage Your payment and data after logging in the Account panel.

7.11. The payment amount depends on the Package and the Subscription Period chosen by the User.

7.12. The prices in the Price List are net amounts. Taxin the invoice shall be settled in accordance with applicable regulations. Prior to the purchase of the Package, the User can obtain transparent information on the invoice gross amount.

7.13. The User may use a Package in which he can negotiate the price terms and conditions. It applies only to the Package indicated in such a way in the Price List. In such a case, an offer shall be presented by electronic means, and it shall be deemed accepted once the offer's acceptance has been confirmed.

7.14. Some banks may collect a fee/commission in the case of card or bank transfer payment (transfer abroad), and add it in accordance with their current price list, which is beyond the control of the Service Provider. Please read the rules for settlements, in particular international settlements, valid in your bank. The above-mentioned costs are not covered by the Service Provider.

8. Content in Survicate's services

8.1. **Your content is your responsibility.** When we say "your content" in these terms, we mean all the things you add (upload, post, share, or stream) to Our Services. This may include text, links, GIFs, emoji, photos, videos, documents, or other media. If we come up with another way for you to add content to the Services, it includes that too. You don't have any obligation to add content to the Services. If you choose to add content to the services, you are responsible for ensuring that you have the right to do so, that you have the right to grant the licenses in the terms, and that your content is lawful. We take no responsibility for any of your content, and we are not responsible for others' use of your content. If anyone reports copyright infringement or other infringement (or suspected infringement) to Us, We have the right to block or remove Your content. In such a situation, we will send You a notification by email.

8.2. You give Us a license to use Your content when You use Service. This license is worldwide, non-exclusive (which means you can still license your content to others), royalty-free (which means there are no fees for this license), transferable and granted for the duration of the Agreement and up to 24 months from the termination of the Agreement. Your content may be protected by certain intellectual property rights. We don't own those. But by using our services, you grant us a license—which is a form of permission—to do the following with your Account Data and content (in particular content, graphics, logos that are used by You to create and brand surveys), in accordance with applicable legal requirements, in connection with operating   for the purpose of Service providing, developing, and improving Our Services:
(a) recording in the IT infrastructure and using or changing,
(b) public performance, public display, (in particular, on the Internet),
(c) copying (also contingency purposes), including backups.

8.3. **Our content is our property.** Any software and content contained on the Website, such as text, graphic elements, logo, photographs, audio and video

files, are the Service Provider's property and are protected by law. Survicate is a trademark owned by the Service Provider. The above-mentioned trademarks and content may not be used without Service Provider's written consent, and, in particular, they may not be used in connections with other entities' products and/or services in a manner which may mislead clients and/or potential clients, or which may, in any manner, do any harm to the Service Provider and/or its products and services. Neither the User nor any person authorized by him may delete, obscure or prevent reading of or change trademarks, copyright information and/or other markings which concern the intellectual property rights contained in the Website, results of using the Service and/or in the content included in the Website. In particular, it is forbidden to delete and/or change the Survicate logo from the pictures made on the Website in the form of screenshots, reports and other effects of using the Service, except for the cases accepted by the Service Provider.

9. Data Processing

9.1. The rules for processing personal data by Us are set out in the Privacy Policy. There we describe Our rights and obligations as a personal data controller, processor and Your rights as a data subject.

9.2. By using Our Service, You may process information that qualifies as personal data of Your respondents and/or other protected information under the laws applicable to You and We may process Account Data in accordance with Our Data Processing Agreement (Schedule 3) and Your documented instructions. You shall be solely and exclusively responsible for the lawfulness of the processing of such personal data of Your respondents and other protected information. This includes obtaining any consent that You are legally or contractually required to obtain from Your respondents or basing the processing of personal data on a different legal basis.

9.3. You shall comply with all laws applicable to the processing of personal data by You in connection with the use of Our Service. For clarity, this includes any processing You carry out after exporting or downloading personal data from the Service and subsequently using it for Your business purposes.

9.4. If You are situated in the European Union (EU) and the European Economic Area (EEA) or If You are situated in a country outside the European Union (EU) and the European Economic Area (EEA) and You process personal data using Our Service and thereby entrust Us with personal data, the Data Processing Agreement applies.

10. Support

10.1. We ensure support available at the e-mail address: support@survicate.com or via our chat. We will reply as soon as possible. The Service Provider's time zone is CET (Central European Time). We do not work on bank holidays.

10.2. Support is provided 5 days a week (Monday - Friday). Support is not provided on holidays and non-working days in the territory of the Republic of Poland. We can differentiate support depending on the pricing plan.

10.3. Please remember that You are prohibited from providing respondents' data when You communicate with Us during support communication. We never ask you for such data and we do not ask for login details. Always check if the support message came from our survicate.com domain and make sure and send us a message if You have any doubts. Please write to: support@survicate.com.

10.4. ifyou have a complaint with respect to your quality of service, billing or invoicing, or you have any concerns about our terms of use or policies, we urge you to contact us so we can try to resolve your complaint or concern as quickly as possible. Contact us using the "send us a message" button inside the Survicte website or product or just email Us at support@survicate.com.

11. Incidents Response

11.1. You can report security incidents to the email address: security@survicate.com

11.2. If we obtain information or learn that Account Data has been disclosed and thus your control over them has been violated, we will inform you in accordance with the Data Processing Agreement. If you find out that unauthorized access to Account Data has taken place, please contact us in accordance with point above.

11.3. In the event of an occurrence or incident involving Account Data, We have the right to inspect your Account, view full log history and provide information to relevant authorized bodies that request such data. In addition, We have the right to take all steps to secure the Website infrastructure and Our Software, which may mean updates from time to time.

12.   Term and Termination

12.1. The Agreement shall be entered into as of the moment at which the Account is created on the Website, and remains in force until its termination (i.e. when the Account is deleted). The Agreement shall be entered into for an indefinite period. Services provided as part of the Packages are for a definite period of time and are accordingly extended for another month by means of repeating subscription renewal.

12.2. In order to create the Account, the User needs to complete the Registration.

12.3. Both during the Registration and at any time during the Term of the Agreement, the User may purchase the Package on the terms and conditions set out in the Terms of Service.

12.4. Deletion of the Account is possible in the case in which the User does not have an active Subscription, and if the User requests for the Account deletion (You can send an email to support@survicate.com or report this fact in the chat). If the account has an active Subscription, then deletion takes place at the end of the Subscription Period.

12.5. The User may resign from the Package and cancel the Subscription. Cancellation of the Subscription takes place at the end of the Subscription Period of the Package purchased. You are not entitled to a refund because the Service is provided during the notice period, even if You are not using them.

12.6. We shall have the right to terminate the Agreement with immediate effect if the User fails to use the Website (i.e. does not log to his Account or does not use the Survicate Service,) for over two months since the day of expiry of the last Subscription Period paid for or immediately if there is a major violation of the Terms of Service or the law or You use Website against provision of section 3 "Your rights and obligations". In such a case, the Service Provider shall send, in advance, the notification on the planned Account deletion should the User fail to purchase the Package (the notification may be sent by Us in the form of an e-mail message or a pop-up visible after logging in).

12.7. The condition for termination of the Agreement is the deletion of the Account. The Account will be deleted on the last day that ends the active Subscription period. The User may request Account deletion by sending an e-mail to: support@survicate.com . We may request User's verification which requires logging on to the Account.

12.8. The Survicate shall have the right to, respectively, block or terminate the Agreement in accordance with applicable law in the case in which the User has breached the provisions of the Terms of Service. If the User considers that Survicate has grossly violated the law or the provisions of the Terms of Service, User also has the right to terminate the Agreement with immediate effect after unsuccessful calls for rectification of deficiencies.

12.9. In the above-mentioned case, the fee paid by the User shall not be refunded.

12.10. In the case of doubts as to whether the termination comes from a given User, the Service Provider may request the User in the email form to confirm the intention to terminate the Agreement. The message is sent to the e-mail address assigned to the Authorized Person being properly empowered and this person has the right to make decisions in relation to the Account.

12.11. If We do not record Your login to the Website within 2 months, We have the right to delete your Account and terminate the Agreement immediately - the provision does not apply if You have an active Subscription.

13. License

13.1. Except as expressly stated in this Terms of Service, this Terms of Service does not grant to You any intellectual property rights or any other rights or licenses in respect of the Survicate software. We expressly reserve all right, title and interest in and to any intellectual property rights not specifically granted to User herein.

13.2. Subject to this Terms of Service, We grant You a limited, revocable, non-exclusive, non-transferable and non-assignable license to use the Our Software solution for commercial use subject to the terms of this Terms of Service and for the time Agreement is binding. You hereby agree not to resell any part of the software to third parties. You may not modify, copy, reverse engineering, distribute, introduce to trade, grant sublicences (unless agreed otherwise), or otherwise use Our content, property, and software. You may not use software or solutions that are designed to circumvent our rights. You have the right to perform activities permitted by law, and in this case, you undertake to inform us of any errors, problems or risks that you have discovered.

13.3. If you violate Our rights and do not comply with the License granted to You, We have the right to close Your Account immediately at Your risk and responsibility.

14. Complaints

14.1. Complaints should be made electronically by support@survicate.com, compliants@survicate.com or via chat. Please report within 30 days of noticing the damage (e.g. faulty operation of the Service) to the support. The complaint should include:

14.1.1. Account login,

14.1.2. as detailed description of the irregularity as possible (taking into account the time and place of its occurrence),

14.1.3. indication, if possible, of the way in which the complaint should be handled,

14.1.4. If the complaint concerns a mistake in an invoice, please provide the invoice number.

14.2. The complaint is looked into at the earliest possible date, but not later than within 14 days.

14.3. The day the Service Provider receives the complaint shall be deemed the day on which the complaint was made. The fact that a complaint has been made does not influence the course of the Subscription Period or the provision of the Service.

15. Confidentiality

15.1. Each Party (both Service Provider and You) is obliged to maintain confidentiality during the term of the Agreement and to use information, materials and data obtained from the other Party for the purpose of implementing the Agreement.

15.2. The Party will receive and maintain all confidential information disclosed or delivered to it by the second Party in strict confidence and will only use it for the purpose of cooperation and disclose it to those officers, employees or agents of this Party to whom it is essential to disclose to accomplish the purpose, provided such persons agreed to be bound by the confidentiality terms.

15.3. The Party agrees that the confidential information disclosed to it pursuant to this Agreement will:

15.3.1. be used only for the purpose implementing the Agreement;

15.3.2. not be used, or disclosed or disseminated for any other purpose whatsoever, other than with the written permission of the second Party; and

15.3.3. from the date of termination or expiry of this Agreement, not be used, or disclosed or disseminated for any purpose whatsoever other than indicated in the Agreement.

15.4. The above does not limit or exclude the possibility of us placing the User's logo and informing about the use of Our Services by the User.

15.5. Each Party is released from the confidentiality obligation if it is permitted by law or an authorized body releases a given Party from the confidentiality obligation in connection with pending proceedings.

16. Warranties

16.1. TO THE FULLEST EXTENT PERMITTED BY LAW, SURVICATE, ITS AFFILIATES, AND THEIR PARTNERS MAKE NO WARRANTIES, EITHER EXPRESS OR IMPLIED, ABOUT THE SERVICES. THE SERVICES ARE PROVIDED "AS IS." WE ALSO DISCLAIM ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, AND ANY WARRANTIES ARISING OUT OF COURSE OF DEALING OR USAGE OF TRADE. THE LAWS OF CERTAIN JURISDICTIONS OR STATES DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES. TO THE EXTENT SUCH WARRANTIES CANNOT BE DISCLAIMED UNDER THE LAWS OF YOUR JURISDICTION, WE LIMIT THE DURATION AND REMEDIES OF SUCH WARRANTIES TO THE FULL EXTENT PERMISSIBLE UNDER THOSE LAWS.

16.2. The above restrictions do not apply to consumer rights. The Service is not provided to consumers, however, if for some reason the consumer uses the Service or software, We reserve that such a provision should not take place because the User accepting the Terms of Service is fully aware that the Service is not addressed to consumers. With regard to our Software and the impact on Your customers, We reserve that We do not provide Services to Your customers and thus consumers.

17. Limitation of liability

17.1. We shall not be held liable for:
17.1.1. any User content,
17.1.2. incorrect data entered by the User,
17.1.3. lack of access to the Service as a result of the lack of operation, limitations in the operation of the Internet, other network services on the part of the User, issues in User's organization roles,
17.1.4. restrictions affecting and/or incorrect operation of software or hardware owned by the User and/or Authorized Persons thanks to which they can use the Services,
17.1.5. losses suffered and profits lost by the Users and/or Authorized Persons as a result of the Password to the User Account being disclosed to third parties by those Users and/or Authorized Persons,
17.1.6. losses suffered and profits lost by the Users and/or Authorized Persons as a result of those Users' and/or Authorized Persons' acts or omissions, in particular due to the fact that they use the Services in a manner which does not comply with the applicable law and/or the Terms of Service,
17.1.7. losses suffered and profits lost by the Users and/or Authorized Persons as a result of actions and/or omissions of third parties,
17.1.8. losses suffered and profits lost by the Users and/or Authorized Persons which have not been caused by the Service Provider's wilful intent.
17.2. The Service Provider has no influence on whether any third parties will or will not take any action and/or actions in connection with the Services provided. We have no influence on the manner in which the User and/or Authorized Persons manage their Account.
17.3. The Survicate:
17.3.1. only stores User data and enables their online transmission,
17.3.2. does not modify the data entered by the Users and/or Authorized Persons,
17.3.3. should the Service Provider receive an official notification, or should he become aware, in a reliable manner, about the unlawful nature of the data made available by the User, it shall contact the User in order to clarify the case and shall act in accordance with the Rules and Regulations as well as law.
17.4. Survicate is responsible for its actions and omissions up to the amount of the annual payment made by You prior to the event giving rise to the liability. If You or the company You represent is injured as a result of our actions or omissions, We are also liable up to the annual amount of remuneration for Services. If the action or omission is intentional, the limit to the annual amount of the liability remains valid. If You have more than one justified claim against Us, you agree that the Our maximum liability is up to the amount of remuneration You paid Us.

17.5. Survicate is not responsible for any lost profits and we are not responsible for the actions and omissions of third parties, with the exception of our employees and subcontractors. In the event that the Service is unavailable as a result of the operation of an IT service provider who provides solutions to us, liability shall apply up to the amount of the monthly remuneration.

17.6. If you cannot use the Service in a particular jurisdiction, we will not be liable for any claims relating to such inability to use the Survicate Services. You are obliged to check legal compliance before you start using the Services.

18. Assumption of Risk

18.1. You use our software and Service at Your own risk and take full responsibility as permitted by law, especially if You use it in a manner inconsistent with the law or decency. The Service may not be available in certain jurisdictions or local law may impose restrictions on the use of Services, therefore it is your responsibility to check the legal compliance and correct use or refrain from using the Service.

19. Governing Law

19.1. This Agreement is governed by and construed in accordance with the laws of Poland.

19.2. You and We agree that any dispute or claim arising out of or in connection with this Agreement or its subject-matter shall be subject to the exclusive jurisdiction of Poland and the territorial jurisdiction of the court is determined for the seat of Survicate.

20. Changes

20.1. The Survicate reserves the right to amend the Terms of Service and the Price List. Each substantial amendment of the Terms of Service shall be communicated to the User by email assigned to the Account owner at least 14 days prior to the planned entry of the amendments into force.

20.2. In the case referred to above, the User shall have the right to terminate the Agreement before the planned entry into force of the new rules and regulations and/or the Price List. Failure to report the intention to terminate the Agreement, or failure to terminate the Agreement by such a deadline shall be deemed as the User's consent to continue to be bound by the Agreement, on the terms and conditions provided for in the new rules and regulations and/or the Price List. If the Terms of Service are changed during the Subscription, the new regulations come into force within 14 days, but if the changes concern prices or the method of provision or functionality, these changes will only apply when You renew the Subscription.

21. Miscellaneous

21.1. The Service Provider makes available the wording of the Terms of Services at URL address https://survicate.com/terms, where the Terms of Service can be displayed and/or printed out. The Terms of Service may also be made available in a different manner, upon individual request of a given person, if such a person encounters problems in displaying or reading the Terms of Service. To this end, they are requested to get in touch with the assistance department at: support@survicate.com.

21.2.   We make available the wording of the Price List at URL address https://survicate.com/pricing, where the Price List can be displayed and/or printed out. The Price List may also be made available in a different manner, upon individual request of a given person, if such a person encounters problems in displaying or reading the Price List. To this end, they are requested to get in touch with the assistance department at: support@survicate.com.

21.3.   Should any provision of the Terms of Service be changed and/or invalidated as a result of a valid court's decision, the remaining provisions shall remain in force.

21.4.   The schedule constitutes and integral part of the Terms of Service.

21.5.   We have the right to refuse to provide Services or suspend the provision of services to companies from countries included in the US/EU/PL government sanctions list.

21.6.   We do not allow assignments. You have no right to transfer Your rights and obligations to another entity until you obtain Our consent.

21.7.   These Terms of Service take precedence over any terms and conditions and documents attached to purchase orders by You. In case of inaccuracies or doubts, the Terms of Service shall be applied directly.

Schedule 1: Price List : https://www.survicate.com/pricing
Schedule 2: Privacy Policy
Schedule 3: Data Processing Agreement

Survicate Privacy Policy

1. General Provisions

We invite you to read the Privacy Policy. We describe how personal data is processed in Survicate.

The Privacy Policy has been in force since 28.02.2025.

It is stipulated that capitalized terms utilized herein shall be interpreted in accordance with the definitions provided within Terms of Service:
https://assets.survicate.com/docs/Terms-Of-Service-Survicate-3.4.pdf
In the event of inaccuracies between the wording of the Privacy Policy and the Terms of Service, the Terms of Service and its provisions shall prevail.

We want you to know how we process personal data. We reserve that all personal data that We process as a data controller are obtained directly from the data subject or personal data of an employee/associate is provided by an employer associated company, e.g. at the stage of adding a person in the system. These are the Users' data. With regard to the respondents' data or any data entered as part of the Account Data, We are not their Data Controller, but the Processor.

2. Data controller

Survicate S.A. with its registered office in Warsaw (postal code 02 – 786) at Zamiany 8 LU2 Street, entered into the register of entrepreneurs of the National Court Register kept by the District Court for the capital city of Warsaw in Warsaw, 13th Commercial Division of the National Court Register under KRS number: 0001021023, NIP number: 9512390641, fully paid-up share capital: PLN 300,000.00, contact e-mail address: support@survicate.com (**"Survicate"**, **"Service Provider"** , **"We"**, **"Our"** or **"Us"**) is a data controller within the meaning of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to with the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter referred to as "**GDPR**") in the cases described below.

a) Persons who have consented to the processing of data
Purpose of processing: The data is processed in order to implement the consent given by the person (the purpose results directly from the consent form).
Legal basis: art. 6 sec. 1 point a) of the GDPR. Consent is given voluntarily and can be withdrawn at any time (please send request to: gdpr@survicate.com). Granting consent is necessary in order to implement the conditions for which consent has been granted (it results directly from the content of the consent message). Withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

Time of processing: The data is processed until the consent is withdrawn or after this period for the purposes of establishing, pursuing or defending legal claims within the period provided for by law.

Data recipients: Data may be made available to data recipients providing IT solutions, customer service, accounting or legal services to the Service Provider, when it is related to the implementation of consent.

b) User

Purpose of processing: The data is processed in order to conclude and perform the Agreement.

Legal basis: art. 6 sec. 1 point b) of the GDPR.

Processing time: The data is processed from the moment of entering into force of the Agreement, i.e. the creation of the Account and after removing the Account for the period required by law to establish, pursue or defend legal claims and/or accounting regulations.

Data recipients: Data may be made available to data recipients providing IT, customer service, accounting or legal services to the Service Provider, who are entitled to view Users' data.

c) Persons who contact Survicate in relation to support issues or consider a complaint in connection with the use of the Service

Purpose of processing: The data is processed as part of the legitimate interest of the Service Provider, which consists in providing answers and support and settling the complaint process.

Legal basis: art. 6 sec. 1 point f) of the GDPR.

Time of processing: We process the data for a period of 12 months from the date of consideration of the complaint, and after removing the Account for the period required by law to establish, pursue or defend legal claims and/or to meet requirements arising out of accounting regulations.

Data recipients: Data may be made available to data recipients providing IT, customer service, accounting or legal services to the Service Provider, when it is related to the implementation of the purpose of processing.

d) Persons who take part in the survey of satisfaction and evaluation of the Services

Purpose of processing: The data is processed as part of the legitimate interest of the Service Provider, which consists in assessing the quality of the Services provided and user experience.

Legal basis: art. 6 sec. 1 point f) of the GDPR.

Time of processing: We process the data for a period of 12 months from the date of consideration of the complaint, and after this period, if it is necessary for the purposes of establishing, pursuing or defending legal claims.

Data recipients: Data may be made available to data recipients providing IT, customer service, accounting or legal services to the Service Provider, when it is related to the implementation of the purpose of processing.

e) People who receive notifications or system messages

Purpose of processing: The data is processed as part of the legitimate interest of the Service Provider, which consists in sending notifications or e-mails in accordance with the Privacy Policy. The detailed list of notifications sent is described in point 8 below.

Legal basis: art. 6 sec. 1 point f) of the GDPR.

Processing time: The data is processed for the period in which the User has an Account, and after this period the Service Provider has the right to process only

information about to whom, when and what messages or notifications were sent as long as it is necessary for the purpose of determining, pursuing or defending legal claims or services settlement after the end of the cooperation.

Data recipients: Data may be made available to data recipients providing IT, customer service, accounting or legal services to the Service Provider, when it is related to the implementation of the purpose of processing.

f) Persons who contact support in connection with the provision of the Services
Purpose of processing: The data is processed as part of the legitimate interest of the Service Provider, which consists in providing support.
Legal basis: art. 6 sec. 1 point f) of the GDPR.
Processing time: The data is processed for a period of 12 months from solving the problem, and after this period, if it is necessary for the purposes of establishing, pursuing or defending legal claims.
Data recipients: Data may be made available to data recipients providing IT, customer service, accounting or legal services to the Service Provider, when it is related to the implementation of the purpose of processing.

g) People who contact with Survicate
Purpose of processing: The data is processed as part of the legitimate interest of the Service Provider, which consists in answering or considering the request.
Legal basis: art. 6 sec. 1 point f) of the GDPR.
Time of processing: The data is processed for a period of 12 months from solving the problem, and after this period, if it is necessary for the purposes of establishing, pursuing or defending legal claims.
Data recipients: Data may be made available to data recipients providing IT, customer service, accounting or legal services to the Service Provider, when it is related to the implementation of consent.

h) **Website visitors**
Purpose of processing: We collect data on the basis of your consent to the processing of cookies or in scope of some cookie files - legitimate interest of the Service Provider, which consists in marketing activities, creating statistics of visits and the way of using the website.
Legal basis: art. 6 sec. 1 point f) of the GDPR
Time of processing: The data is processed until the consent is withdrawn or after this period for the purposes of establishing, pursuing or defending legal claims within the period provided for by law.
Data recipients: Data may be made available to data recipients providing IT, customer service, accounting or legal services to the Service Provider, when it is related to the implementation of consent.

3. How long data is kept

3.1. Survey Data and Feedback Analysis

Survicate does not determine the retention period for data related to surveys and feedback analysis, including respondent information. The user has full control over the data and can manage its retention by either deleting specific records or removing the entire account. Until such actions are taken, the data remains stored in the system. Users also have the ability to search for and retrieve specific data as needed.

3.2. Application Users' Data

For users of the application, data is processed from the moment of account creation (i.e., when the Agreement enters into force). After an account is deleted, data is retained for the period required by applicable law for the purpose of establishing, pursuing, or defending legal claims and/or to comply with accounting regulations.

4. Your rights related to the protection of personal data

You have the right to access your data, rectify, transfer (if the basis for processing is consent - art. 6 section 1 lit. a GDPR), delete or limit processing, the right to object (if the basis for processing is art. 6 section 1 lit. f GDPR), the right to lodge a complaint to the supervisory body (in Poland to the President of the Office for Personal Data Protection).

A request related to personal data can be submitted by emailing gdpr@survicate.com.

5. Is the data shared with third parties and or transferred outside the European Economic Area?

The transfer of data to third countries takes place on the basis of the agreements we have signed. Entrusting data processing is related to the performance of the Agreement. Here is the full list of providers:

No	Entity Name	Country	Service/purpose of data processing	What data is shared
1	Amazon Web Services EMEA SARL	Luxemburg/ Ireland	IT infrastructure	Data concerning respondents and users in the application, contact information, identification data, usage data, and survey responses for cloud storage and computing services.
2	Intercom R&D Unlimited Company,	Ireland	Website chat service	User contact information, interaction history, and behavioral data for customer support and engagement tools.
3	Mixpanel, Inc.	USA	Analysis of aggregated data about the behavior of application users	Anonymized user activity data, event tracking information, and engagement metrics for analytics and performance monitoring.
4	API Hub, Inc. (acting under Clearbit brand)	USA	Enriching information about users' companies with publicly available data about them	Email addresses, company information, and professional titles for enhancing contact and company data enrichment services.
5	Atlassian Pty Ltd (Jira)	Australia	Communication with clients on projects	Issue and bug report details, user feedback, and product development

				data for project management and tracking.
6	Recurly, Inc.	USA	An external service for managing subscriptions, including invoicing clients	Billing information, subscription data, and payment history for subscription management and payment processing.
7	Chartmogul	Germany GmbH & Co.	Subscriptions analysis	Subscription data, revenue information, and customer lifecycle metrics for subscription analytics and revenue reporting.
8	Google LLC	USA	E-mail solutions, storage of documents, agreements, notes; remote meets tool, APIs	Contact information: Details that allow for communication with individuals, such as phone numbers, email addresses, and mailing addresses.

Identification data: Information that can be used to identify individuals, which could include names, ID numbers, or other unique identifiers.

Documents: Files and records that users create, store, or share, including text files, spreadsheets, presentations, and PDFs.

Emails: Electronic messages sent or received by users, including their content and metadata (such as sender, receiver, date, and time).

Calendar events: Appointments, meetings, and other scheduled activities that users add to their calendars, including details about the time, participants, and descriptions of the events.

Interaction data across Google Workspace services: User actions and activities within Google Workspace applications, such as document edits, comments, and shares.

User behavior data: Information on how users interact with a service or website, including pages visited, time spent on pages, and navigation paths.

Traffic sources: Data about how users arrive at a website or application, such as through search |

				engines, direct navigation, or referral sites. Anonymized identifiers for advertising, analytics, and cloud services: Unique but anonymized codes used to track user activities and preferences for the purposes of advertising, analyzing user behavior, and providing cloud-based services.
9	Notion Labs, Inc.	USA	For project management and intranet function	Project documentation, team collaboration data, and organizational structure information for documentation and project management.
10	Smartlook.com s.r.o.(CISCO)	Czech Republic	Chat Session recording and heatmaps software	User interaction data, session recordings, and behavioral analytics for website and app performance analysis.
11	HubSpot Inc.	USA	CRM, platform of marketing, sales, customer service, and CRM software	Customer information (name, email, contact details), marketing analytics, customer interactions, and sales data.
12	Savio Technology Inc.	Canada	Track feature requests and product feedback from support and NPS tools, CRM, and Google Docs.	Feature request details, user feedback, and prioritization data.
13	CUSTIFY S.R.L	Romania	Cloud based customer success platform	Customer success data, user interaction records, and account usage information.
14	Autenti sp. z o.o.	Poland	Document signing tool	Electronic signatures, identity verification information, and document transaction logs.
15	DocuSign, Inc.	USA	Document signing tool	electronic signatures, identity verification data, and document transaction records.
16	Braintree (PayPal (Europe) S.à r.l. et Cie, S.C.A.)	Luxembur g	Payment services	Payment information, transaction history, and billing addresses.
17	Clay Labs Inc	USA	Stitch together apps, APIs and software code by building, using and tracking automated workflow engines	Could include contact management details, integration data, and workflow automation information.
18	521 Products Pty Ltd (Smartlead)	Australia	Tool for sales, or marketing, providing features that help	Lead information, engagement data, and sales lead management details.

				businesses identify, track, or manage potential customers	
19	Open AI LLC (Chat GPT, API)	USA	AI-assisted search in the tool, Text Responses Summarization	Text input from users, including feedback, opinions, and other responses collected through Survicate's surveys; Text queries entered by Survicate users while using the AI-assisted search feature, User Interaction Data, Usage Metrics.
20	Linear Orbit, Inc.	USA	Project management	Issue and bug report details, user feedback, and product development data for project management and tracking.
21	Slack Technologies, LLC	USA	Survicate team communication tool	Contact details of clients' representatives and tool users
22	Vero Labs, Inc.	USA	e-mail tool - Marketing automation software for software companies. Multi-channel messaging	Contact details of clients' representatives and tool users
23	Sendgrid (Twilio, Inc.)	USA	Email distribution tool	Contact details of clients' representatives and tool users
24	tl;dv GmbH	Germany	A tool for recording, transcribing, and summarizing online meetings	Meeting recordings, transcripts, and summaries: Audio and video recordings of virtual meetings, along with automatically generated transcriptions and key takeaways.

User interaction data: Information on how users engage with the tool, including meeting participation, transcript edits, and note-taking.

Metadata from meetings: Details such as meeting timestamps, participant names, and agenda points for tracking and organization.

Integration data: Interactions with third-party tools like Google Meet, Zoom, or Slack to enhance meeting documentation and workflow automation. |
| 25 | Anthropic PBC | USA | AI-powered assistant for text-based inquiries, content | User queries and interactions: Text-based inputs from users for AI |

| | | | | generation, and customer support | processing, including questions, prompts, and commands.

Generated responses: AI-generated text responses based on user input, providing information, summaries, or assistance.

Metadata and usage analytics: Data on interaction frequency, session duration, and engagement patterns for service improvement.

Anonymized identifiers: Unique but depersonalized identifiers used for tracking user interactions and refining AI model performance. |
|---|---|---|---|---|---|
| 26 | CleanShot X (by Make The Web) | Netherlands | A tool for capturing, annotating, and sharing screenshots and screen recordings | | Screenshots and screen recordings: Captured images and videos of the user's screen for documentation, sharing, or reference.

Annotations and edits: User-added comments, highlights, blurs, and other modifications applied to screenshots or recordings.

Metadata: Information such as timestamps, file formats, and device details associated with captured media.

Cloud storage and sharing data: If cloud sync is enabled, files may be stored on external servers with sharing links and access permissions. |

In the case of above-mentioned providers, data is transferred to a third country.
Please be aware, that the USA does not have an adequacy decision issued by the European Commission and European regulations on the protection of personal data do not apply there. It is our duty to inform you that the transfer of data to the US involves the risk of access to data by US intelligence services on the basis of applicable law. As we informed above, we have concluded a data processing agreement with each of the entities.

Categories of Third-parties engaged by the Survicate
1) Transfer to Third Parties Requiring Consent: For some third-party tools, particularly those involving cookies and similar tracking technologies, we obtain

your consent through a cookie banner displayed on the login page of panel.survicate.com. You have the freedom to choose whether to accept or reject these cookies both at the point of entry and later through our Survicate Privacy Center, where you can also modify your consent choices at any time.

2) Transfer to Third Parties Based on Legitimate Interests: We engage with certain third parties whose services are integrated based on our legitimate interest, such as significant improvements to our service provision or additional product features. You have the right to object to the processing of your data by these third parties. Objections can be made through our Survicate Privacy Center.

3) Essential Survicate's Service Providers: There are third parties whose involvement is essential for the providing of our services. Accepting our services implicitly requires acceptance of these third parties, as their role is crucial for the functionality of Survicate. An example of such essential services is cloud infrastructure provided by AWS, which forms the backbone of the Survicate tool. Any changes in this regard are not possible, and the only way to prevent data transfer to these third parties is to discontinue using Survicate's services.

Consent and Your Choices
Your privacy is of utmost importance to us. We provide mechanisms for you to manage your consent/ opt-out and make informed decisions about the sharing of your data:
- At Entry: You are presented with options to consent to or reject the use of third-party tools that require your explicit consent via a cookie banner.
- Privacy Center: For ongoing consent management, including the ability to change your preferences or object to data processing based on legitimate interests, you can visit our Privacy Center at Survicate Privacy Center.

Your choices regarding the use of your data are respected, and we strive to provide you with control over your information. However, please note that the rejection of certain third parties may impact the functionality of our services.
For any further questions or concerns regarding our data sharing practices, please contact our privacy team at gdpr@survicate.com.

6. Use of Google APIs

Use of Google APIs
Survicate leverages various Google APIs to enhance our offerings.
This approach is applied in two main contexts: for secure login to our panel and for facilitating OAuth-based integrations with our services.
This ensures that we manage the information sourced from and sent to Google APIs with the highest level of care and responsibility, particularly emphasizing the secure management of authentication data.

Adherence to Google API Services User Data Policy
We strictly comply with the Google API Services User Data Policy, including adhering to the Limited Use requirements. This compliance ensures that the processing, use, and transfer of data received from or sent to Google APIs by our application are conducted in a manner that respects both the policy's stipulations and your privacy.

Limited Application of Google API Data through OAuth

The information obtained from and sent to Google APIs is exclusively utilized for the intended purposes of the specific APIs and within the context of our services to You. We ensure that:

1. The data is not employed for advertising objectives.
2. The data sent to or received from Google is not disclosed to any third parties, unless such disclosure is necessary for the provision of our services.
3. The data is stored securely and is accessible solely to authorized personnel.

In addition to receiving data from Google APIs, our application also transmits data to Google for various purposes, such as updating records or retrieving information. This process is conducted in strict compliance with Google's policies and with a focus on protecting your data privacy and ensuring secure access.

Your Rights and Choices

As a user, you possess rights and options concerning the information sent to and received from Google APIs. You can adjust your preferences and settings to manage the data shared with our services.

7. Do we profile personal data?

No.

8. How can you get in touch with us?

We will be happy to answer any questions by e-mail. We encourage you to contact us by e-mail: gdpr@survicate.com
Alternatively, you can use the address: Zamiany 8 LU2 Street, 02-786 Warsaw, Poland

9. In what cases is the Survicate a processor?

We are a processor within the meaning of the GDPR at the moment of concluding a Data Processing Agreement (to entrust the processing of personal data in relation to Account Data). The User decides what data is processed by means of surveys. The rules of processing are set out in a separate Data Processing Agreement (DPA).
We are the processor of respondents' data and Account Data that are stored in the User's Account. If you have questions about how your personal data is processed, please contact the creator of the survey.

Scope of data related to respondents:
1. Visitor ID,
2. Visitor attributes passed using traits or survey URLs,
3. IP,
4. browser language,
5. email address in link surveys (sending through client's e-mail),
6. operating system version, device type, device,

whereby, in the scope of Visitor ID and Visitor attributes passed using traits or survey URLs, the data is stored in Local Storage.

Survicate does not use cookies for the respondents, does not use cookies placed on the respondent's device, nor does it initiate their installation. We do not create/use any cookies for the purpose of targeting, showing or marketing activities. We do not use them in completing survey purposes as well. However we can deliver a product feature that allows us to show a survey based on visitor cookies.

Survicate uses the geographic location of respondents based on IP address. We do not collect precise GPS co-ordinate locations. We just infer location from IP address. What is important, we do not store this information, i.e. it is processed live for the purposes of technical delivery of the service (CDN).

The respondent's IP could be processed for the purpose of IP blacklisting. The Firewall has the functionality of permanently blocking connections from specific IP addresses and integrating user identity management. To use this functionality, it is necessary to engage the IP addresses of individual respondents.

10. What notifications does the Service Provider send and why?

We send system notifications that are visible after logging in. This is due to ensuring a better flow of information.

• **Notification about the purchase of the Service**
 You will receive information about the purchase of the Service.

• **Notification about the approaching end of the subscription**
You have the option not to extend the Services, and if you do not perform any action, they will automatically be extended for the next period.

* **Notification about product functionalities**
 You will receive information about the product updates and new features.

• **Notification of service interruption/update**
You will receive information about the planned maintenance break, its duration and reasons. Please note these changes are made from time to time to ensure the security of the Services.

• **Notification of changes to the Terms of Service or Price List**
We will notify you of changes to the Regulations or the Price List so that you can familiarize yourself with them.

11. What reports can Survicate generate based on anonymous data?

We have the right to generate anonymous and static reports. These reports may later be presented by the Service Provider for promotional or advertising purposes or for the development or provision of its own services. Reports are based on numbers or other statistical data, so they present quantitative summaries. For example, how many users

from a given country used our Services in month X, how many surveys were created in month X, etc. Personal data is neither processed nor presented.

12. Security

1. The principles we follow:
   a) We respect the right to privacy.
   b) We take care of data, including personal data.
   c) Connection with our Website is encrypted.
   d) We do not request you to log on to the Account when we send invoices or any e-mail correspondence.
   e) We do not request you to provide data by e-mail. We always conduct verification after logging on to the Account. We would like to ask you for understanding if certain actions require confirmation and verification. In such a case we may ask you to log on to the Account or additional formal representatives of your organization involvement.
2. When using the Internet, choose only safe devices and networks. If you use the Website for work purposes, follow the security recommendations at your organization.

13. Cookies

1. Cookies are sent to Internet browsers, then stored in the memory of devices, and read by the server at each connection with the Website.
2. You can obtain information about cookies processed by Survicate and manage the consent to cookies by clicking here: https://survicate.com/#cookie-settings
3. If you don't want to store some cookies on your device, you can manage them through your device browser settings, giving you more control over your privacy and preferences. This means that you may disable cookies from all sites except those that you trust.
   a. **Google Chrome** (https://support.google.com/chrome/answer/95647?hl=en)
   b. **Edge** (https://support.microsoft.com/en-us/microsoft-edge/delete-cookies-in-microsoft-edge-63947406-40ac-c3b8-57b9-2a946a29ae09)
   c. **Mozilla** (https://support.mozilla.org/en-US/kb/cookies-information-websites-store-on-your-computer)
   d. **Opera** (https://www.opera.com/pl/use-cases/clean-browser-and-remove-trackers)
   e. **Safari** (https://support.apple.com/pl-pl/guide/safari/sfri11471/mac; https://support.apple.com/en-us/HT201265)

Data Processing Agreement

If you are a Data Controller and Survicate Data Processor, module 2 applies.
If you are a Data Processor and Survicate Data Sub-Processor, module 3 applies.
If you are a Data Controller outside EEA receiving personal data gathered by Survicate acting as Data Processor, module 4 applies.

DATA PROCESSING AGREEMENT (Survicate as the Data Processor)

STANDARD CONTRACTUAL CLAUSES - MODULE 2

Text adopted by the European Commission in the following version

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:
  (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "**entity/ies**") transferring the personal data, as listed in Annex I.A. (hereinafter each "**data exporter**"), and
  (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "**data importer**")

have agreed to these standard contractual clauses (hereinafter: "**Clauses**").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards,

provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  - (i)   Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - (ii)   Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
  - (iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
  - (iv)   Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
  - (v)   Clause 13;
  - (vi)   Clause 15.1(c), (d) and (e);
  - (vii) Clause 16(e);
  - (viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1   Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2   Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3   Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4   Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5   Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6   Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[4] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(a) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
(b) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
(c) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
(d) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [**14 DAYS**] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall

provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

(h) Survicate's liability is limited in accordance with the service agreement.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative

within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
  (i)   the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
  (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

15.1   Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
   (i)   receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
   (ii)   becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2   Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
  (i)   the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  (ii)   the data importer is in substantial or persistent breach of these Clauses; or
  (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

  In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Republic of Poland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
(b) The Parties agree that those shall be the courts of court in Poland, competent for the seat of the Data Importer.
(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
(d) The Parties agree to submit themselves to the jurisdiction of such courts.

DATA PROCESSING AGREEMENT (<u>Survicate as the Data Sub-Processor</u>)

STANDARD CONTRACTUAL CLAUSES - MODULE 3

Text adopted by the European Commission in the following version

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) Annexes I to IV are an integral part of the Clauses.

(c) The Parties:
  (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and
  (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(d) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(e) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  (ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
  (iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

  (iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

  (v) Clause 13;

   (vi) Clause 15.1(c), (d) and (e);

   (vii) Clause 16(e);

   (viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.
(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.
(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.
(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter

throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[6] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iv) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(v) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9   Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.
(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.
(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.
(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.
(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.
(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least [**14 DAYS**] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[9] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

    (ii)   refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

(h) Survicate's liability is limited in accordance with the service agreement.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
  (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
  (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation , if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
  (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

  The data exporter shall forward the notification to the controller.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
   (i)   the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
   (ii)   the data importer is in substantial or persistent breach of these Clauses; or
   (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority and the controller of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.

The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

[OPTION 2 (for Modules Two and Three): These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Poland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of court in Poland, competent for the seat of the Data Importer.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

DATA PROCESSING AGREEMENT (Survicate as the Data Processor transferring data to the Controller located outside the EEA)

STANDARD CONTRACTUAL CLAUSES - MODULE 4

Text adopted by the European Commission in the following version

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
   (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
   (ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
   (iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
   (iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
   (v) Clause 13;
   (vi) Clause 15.1(c), (d) and (e);
   (vii) Clause 16(e);
   (viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1   Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.
(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.
(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

Not applicable

Clause 10

Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

(f) Survicate's liability is limited in accordance with the service agreement.

Clause 13

Supervision

Not applicable

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

  (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

  (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii)   any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

15.1   Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
  (i)   receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  (ii)   becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular,

number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2   Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
   (i)   the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
   (ii) the data importer is in substantial or persistent breach of these Clauses; or
   (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter

may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Poland.

Clause 18

Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the court in Poland, competent for the seat of the Data Importer.

ANNEX I:

A. LIST OF PARTIES

Data Exporter / Data Controller(s): the customer

Data Importer / Processor(s): [*Identity and contact details of the processor(s) and, where applicable, of the processor's data protection officer*]

1. Name: Survicate S.A.

Address: Zamiany 8 LU2 Street, 02 – 786 Warsaw, Poland

Contact person's name, position: Marcin Przybył, Member of the Board

Processor's data protection officer: Rudi Kosiór - Security Officer, DPO, gdpr@survicate.com,

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

respondents, customers' and contractors' representatives of the Data Controller, potential customers of the Data Controller, employees of the Data Controller,

Categories of personal data transferred

IP, Visitor ID, name, surname, sex, email address

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Customer Personal Data may include special categories of personal data (as defined in the GDPR). This may include, for example: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous basis.

Nature of the processing

data processed in the IT infrastructure; in the SaaS model based on the cloud environment

Purpose(s) of the data transfer and further processing

feedback surveys conducting, according to the service agreement

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

From the moment of creating the Account and for a period of 12 months after deleting the Account. The data processed after deleting the Account are only for the purposes of backup for the Controller and are part of the Service provided after its termination, which is performed by the Processor

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

As above

C. COMPETENT SUPERVISORY AUTHORITY

For Module 2 and Module 3

Identify the competent supervisory authority/ies in accordance with Clause 13

President of the Personal Data Protection Office in Poland (uodo.gov.pl).

ANNEX II: TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Technical and Organizational Measures
1. Confidentiality
• **Physical access control** *No unauthorized access to data processing facilities, e.g., magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems,*

• **Electronic access control** *No unauthorized use of the data processing and data storage systems, e.g.: (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media,*
• **Internal access control** *(permissions for user rights of access to and amendment of data) No unauthorized reading, copying, changes, or deletions of data within the system, e.g., rights authorization concept, need-based rights of access, logging of system access events,*
• **Isolation control** *The isolated processing of data, which is collected for differing purposes, e.g., multiple client support, sandboxing,*
• **Pseudonymization** *The processing of personal data in such a method/way, that the data cannot be associated with a specific data subject without the assistance of additional information, provided that this additional information is stored separately and is subject to appropriate technical and organizational measures.*
• *Survicate use the HTTPS protocol in transit to protect your data. Survicate's TLS/SSL setup follows the latest recommendations.*
• *Possibility of enabling Two-factor authentication on your Account logging.*
• *Survicate has antimalware, firewall, and device control software installed on all workstations and uses full-disk encryption in place for our laptop fleet.*
• *Access to Survicate databases and servers is restricted and securely configured within private subnets.*

2. Integrity
• *Data transfer control No unauthorized reading, copying, changes or deletions of data with electronic transfer or transport, e.g., encryption, electronic signature,*
• *Data entry control Verification, whether and by whom personal data is entered into a data processing system, is changed or deleted, e.g., logging, document management.*

3. Availability and Resilience
• *Availability control Prevention of accidental or willful destruction or loss, e.g., backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS), virus protection, firewall, reporting procedures and contingency planning,*
• *Rapid recovery.*

4. Procedures for regular testing, assessment, and evaluation
• *Data protection management,*
• *Data protection by design and default (Article 25 Paragraph 2 GDPR),*
• *No third-party data processing without corresponding instructions from the Controller, e.g., unambiguous contractual arrangements, formalized order management, strict controls on the service provider selection, duty of pre-evaluation, and supervisory follow-up checks.*

5. Other
• *Single Sign-On (SSO) - SAML single-sign-on gives users a centralized and secure way of controlling access to their organizations. Survicate supports SSO via SAML 2.0 standard. We have dedicated tutorials for Okta and OneLogin, but it's also possible to integrate with other providers for as long as they support SAML 2.0.*
• *Content Security Policy (CSP) is a security standard introduced to prevent code injection attacks resulting from the execution of malicious content in the trusted web page context.*
• *Incident response management,*
• *Measures for ensuring events logging;*
• *The information risk assessment program defines periodic identification of risks, vulnerabilities and mitigation mechanisms across the Survicate organization, which is verified through appropriate management levels and dedicated internal functions,*
• *Application tests are carried out periodically in accordance with generally accepted methodologies, including OWASP TOP10 and developed good internal practices for conducting security tests. Pen-tests are also regularly carried out by external auditors. All identified gaps are removed or corrected in the time adequately to the severity of the gap, critical or high gaps - immediately, remaining gaps - in the normal software development cycle,*

• *Survicate has a patch management program that fixes security flaws with patches. Administrators are required to distribute software patches effectively,*
• *The firewall rule sets are checked regularly to determine if corrections are needed. Device configuration is performed to obtain current security standards,* • *The organization maintains an up-to-date complex antivirus engine and runs periodic antivirus scans,*
  • *The formal risk assessment process is adjusted to GDPR requirements and internal policies. The organization assesses the effectiveness of the information security program through periodic assessments and/or audits to implement appropriate technical and organizational measures ensuring a level of security appropriate to the identified risks,*
• *Considering that Survicate operates in the AWS cloud environment, all kinds of IT infrastructure-related vulnerabilities are additionally searched by AWS and reported to Survicate on a daily basis. AWS are independent third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives. AWS Reports: AWS SOC 1 Report, AWS SOC 2 Security, Availability & Confidentiality Report, AWS SOC 2 Privacy Type I Report, AWS SOC 3 Security, Availability & Confidentiality Report, ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2019, ISO/IEC 27701:2019, ISO/IEC 9001:2015, ISO/IEC CSA STAR CCM v3.0.1.*
• *Survicate holds*
  - *PCI DSS Merchant Compliance Certificate and*
  - *ISO 27001:2023 Certificate .*

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller

Description of the specific technical and organisational measures to be taken by the processor to be able to provide assistance to the controller.

ANNEX III: LIST OF SUB-PROCESSORS

For Module 2 and Module 3

EXPLANATORY NOTE:

This Annex needs to be completed in case of specific authorisation of sub-processors (Clause 7.7(a), Option 1).

The controller has authorised the use of the following sub-processors:

Here is the full list of providers:

No	Entity Name	Country	Service/purpose of data processing
1	Amazon Web Services EMEA SARL	Luxemburg/ Ireland	IT infrastructure
2	BUNNYWAY, informacijske storitve d.o.o.	Slovenia	Content delivery network
3	OpenAI, L.L.C.	Republic of Ireland, USA	Artificial Intelligence, data analysis and summarization
4	Cloudflare, Inc.	USA	Network traffic security improvement, assisting with content delivery and DDoS protection
5	Datadog, Inc.	USA	Security log processing and analysis

6	Sendgrid (Twilio, Inc.)	USA	Email notifications deliver information to the user about responses provided by respondents.
7	Cloudinary, Inc.	USA	Managing and optimizing images and videos for enhancing the visual quality and engagement of online surveys; optimized delivery through a content delivery network (CDN).
8	Intercom, Inc.	USA	Managing customer interactions, support case management, communication for problem-solving with the tool
9	Linear Orbit, Inc.	USA, Belgium	Support case management, coordination of problem-solving with the tool
10.	AssemblyAI, Inc.	USA	API to transcribe Audio/Video recordings, for Insights Hub service purposes
11.	Anthropic Ireland, Limited	USA, Ireland	Artificial Intelligence, data analysis and summarization
12.	Google LLC, Google Ireland Limited, Google Cloud Poland Sp. z o.o.	USA, Ireland, Poland	Open-text responses translation feature using Google API
13.	DeepL SE	Germany, European Economic Area	Translating survey content & open-text responses