JOINT CONTROLLERSHIP AGREEMENT

Last updated: December 12, 2022

This Joint Controllership Agreement (the "**Agreement**") defines the regulation of the relationship between Snovio Inc. (the "**Company**", "**Snov.io**", "**Snovio**", "**we**", "**us**" or "**our**") and Clients of the Company who use the Company's services (the "**Client**", "**you**" or "**your**") regarding the processing of Prospects' personal data by Snovio and Client and supplements the Snovio's Terms and Conditions (hereinafter '**Terms**'), the agreement between you and Snovio Inc., which is governing your use of the Services.

ALL CLIENTS OF THE COMPANY ARE REQUIRED TO READ THIS JOINT CONTROLLERSHIP AGREEMENT TO UNDERSTAND HOW COMPANY USES, PROCESSES AND STORES PROSPECTS' PERSONAL DATA WHILE PROVIDING SERVICES TO THE CLIENTS.

1. DEFINITIONS

"Joint controller" means the natural or legal person, public authority, agency or other body, which jointly with other controllers determines the purposes and means of the processing of personal data.

"Personal data" means any information relating to a data subject, namely an identified or identifiable natural personal.

"Prospect" means a third-party data subject whose personal data related to their business interests or occupation is used in the process of providing services by us to our clients within our Platform..

"Services" means sourcing, lead generation and sales automation services provided by the Company via online platform and web application to Clients.

"Platform" means collectively the website https://snov.io/, web and mobile application app Snov.io, API methods available by api.snov.io hostname.

"Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

"GDPR" means the regulation (EU) 2016/679 of the European Parliament and of the Council of the 27th of April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

"Profiling" means any automated profiling, namely any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behavior.

2. GENERAL PROVISIONS

2.1. When processing personal data of Prospects, parties shall respect the obligations set forth in this Agreement and in the applicable laws and regulations.

2.2. Snovio and you may act as the joint controllers of the following personal data of Prospects: email address and/or first name, last name, corporate email, location (not precise), industry, current and previous position, place of work, links to social media (the "Prospect data").

2.3. Snovio and you are the joint controllers of the Prospects' data regarding the processing of such personal data.

2.4. Parties jointly determined that purposes of the processing of the Prospects' data are as follows:

for Clients, to process (store, use, delete, etc.) the Prospects' data within the Platform to be able to use the Services;
for Snovio, to provide Services to you and other Clients and maintain the operation of the Platform.

2.5. Parties jointly determined that the Prospects' data hereunder shall be processed by the means specified in Snovio's [Terms and Conditions](#) incorporated by reference hereunder.

2.6. Snovio processes Prospects' data on a basis of article 6(1)(f) of the GDPR and pursuant to the respective warranties specified in section 4 hereunder. Legitimate interests of Snovio, clients and Prospects are as follows:

contribute to business cooperation between you and your potential business partners;
create and assist in discovering new business-targeted marketing and sales opportunities for you and your potential business partners;
allow you to expand your database of the potential business partners;
develop the new unique platform that simplifies and facilitates professional interaction between businesses;
allow you to use an online platform for businesses that combines sales, CRM, analytics, marketing and email service functionality;
allow your potential business partners to approach new potential and verified clients or suppliers;
allow your potential business partners to commercialise the use of their publicly posted information related to their professional or business interests/occupation.

2.7. Snovio has completed the balancing test and verified that the fundamental rights and freedoms of the Prospects that require protection of the Prospects 'personal data do not override the legitimate interests of Snovio, Clients and Prospects specified in clause 2.6 herein.

2.8. Snovio stores Prospects' personal data for the entire period during which you use the Services and for 3 (three) months after the termination of the Client's account on the Platform. However, Snovio may store particular Prospects' data thereafter for the entire period during which other Clients use the Services if you and other Clients have simultaneously provided such Prospects' data to Snovio, but in any case only as long as necessary to provide Services to you and other Clients hereunder.

2.9. Snovio and you may have other processing roles and status during other processing operations involving the Prospects' personal data or other personal data as provided under Snovio's [Privacy Policy](#) and other personal data policies/agreements.

3. DATA TRANSFER

3.1. Snovio may transfer Prospects' personal data to its contractors located in third countries outside the EU, including the onward transfers of the personal data from the third countries to other third countries, inter alia in the USA.

3.2. Snovio may transfer Prospects' personal data as specified in clause 3.1 afore to the following contractors:

Name	Country of location	Website	Data transfer policy

Amazon Web Services	USA	https://aws.amazon.com/?nc2=h_lg	https://aws.amazon.com/privacy/?nc1=f_pr
Snovio's outsource technical, legal, sales and marketing specialists	Ukraine, USA, Brazil, China	-	Non-disclosure agreements and Data Processing Agreement signed between Snovio and each outsource specialist.

3.3. If so, Snovio may transfer Prospects' personal data to its contractors located in third countries outside the EU, including the onward transfers of the personal data from the third countries to another third countries, only on a basis of the appropriate safeguards, namely standard data protection clauses between Snovio and its contractors. Such standard data protection clauses embodied in company's public documents may be provided either by Snovio or by Snovio's contractors.

3.4. Snovio undertakes appropriate technical and organizational measures to secure the transfer Prospects' personal data to its contractors located in the third countries outside of the EU and onward, namely:

written information and access security policies and procedures;
encryption of all transferred data;
protected server and admin panel access via corporate VPN network only;
two-factor authentication of Snovio team members who access Prospects' personal data;
limitation of access to Prospects' data based on authority and tasks of the departments;
security measures implemented by contractors specified in their data transfer policies enlisted in clause 3.2 afore, e.g. key management, threat detection, DoS and DDoS protection, rotate, manage, and retrieve secrets, deployment of public and private SSL/TLS certificates etc.

3.5. Snovio DOES NOT sell or trade personal data to any legal persons or individuals. Snovio DOES NOT use Profiling.

4. REPRESENTATIONS AND WARRANTIES

4.1. Each party undertakes to implement appropriate technical and organisational measures that complies with applicable laws and regulations designed to:

ensure and protect the security, integrity and confidentiality of the Prospects' data; and
protect the Prospects' data against any unauthorized processing, loss, use, disclosure or acquisition of or access.

4.2. Each party ensures that the Prospects' data is accurate and undertakes to notify the other Party with undue delay if it becomes aware of inaccuracies in the Prospects' data.

4.3. You hereby represent and warrant that:

you collected the Prospects' data on a lawful basis provided under the GDPR;
transfer of the Prospects' data to Snovio and further processing of the Prospects' data by Snovio do not violate the Prospects' rights and interests AND rights and interests of any third parties AND complies with the requirements of GDPR and all applicable laws and regulations;
you will comply with the GDPR provisions, in particular with the controller's transparency obligations to provide all data subjects whose Prospect's data you obtain using Snovio services and

tools with all the information indicated in Articles 13 and 14 of the GDPR within a period provided by the GDPR, including at the latest at the time of the first communication to that data subject as (i) informing all data subjects whose Prospect's data Clients provide Snovio with regarding the processing of their data constitutes disproportionate efforts for Snovio and (ii) processing of the Prospect's data does not always allow Snovio to obtain the correct contact details of the data subject to inform them on the fact of data processing;

you will inform us of any Prospects' complaints, claims or requests related to the respective Prospects' data and will not undertake any actions in this regard without the approval of Snovio;

you will fulfil all data subjects' requests related to the processing of personal data as specified herein without undue delay and according to your capacity; whether your capacity does not allow to fulfil the particular data subject's request, you will undertake best possible efforts to facilitate the fulfilment of such request;

you informed all Prospects whose Prospects' data you transferred to Snovio of the possible risks of the data transfer specified in section 3 hereof pursuant to the absence of an adequacy decision under the GDPR in this regard and none of the respective Prospects objected to such transfer;

you will inform us of any complaints, claims or requests from supervisory authority related to the respective Prospects' data and will not undertake any actions in this regard without the approval of Snovio;

you will promptly and properly deal with all inquiries from Snovio regarding the processing of the Prospects' data;

you will promptly notify Snovio of the commencement of any litigation or proceedings against Snovio or any of its officers/employees/contractors etc. in connection with the processing of the Prospects' data as specified hereunder;

you apply the appropriate security measures to protect the Prospects' data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation.

4.4. Snovio fully relies on the representations and warranties provided above during the processing of the Prospects' data as specified hereunder.

4.5. You agree to indemnify and hold harmless Snovio and each of its directors, officers, employees, contractors and any person, if any, who controls Snovio against any loss, liability, claim, damages or expense (including the reasonable cost of investigating or defending any alleged loss, liability, claim, damages, or expense and reasonable counsel fees incurred in connection therewith) arising, including without limitation by reason of:

any actions or omissions committed by you, your directors, officers, employees, contractors or any related person;

violation of any representations or warranties specified afore;

filing complaints regarding the processing of the Prospects' data as specified hereunder regardless whether such complaints were filed by the Prospect(s) or not; and

decision of the supervisory authority.

5. DATA SUBJECTS RIGHTS

5.1 Data subjects whose personal data are processed as specified hereunder may exercise the following rights:

right to access, namely to know whether their personal data are being processed and if so, access such data;

right to rectification, namely to ask the Snovio or you to correct his/her personal data if they are inaccurate;

right to erasure ("right to be forgotten"), namely to obtain from the Snovio the erasure of his/her personal data without undue delay and the Snovio has to erase such personal data without undue

delay;
right to restriction of processing, namely to limit processing of his/her personal data with several exceptions under the scope of the GDPR;
right to be informed, namely you are obliged to inform data subjects of what data is being collected, how it's being used, how long it will be kept and whether it will be shared with any third parties; this information must be communicated concisely and in plain language;
right to data portability, namely to obtain and reuse his/her personal data for his/her own purposes across different services; this right only applies to personal data that data subject has provided Snovio/you with by way of the consent;
right to object, namely to object to the processing of personal data that are being processed by the Snovio; Snovio stops processing of personal data unless Snovio can demonstrate the compelling legitimate grounds for the processing that overrides the interests, rights and freedoms of the individual or if the processing is undertaken for the establishment or exercise of defense of legal claims;
right not to be subject to a decision based solely on automated processing, namely to object to Profiling that is occurring without consent; herewith, data subjects may request their personal data to be processed with the human involvement;
right to lodge a complaint with the supervisory data protection authority pertaining to the processing of your personal data.

5.2 Any data subject may exercise any of the rights provided above by sending a request to the e-mail address help@snov.io or by contacting Snovio via the Platform's chat window available at https://snov.io/ or realize right to erasure or right to object via Snovio's Clear Email tool to automatically delete their email address from the Platform for further use by Clients within the Platform. Any request of data subject must include name, contact information of the data subject, right which data subject wants to exercise, personal data processed by the Snovio/Client, details and reason/justification of such request.

5.3 Periods of fulfillment of data subjects' requests (taking into account that periods start since the moment Snovio/Client receives the request) are as follows:

Right to be informed - when data is collected;
Right to access - 1 month;
Right to rectification - without undue delay;
Right to erasure - without undue delay;
Right to restrict processing - 1 month;
Right to data portability - 1 month;
Right to object - on receipt of objection;
Rights in relation to automated decision making and profiling - 1 month.

5.4 In some cases, a data subject has the right to lodge a complaint about the use of his/her personal data with a data protection authority. If so, the data subject shall contact his/her national data protection authority. Parties hereby represent and warrant to cooperate with the appropriate governmental authorities to resolve any privacy-related complaints that cannot be amicably resolved between the data subject and any of the parties.

6. REQUESTS OF PROSPECTS

6.1. If you receive any complaint, claim or request from the Prospect regarding the use of the respective Prospects' data, you shall undertake to inform us of it immediately and avoid taking any actions in reaction to the received complaint/claim/request without the approval of Snovio.

6.2. Subject to the consultation with/approval of Snovio, you warrant to fulfil all data subjects' requests related to the processing of personal data as specified herein without undue delay and according to your capacity. Provided that your capacity does not allow you to fulfil the particular data subject's request, you will undertake best possible efforts to facilitate the fulfilment of such request.

6.3. If Snovio receives any complaint, claim or request from the Prospect regarding the use of the respective Prospect's data, we shall immediately notify you of this request and take the necessary preliminary actions, e.g., send a response to the Prospect acknowledging the receipt of the request/claim/complaint and informing them of the proposed further action to be taken on our part.

6.4. You undertake to respond to Snovio's notification specified in clause 6.3 herein within twenty four (24) hours and provide the necessary explanations, required information, any other details and available instructions requested by the Snovio to serve the Prospect's complaint/claim/request. If you fail to respond, you hereby authorise Snovio to choose the way of fulfilment of such complaint/claim/request at our sole discretion, including the erasure of the Prospect's data specified by the Prospect.

7. DATA BREACHES

7.1. Parties will notify each other as soon as possible of any potential or actual loss of the Prospects' data and/or any breach of the technical and/or organizational measures taken, but, in any event, within 24 hours after identifying any potential or actual loss and/or breach.

7.2. Parties will provide each other with reasonable assistance as required to facilitate the handling of any Data Breach.

8. RESOLUTIONS OF DISPUTES AND CLAIMS RELATED TO PERSONAL DATA

If the Prospect, data protection authority or any other person brings a dispute or claim concerning the processing of the Prospects' data against Snovio or both Parties, Parties will inform each other about such disputes or claims and will cooperate with each other as far as permitted by the applicable laws and regulations.

9. COMMENCEMENT, DURATION AND SURVIVAL

9.1. This Agreement shall commence on the date specified in the beginning of the Agreement and shall last for the entire period of provision of Services and processing of the Prospects' data as specified hereunder.

9.2. The obligations set forth in this Agreement shall survive the expiration or termination (for whatever reason) of the Parties' cooperation for as long as the processing of the Prospects' data as specified hereunder will take place.

10. NULLITY

If any provision of this Agreement is null and void or cannot be otherwise enforced, the remaining provisions will remain in full force. Parties will then agree on a provision that approximates the scope of the void or unenforceable provision as much as possible.

11. GOVERNING LAW AND RELATED DOCUMENTS

11.1. All disputes relating to this Agreement, its execution and interpretation OR any Prospects' data hereunder will be governed by the substantive law of the State of Delaware, USA.

11.2. All disputes relating to this Agreement, its execution and interpretation OR any Prospects' data hereunder will be submitted to the competent courts in the State of Delaware, USA.

11.3. The following documents and policies constitute an integral part of this Agreement:

Snovio's Terms and Conditions available at https://snov.io/t_and_c;
Snovio's Privacy Policy available at https://snov.io/privacy-policy.

12. TRANSFER OF PERSONAL DATA

12.1. You acknowledge and agree that with regard to the transfer of personal data under this Agreement, you can be considered a data controller and Snovio can be simultaneously considered as a data controller (as defined by the GDPR), as further described in the Standard Contractual Clauses agreed under this Agreement (the "**Clauses**").

12.2. These Clauses form an integral part of this Agreement and shall not apply to situations where Snovio acts as a processor in accordance with Snovio's Privacy Policy and respective Data Processing Addendum (DPA).

12.3. Both parties agree to abide and process personal data protected by the GDPR in compliance with the Standard Contractual Clauses approved by the European Commission decision 2021/914 of 4 June 2021 in order to adduce adequate safeguards with respect to protection of privacy and fundamental rights and freedoms of natural and legal persons for transfer of personal data specified in Annex I. For the purposes of the descriptions in the Clauses, both parties agree that Snovio is the 'data exporter' and you are the 'data importer'.

COMPANY DETAILS:

Snovio Inc., a Delaware company, company number 6896854;

Address: 220 East 23rd Street, 5th Floor, Office 500, New York, 10010 USA.

Data Protection Officer (external):

Legal IT Group LLC

Office 1, 38 Volodymyrska Str.

01030 Kyiv, Ukraine

Email: snovio_dpo@snov.io.

Standard Contractual Clauses

SECTION I

Clause 1. Purpose and Scope

For the purposes of the Clauses:

(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 8.5 (e) and Clause 8.9(b);

(iii) Clause 11(a) and (d);

(iv) Clause 12;

(v) Clause 14.1(c), (d) and (e);

(vi) Clause 15(e);

(vii) Clause 17(a) and (b).

(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. 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 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. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 9, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties 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.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

8.5 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 personal data, including 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, 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.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) 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 personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 12. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 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 or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefiting 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 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

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

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject. Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9. Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 11(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

Clause 10. 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.

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

(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 12; (ii) refer the dispute to the competent courts within the meaning of Clause 17.

(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 11. 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.

Clause 12. Supervision

(a) 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.

(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 13. Local laws and practices affecting compliance with the Clauses

(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 15(d) and (e) shall apply.

Clause 14. Obligations of the data importer in case of access by public authorities

14.1 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 13(e) and Clause 15 to inform the data exporter promptly where it is unable to comply with these Clauses.

14.2 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 13(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 15. 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 13(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 16. Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Federal Republic of Germany.

Clause 17. 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 the Federal Republic of Germany.

(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.

Appendix

Annex I

A. LIST OF PARTIES

Data exporter

Name: Snovio Inc.

Address: 220 East 23rd Street, №401, New York, NY, USA 10010

Contact person's name, position and contact details: the Director Eugene Medvednikov, admin@snov.io

Activities relevant to the data transferred under these Clauses:

- Collection;
- Recording;
- Organisation;
- Structuring;
- Storage;
- Adaptation or alteration;
- Retrieval;
- Consultation;
- Alignment or combination;
- Restriction;
- Erasure or destruction.

Signature and date: The parties agree that execution of Snovio's Terms and Conditions by the data importer shall constitute execution of these Clauses by both the data importer and data exporter. The date of the registration of the account on the Snovio platform shall be considered the date of execution of these Clauses.

Role: controller

Data importer

Name: You, «Client», «User»

Address: the relevant information is contained in the Client's account.

Contact person's name, position and contact details: the relevant information is contained in the Client's account.

Activities relevant to the data transferred under these Clauses:

- Collection;
- Recording;

- Organisation;
- Structuring;
- Storage;
- Adaptation or alteration;
- Retrieval;
- Consultation;
- Alignment or combination;
- Restriction;
- Erasure or destruction.

Signature and date: The parties agree that execution of Snovio's Terms and Conditions by the data importer shall constitute execution of these Clauses by both the data importer and data exporter. The date of the registration of the account on the Snovio platform shall be considered the date of execution of these Clauses.

Role: controller

B. DESCRIPTION OF TRANSFER

1. Categories of data subjects whose personal data is transferred:

- Clients' prospects.

2. Categories of personal data transferred: Prospect data: email address and/or first name, last name, corporate email, location (not precise), industry, current and previous position, place of work, links to social media.

3. Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved:

The data importer does not obtain access to the special categories of data (sensitive data).

4. The frequency of the transfer:

The personal data is transferred on a continuous basis.

5. Nature of the processing:

Personal data processing consists of the following: collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, alignment or combination, restriction, erasure or destruction.

6. Purpose(s) of the data transfer and further processing:

The purpose of the data processing under these Clauses is the performance of the services for data importer by the data exporter under the Terms concluded between the data importer and the data exporter.

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

The personal data shall be stored for the duration of this Agreement concluded between the data importer and the data exporter, unless otherwise agreed in writing or the data importer is required by applicable law to retain some or all of the transferred personal data.

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

The data importer may engage other processors, for example, for providing secure transfer and storage of personal data on servers. Such processing may involve collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, alignment or combination, restriction, erasure or destruction of personal data. The personal data transferred to processors shall be deleted after the end of the provision of the services by the data exporter under the Terms, unless the data importer is required by applicable law or contractual obligations to retain some or all of the transferred personal data.

C. COMPETENT SUPERVISORY AUTHORITY

In accordance with Clause 12, competent supervisory authority under these Clauses is the Federal Commissioner for Data Protection and Freedom of Information (BfDI) (Federal Republic of Germany).

Annex II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The technical and organisational measures implemented by the data importer(s) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons is described in the data importer's Privacy Policy or in any other document provided that such document contains the list of technical and organisational measures implemented by the data importer.