VARTION'S GENERAL TERMS AND CONDITIONS
ADDENDUM A

## Addendum A: DATA PROCESSING TERMS FOR WITHIN THE EEA AND UK

### GENERAL

### 1 Applicability and capacity

1.1. These Data Processing Terms are applicable if the Client is a sole proprietorship, partnership or entity organized under its applicable law but located and having its principle office in any country within the EEA or UK.

1.2. Vartion can be both a Data Controller and Data Processor with providing the Software and/or Services. Depending on the different aspects of the Service and/or Software Vartion shall either be Data Controller or Data Processor. For instance:

(a) In case of Software being modified due to the generating and analysing of Personal Data entered into the system by the Client, Vartion considers itself a Data Controller. The Client is a Data Controller with regard to the Software or the Service.
(b) With regard to Pascal onboarding, Pascal screening and Pascal transaction monitoring Vartion shall be considered a Data Processor and the Client a Data Controller.
(c) With regard to the provision of Services, either related to the Software or otherwise, Vartion shall be a Data Processor, except when agreed otherwise. The Client shall be a Data Controller and instruct Vartion as to how to use the Personal Data.
(d) In the instances that Vartion can instruct or use the Personal Data for its own means, Vartion shall be considered a Data Controller. The Client shall also be considered a Data Controller in these instances.

1.3. In the case that Vartion exports Personal Data it is considered a Data Exporter and the Client the Data Importer. In case Vartion imports Personal Data it is considered a Data Importer and the Client is considered a Data Exporter. Parties can be regarded both Data Exporter and Data Importer within the same Agreement. For instance:

(a) With regard to the Software and SaaS-Service Vartion is the Data Importer when the Personal Data is entered into the system of the Software. Vartion is regarded a Data Exporter when Vartion generates and displays results to the Client in which case the Client is the Data Importer; and
(b) With regard to the Services the Personal Data that is provided by the Client to Vartion the Client is Data Exporter and Vartion Data Importer. If Vartion processes the provided Personal Data and the Client gets access to the processed Personal Data, Vartion is considered a Data Exporter and the Client a Data Importer.

1.4. In any case Annex I up and until Annex III shall be applicable. For each specific processing of Personal Data the applicable module shall apply.

1.5. If there is any contradiction between the Agreement, General Terms and Conditions, the Data Processing Terms or the Annexes, the following order shall apply:

1. the Annexes;
2. these Data Processing Terms;
3. the Agreement; and lastly
4. the General Terms and Conditions.

1.6. if the selection that the Parties are Controllers, Processors or Sub-Processors is wrong (either as a matter of fact or as a result of applying the EU Data Protection Laws) then:

(a) the terms and conditions of the Data Processing Terms which apply to the correct option which was not selected will apply; and

(b) the Parties and any relevant Data Subjects are entitled to enforce the terms and conditions of Data Processing Terms which apply to that correct option.

## 2 Term of Processing

2.1 The term for processing is as long as the Agreement is into place and it is necessary to process the Personal Data to execute the Agreement, hereinafter the Term of Processing.

## OPTION 1: VARTION IS DATA PROCESSOR AND CLIENT IS DATA CONTROLLER

## 1 Data deletion

1.1. If the Client does not have the option to delete Personal Data during the provision of Software and related technical support and/or Services, Vartion will comply with any reasonable request from the Client to enable the deletion of such data, to the extent possible considering the nature and functionality of the Processing Services. This shall not apply when storage is required by Applicable Law.

1.2. Upon expiration of the term of the Agreement, the Client hereby instructs Vartion to delete or return all Personal Data provided by the Client, in accordance with Applicable Law. Vartion shall delete all copies of the Personal Data from Vartion's systems. Vartion will comply with this instruction as soon as reasonably practicable unless: (i) storage is required by the Applicable Law, or (ii) the Agreement has been continued in or replaced by a new agreement or terms between Client and Vartion relating to Client's use of the Services and Client confirms that the processing of Client's Personal Data should continue in accordance with these Data Processing Terms.

## 2 *Security measures*

2.1. Vartion does not guarantee that its security measures shall be effective under all possible circumstances.

2.2. Vartion will implement such measures to ensure a level of security appropriate to the risk involved, such as:

(a) the pseudonymisation and encryption of Personal Data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

2.3. Vartion takes reasonable measures to isolate and protect the Personal Data. A list of security measures is added in Annex II.

## 3 Data incidents

3.1. In the case that Vartion has become aware of a Data Incident, Vartion will: (i) promptly and without delay notify the Client of the Data Incident; and (ii) promptly take reasonable steps to minimize the damage and secure the Personal Data.

3.2. The notification as mentioned in Clause 3.1. sub (i) will include a description of the Data Incident, the involved Data Subject and the Personal Data to the extent that a description is possible. This shall include the measures that have been taken by Vartion, the potential risks and a suggestion of the measures the Client can undertake to address the Data Incident, including, where appropriate, measures to mitigate any adverse consequences thereof.

3.3. The notification and information will be disclosed to the contact information as has been disclosed to Vartion.

3.4. Immediately following any accidental, unauthorised or unlawful Personal Data processing or Data Incident, the Parties will co-ordinate with each other in order to investigate the matter. Vartion and the Client can enter into negotiation on the possible assistance of the Client's handling of the matter.

3.5. The Client is solely responsible for complying with Data Incident reporting legislations applicable to Client and complying with any reporting obligations to third parties in connection with Applicable Law.

3.6. If Vartion incurs any additional costs for complying with this Clause 3 it is entitled to invoice the Client, at rates applicable at the time.

3.7. Notice of or response to a Data Incident by Vartion under this Clause 3 shall not be construed as an admission by Vartion of fault and/or liability with respect to the Data Incident.

## 4 Responsibilities of the Client

4.1. The Client acknowledges its own responsibilities with regard to EU Data Protection Laws and other Applicable Law.

4.2. Vartion has no obligation to protect the Personal Data that Client elects to store or transfer outside the systems of Vartion and that of Vartion's sub-processors.

4.3. The Client shall use the Services and ensure a level of security appropriate to the risk associated with the Personal Data.

4.4. The Client shall secure authentication credentials of accounts, systems and devices used by Client to access and use the Services.

4.5. The Client confirms that the security measures taken and maintained by Vartion, as described in the Data Processing Terms, provide a level of security appropriate to the risk regarding the Personal Data.

## 5 Audit rights and assessment

5.1. If the Client has grounds to believe that the Personal Data is not being processed in accordance with the Processing Terms, then Vartion will give all necessary and reasonable assistance to an independent expert in case of an audit which audit's scope is limited to verifying the Vartion's compliance with its obligations under the Data Processing Terms and the Client has notified Vartion of the reasons for conducting such an audit.

5.2. Vartion has the right to object against a third-party auditor when Vartion's reasonable opinion, is not properly qualified or independent, is a competitor of Vartion or is otherwise manifestly unsuitable.

5.3. In the event of such an objection by Vartion, Vartion shall appoint another auditor or conduct the audit itself. The Client shall contact Vartion for an audit. The start date and end date and further specifications of such audit shall be discussed and agreed upon by the Parties.

5.4. Vartion shall not comply with instructions from the auditor if Vartion deems such instructions to be inconsistent with EU Data Protection Laws or Applicable Law.

5.5. Vartion is not obliged to disclose any information which regards the data of other Clients, accounting and financial statement of Vartion, Vartion's company secrets, trade secrets, any information which could endanger the security of Vartion's systems, any information which could result in Vartion breaching her legal obligations, or any information to which the Client or its third-party auditor wishes to obtain access for any reason other than good faith compliance with the Client's obligations under the EU Data Protection Laws.

5.6. The expert shall be bound by a duty of confidentiality with regard to the findings in relation to such audit and shall only notify the Client of matters which cause Vartion to fail to comply with its obligations under the Processing Terms. The expert shall provide Vartion with a copy of the rapport relating to such audit.

## **6** Rights of the Data Subjects

6.1. When Vartion receives a request from a Data Subject in connection with the Personal Data, Vartion will refer the Data Subject to submit his/her/its request to the Client. Client shall be responsible for responding to such request.

6.2. Vartion will notify the Client of requests or complaints related to the Processing and will assist the Client in responding to any complaint, notice, communication or Data Subject request, in accordance with article 28(3)(e) of the EU Data Protection Laws.

6.3. Vartion will take such technical and organisational measures as may be reasonable and appropriate, and may provide such necessary information to the Client to enable the Client to comply with its legal obligations concerning:

(a) the rights of data subjects under the EU Data Protection Laws and other data protection legislation, including, but not limited to, subject access rights, the rights to rectify, the right to data portability and erasure of Personal Data, object to the processing and automated processing of Personal Data, and restrict the processing of Personal Data; and

(b) information or assessment notices served by the Commissioner or other relevant Supervisory Authority on the Client related to its Personal Data obligations under the Applicable Law.

6.4. If the Client is required to carry out a Data Protection Impact assessment or a subsequent consultation within the meaning of articles 35 and 36 of the EU Data Protection Laws, then Vartion shall endeavour to cooperate therewith.

## 7 Data transfers

7.1. Vartion will not transfer or otherwise process the Personal Data outside the UK or the EEA, without obtaining the Client's prior written consent. This consent shall not unreasonably be withheld.

## 8 Data Liability

8.1 Notwithstanding any provision in the Agreement to the contrary, the aggregate liability of each party to the other party under or in connection with these Data Processing Agreement shall be limited to the maximum amount to which the Party's liability under the Agreement is limited.

8.1.1 Administrative fines imposed on the Client by a Supervisory Authority cannot be recovered from Vartion.

## 9 Sub-processors

9.1.1 The Client provides Vartion hereby with a general authorisation to engage sub-processors. Vartion will ensure that its sub-processors will adhere to the same standard as this Agreement holds.

VARTION'S GENERAL TERMS AND CONDITIONS
ADDENDUM A

OPTION 2: BOTH PARTIES ARE CONTROLLER

## 1 Applicability

1.1 Due to the fact that both Parties are a controller in this instance, but depending on the specific Personal Data related activity is either an exporter or importer of Personal Data, the terms Data Exporter and Data Importer shall be used, either meaning Vartion or the Client depending on the circumstances.

1.2 The Data Importer shall process the Personal Data only for the specific purpose(s) of the transfer, as set out in Annex I.

1.3 Personal Data can be processed by modifying, retrieving, using, disclosing, merging, erasing and destroying Personal Data for the purpose of providing the Software and in some instances Services in accordance with these Data Processing Terms.

1.4 Vartion can also process the Personal Data that has been generated by use of the Service or Software by the Client or User. Vartion will only process the Personal Data to the extent, and in such a manner, as is necessary for the Agreement and aligns with the purpose of processing as set out in Annex I.

1.5 The Client retains control of the Personal Data and remains responsible for its compliance obligations under EU Data Protection Laws and other data protection laws, and the Client will ensure that the Client has any required notices and consents in place to enable lawful processing of the Personal Data by the Client.

1.6 References to certain Articles are references to the relevant articles in the EU Data Protection Laws.

## 2 Transparency

2.1 In order to enable data subjects to effectively exercise their rights pursuant to Clause 7, the Data Importer shall inform them, either directly or through the Data Exporter:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2.2 In addition to the information referred to in Clause 2.1, the Data Importer shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

(d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(e) the right to lodge a complaint with a supervisory authority;

(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

(g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2.3 The Data Importer shall provide the information referred to in Clauses 2.1 and 2.2:

(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

2.4 Where the Data Importer intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in Clause 2.

2.5 Clause 2.1 up and until 2.4 shall not apply where and insofar as:

(a) the data subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

## 3 Accuracy and data minimisation

3.1 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.

3.2 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.

3.3 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.

## 4 Storage limitation

4.1 The Data Importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed, in this case the provision of Service and/or Software on the Agreement. 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.

## 5 Security of processing

5.1 The Parties have agreed on the technical and organizational 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.

5.2 The Data Importer shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5.3 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.

5.4 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 Clause10.1. 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.

5.5 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 Clause 5.4., 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.

5.6 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.

## 6 Sensitive data

6.1 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.

## 7 Data Subject Rights

7.1 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.

7.2 In particular, upon request by the data subject the Data Importer shall, free of charge:

(a) 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; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 10.1;

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

(c) 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.

7.3 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.

7.4 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:

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

(b) 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.

7.5 Where requests from a data subject are excessive, in particular because of their repetitive character, the Data Importer may either charge a reasonable fee considering the administrative costs of granting the request or refuse to act on the request.

7.6 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.

7.7 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.

7.8 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.

## 8 Liability

8.1 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.

8.2 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.

8.3 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.

8.4 The Parties agree that if one Party is held liable under Clause 8.3 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.

8.5 The Data Importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

## 9 Dispute resolution

9.1 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.

9.2 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:

(a) 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 1§0.1l;

(b) refer the dispute to the competent courts within the meaning of Clause 19.2 of the General Terms and Conditions.

9.3 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 the EU Data Protections Laws.

9.4 The Data Importer shall abide by a decision that is binding under the applicable EU or Applicable Law.

9.5 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.

## 10 Supervisory authority

10.1 The supervisory authority with responsibility for ensuring compliance by the Data Exporter with the EU Data Protections Laws as regards the data transfer, as indicated in Annex I shall act as competent supervisory authority.

10.2 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.

## 11 Warranties

11.1 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 the EU Data Protections Laws, are not in contradiction with these Clauses.

11.2 The Parties declare that in providing the warranty in Clause 11.1 they have taken due account in particular of the following elements:

(a) 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;

(b) 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 safeguard;

(c) 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.

11.3 The Data Importer warrants that, in carrying out the assessment under Clause 11.2 (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.

11.4 The Parties agree to document the assessment under Clause 11.2 and make it available to the competent supervisory authority on request.

11.5 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 Clause 11.2, 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 Clause 11.2.

11.6 Following a notification pursuant to Clause 11.5, 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 [for Module Three: 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 13 shall apply.

## 12 Notification

12.1 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:

(a) 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

(b) 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.

12.1 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.

12.2 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.

12.3 The Data Importer agrees to preserve the information pursuant to this Clauses 12 for the duration of the Agreement and make it available to the competent supervisory authority on request.

12.4 These Clauses are without prejudice to the obligation of the Data Importer to inform the Data Exporter promptly where it is unable to comply with these Clauses.

## 13 Review of legality and data minimization

13.1 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 12.

13.2 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.

13.3 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.

## 14 Non-compliance with the Clauses and termination

14.1 The Data Importer shall promptly inform the Data Exporter if it is unable to comply with these Clauses, for whatever reason.

14.2 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 12.

14.3 The Data Exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(a) the Data Exporter has suspended the transfer of personal data to the Data Importer pursuant to Clause 14.2 and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(b) the Data Importer is in substantial or persistent breach of these Clauses; or

(c) the Data Importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

14.4 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.

14.5 Personal data that has been transferred prior to the termination of the contract pursuant to Clause 14.3 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.

14.6 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 the EU Data Protections Laws that covers the transfer of personal data to which these Clauses apply; or (ii) the EU Data Protections Laws become 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 the EU Data Protections Laws.

## ANNEX B: DATA PROCESSING AGREEMENT FOR OUTSIDE THE EEA AND UK

### GENERAL

### 1 Applicability and capacity

1.1. These Data Processing Terms are applicable if the Client is a sole proprietorship, partnership or entity organized under its applicable law but located and having its principle office in any country outside the EEA or UK.

1.2. De Data Processing Agreement shall commence at the moment the Parties have signed the relevant Agreement.

1.3. This Data Processing Terms are based on the European Standard Contractual Clauses and the UK Addendum published on 4 June 2021 and 21 March 2022 ("**SCC**") respectively, the relevant Clauses and modules apply as selected in Tabel 1. The Data Processing Agreement consists out of these Clauses and Annex I. The UK Addendum can be accessed via our website Vartion

1.4. If there is any contradiction between the Agreement, General Terms and Conditions, the Data Processing Agreement or the Annexes, the following order shall apply:

1. The SC and the Annexes;

2. these Data Processing Terms;
3. the Agreement; and lastly
4. the General Terms and Conditions.

1.5. In the case that Vartion exports Personal Data it is considered a Data Exporter and the Client the Data Importer. In case Vartion imports Personal Data it is considered a Data Importer and the Client is considered a Data Exporter. Parties can be regarded both Data Exporter and Data Importer within the same Agreement. For instance:

(a) With regard to the Software and Saas-Service Vartion is the Data Importer when the Personal Data is entered into the system of the Software. Vartion is regarded a Data Exporter when Vartion generates and displays results to the Client in which case the Client is the Data Importer; and
(b) With regard to the Services the Personal Data that is provided by the Client to Vartion the Client is Data Exporter and Vartion Data Importer. If Vartion processes the provided Personal Data and the Client gets access to the processed Personal Data, Vartion is considered a Data Exporter and the Client a Data Importer.

1.6. Vartion can be both a Data Controller and Data Processor with providing the Software and/or Services. Depending on the different aspects of the Service and/or Software Vartion shall either be Data Controller or Data Processor. For instance:
(a) In case of Software being modified due to the generating and analysing of Personal Data entered into the system by the Client, Vartion considers itself a Data Controller. The Client is a Data Controller with regard to the Software or the Service.
(b) With regard to Pascal onboarding, Pascal screening and Pascal transaction monitoring, Vartion shall be considered a Data Processor and the Client a Data Controller.
(c) With regard to the provision of Services, either related to the Software or otherwise, Vartion shall be a Data Processor, except when agreed otherwise. The Client shall be a Data Controller and instruct Vartion as to how to use the Personal Data.
(d) In the instances that Vartion can instruct or use the Personal Data for its own means, Vartion shall be considered a Data Controller. The Client shall also be considered a Data Controller in these instances.

1.7. In any case, regardless of each of the Parties capacity, Annex I shall be applicable.

1.8. if the selection that the Parties are Controllers, Processors or Sub-Processors is wrong (either as a matter of fact or as a result of applying the EU Data Protection Laws) then:
(a) the terms and conditions of the Data Processing Agreement which apply to the correct option which was not selected will apply; and
(b) the Parties and any relevant Data Subjects are entitled to enforce the terms and conditions of Data Processing Agreement which apply to that correct option.

## 2 Selected SSC

2.1 In table 1 the selected SCC are presented together with the additional information to complete the SCC.

### 1.1.1 Table 1: Selected SCCs, Modules and Selected Clauses

| | |
|---|---|
| Addendum EU SCCs | the Approved EU SCCs, including the Appendix Information |

| | and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum: | | | | | |
|---|---|---|---|---|---|---|
| Module | Module in operation | Clause 7 (Docking Clause) | Clause 11 (Option) | Clause 9a (Prior Authorisation or General Authorisation) | Clause 9a (Time period) | Is personal data received from the Importer combined with personal data collected by the Exporter? |
| 1 | Yes | No | No | | | Yes |
| 2 | Yes | No | No | general authorisation (option 2) | three months | Yes |
| 3 | | | | | | |
| 4 | Yes | No | No | not applicable | | Yes |

1.1.2

| Module | Module in operation | Clause 17 | Clause 18 |
|---|---|---|---|
| 1 | Yes | the Netherlands | the Netherlands |
| 2 | Yes | the Netherlands | the Netherlands |
| 3 | | | |
| 4 | Yes | the Netherlands | |

VARTION'S SPECIFIC TERMS AND CONDITIONS AND STANDARD CONTRACTUAL CLAUSES

*ANNEX I*

## A. DESCRIPTION OF TRANSFER

MODULE ONE: Transfer controller to controller MODULE TWO: Transfer controller to processor MODULE THREE: Transfer processor to processor MODULE FOUR: Transfer processor to controller *Categories of data subjects whose personal data is transferred*

| | |
|---|---|
| Relevant Data Subjects | The categories of Data Subjects will update automatically if the information is updated in the Linked Agreement referred to.<br><br>SECTION B: USE OF SERVICE<br>The Data Subjects will be adults in accordance with the country or nationality.<br><br>SECTION C: SAAS-SERVICE<br>The Data Subjects will be adults in accordance with the country or nationality. |

*Categories of personal data transferred*

| | |
|---|---|
| Relevant Personal Data | The categories of Personal Data will update automatically if the information is updated in the Linked Agreement referred to.<br><br>SECTION B: USE OF SERVICE<br>Personal Data categories will be names, aka's, address, date and place of birth, passport number(s), identity card number(s), nationality(-ies), profession, or possibly any other background data generated by using the Software.<br><br>SECTION C: SAAS-SERVICE<br>Personal Data categories will be names, aka's, address, date and place of birth, passport number(s), identity card number(s), nationality(-ies), profession, or any other background data generated by the Client using the Software. |

*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.*

| | |
|---|---|
| Sensitive data | Parties do not transfer Sensitive Data. If in any case 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, 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. The measures hereunder shall in any case be applied with data transferring. |
| Security of Transmission | - Use of data segregation; and<br>- Use of anonymization of data. |
| Security of Storage | - the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and<br>- Data backups (daily). |
| Security of Processing | - a process for regularly testing, assessing and evaluating the effectiveness of the security measures;<br>- Physical access controls.<br>- System access controls. |
| Organisational security measures | - Only the authorized employees of the Parties can access the data. Parties only work with systems that: (i) only allow authorized individuals to access the Personal Data to which they have been granted access; and (ii) ensure that the Personal Data cannot be read, copied, modified or deleted without authorization during processing.<br>- All employees of the Parties are instructed to conduct themselves in a manner consistent with the Party's guidelines regarding confidentiality, Personal Data protection, business ethics, appropriate use and professional standards; and<br>- Parties make use of password protection and use of passwords and two factor authentications. |
| Technical security minimum requirements | - Encryption of Personal Data;<br>- Use of antivirus;<br>- Use of Anti-Malware Software |

| | |
|---|---|
| Updates to the Security Requirements | - The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to. |

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

| | |
|---|---|
| Frequency of the transfer | SECTION B: USE OF SERVICE<br><br>During the Agreement, on various moments.<br><br>SECTION C: SAAS-SERVICE<br>The transfer shall happen when Personal Data is entered into the system and in turn results are being generated with that Personal Data, which is as frequent as the Client enters Personal Data into the system.<br><br>Monitoring<br>In the case of Monitoring, the Client is able to choose the frequency. With Monitoring the data transfer from new generated results, with Vartion as Data Exporter, shall happen on a more frequent basis which frequency is decided by the Client. |

VARTION'S SPECIFIC TERMS AND CONDITIONS AND STANDARD CONTRACTUAL CLAUSES

*Nature of the processing*

| | |
|---|---|
| Nature of the processing | SECTION B: USE OF SERVICE<br><br>Vartion can process by collecting, capturing, organizing, structuring, storing, modifying, retrieving, using, disclosing, merging, erasing and destroying Personal Data for the purpose of providing the Services and technical support to Client for Software in accordance with these Data Processing Agreement. Vartion will only process the Personal Data to the extent, and in such a manner, as is necessary for the Agreement in accordance with the instructions of the Client.<br><br>SECTION C: SAAS-SERVICE<br><br>Vartion processes Personal Data relating to individuals provided to Vartion via the SaaS-Service, by (or at the direction of) the Client or by its Users. Vartion can also process the Personal Data that has been generated by use of the Service or Software by the Client or User. Vartion will only process the Personal Data to the extent, and in such a manner, as is necessary for the Agreement in accordance with the instructions of the Client. |

*Purpose(s) of the data transfer and further processing*

| | |
|---|---|
| Purpose | SECTION B: SERVICE<br><br>The purpose of processing Personal Data is to execute the relevant<br><br>Agreement and the Services, which can also relate to assisting the Client with complying with its legal obligations with regard to Client Due Diligence.<br><br>SECTION C: SAAS-SERVICE<br>The purpose of processing Personal Data is to provide the Client certain service such as the filling in of the KYC-checklist with Pascal onboarding or give the Client the possibility to screen possible costumers itself for KYC purposes through and in connection with a tool designed and developed for the compliance with legal obligations such as to (1) support risk and compliance professionals during a Client due diligence (CDD), and if applicable (2) constantly monitor the Database – or any other database on which is de Software is applied by the Client – for Client related events (direct and indirect) and Client transactions, thereby boosting efficiency and providing insight into data, made available by Vartion to the Client via the internet or another network. |

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

| | |
|---|---|
| Retention period | SECTION B: SERVICE<br><br>Personal Data shall be detained as long as necessary for the execution of the Agreement. If the Agreement is terminated all Personal Data shall be destroyed except for the Personal Data which has to be retained under Applicable Law.<br><br>SECTION C: SAAS-SERVICE<br><br>Personal Data shall be detained as long as necessary for the execution of the Agreement. If the Agreement is terminated all Personal Data shall be destroyed except for the Personal Data which has to be retained under Applicable Law or in case it has been reused to improve the Software. |

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

| | |
|---|---|
| List of sub-processors | Asana, Inc. processes feedback provided by our users. By using Pascal, you acknowledge and agree that your information is subject to Asana. Their privacy statement can be found at the following location: https://asana.com/terms/privacy-statement Processes user feedback, including user email addresses, usernames, organisation names, browser information, and written messages.<br><br>Cloudflare, Inc. provides a proxy services for Pascal. By using Pascal, you acknowledge and agree that your information is subject to Cloudflare. Their privacy statement can be found at the following location: https://www.cloudflare.com/privacypolicy/ Handles all encrypted internet traffic between clients and Pascal.<br><br>DigitalOcean, LLC provides data storage of Pascal. By using Pascal, you acknowledge and agree that your information is subject to DigitalOcean. Their privacy statement can be found at the following location: https://www.digitalocean.com/legal/privacy-policy Stores all Pascal data, including PDF reports and backups of the application's databases.<br><br>Microsoft B.V. provides hosting for our services and processes all our data. By using Pascal, you acknowledge and agree that your information is subject to Microsoft. Their privacy statement can be found at the following location: https://privacy.microsoft.com/en-gb/privacystatement Hosts and processes all Pascal data.<br><br>Mollie B.V. provides payment services and processes payments made in Pascal. By using Pascal, you acknowledge and agree that your information is subject to Mollie. Their privacy statement can be found at the following location: |

https://www.mollie.com/privacyProcesses payment details, payment method information, and consumer names for payments made through Pascal.

Twilio Ireland Ltd. provides email services and processes emails send from Pascal. By using Pascal, you acknowledge and agree that your information is subject to Twilio. Their privacy statement can be found at the following location: https://www.twilio.com/en-us/legal/privacy Processes email services, including user email addresses and usernames.

Functional Software, Inc. provides error monitoring for Pascal. By using Pascal, you acknowledge and agree that your information is subject to Functional Software, Inc. Their privacy statement can be found at the following location: https://sentry.io/privacy/ Provides error monitoring, which may include usernames, activity logs, and error-related data from Pascal.

TransIP Group B.V. provides hosting for Pascal and acts as the register for vartion.com. TransIP's privacy policy can be found at the following location: https://www.transip.nl/legal-and-security/privacy-policy/ Provides hosting services and acts as the domain registrar for vartion.com.

Userpilot, Inc. provides onboarding and adoption services for Pascal. By using Pascal, you acknowledge and agree that your information is subject to Userpilot. Their privacy statement can be found at the following location: https://userpilot.com/privacy-policy/ Manages onboarding and adoption services, processing user email addresses, usernames, organisation names, browser information, and account activity logs.

HubSpot, Inc. provides customer services for Pascal. By using Pascal, you acknowledge and agree that your information is subject to HubSpot. Their privacy statement can be found at the following location: https://legal.hubspot.com/privacy-policy Supports customer service operations by processing user email addresses, usernames, organisation names, and account activity data.

Eurofiber Cloud Infra B.V. provides hosting for our services and processes all our data. By using Pascal, you acknowledge and agree that your information is subject to Eurofiber Cloud Infra B.V.. Their privacy statement can be found at the following location: https://www.eurofibercloudinfra.com/en/privacy-policy.

Google, LLC provides advertisements and analytics services. Their privacy statement can be found at the following location: https://policies.google.com/privacy Provides advertising services through Google Ads, processing data such as user interactions with advertisements, campaign performance metrics, and device/browser information.

OVH Groupe SAS provides hosting services. Their privacy statement can be found at the following location: https://www.ovhcloud.com/en/terms-and conditions/privacy-policy/ Provides hosting services used to collect and store analytics data, including aggregated usage statistics

| | |
|---|---|
| Changes of sub-processors | Processor shall notify Controller of any intended changes concerning the engagement or replacement of a sub-Processor. The Controller shall be given thirty (30) days to object, duly motivated and in writing. Consent shall not unreasonably be withheld. |

## B. COMPETENT SUPERVISORY AUTHORITY

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

| | |
|---|---|
| Competent Supervisory Authority | The competent supervisory Autority is the Autoriteit Persoonsgegevens (AP) located in the Netherlands. |

*ANNEX II*

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

2 MODULE ONE: Transfer controller to controller

3 MODULE TWO: Transfer controller to processor

4 MODULE THREE: Transfer processor to processor

| | |
|---|---|
| Security of Transmission | - Use of data segregation; and<br>- Use of anonymization of data. |
| Security of Storage | - the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and<br>- Data backups (daily). |
| Security of Processing | - a process for regularly testing, assessing and evaluating the effectiveness of the security measures;<br>- Physical access controls.<br>- System access controls. |
| Organisational security measures | - Only the authorized employees of the Parties can access the data. Parties only work with systems that: (i) only allow authorized individuals to access the Personal Data to which they have been granted access; and (ii) ensure that the Personal Data cannot be read, copied, modified or deleted without authorization during processing.<br>- All employees of the Parties are instructed to conduct themselves in a manner consistent with the Party's guidelines regarding confidentiality, Personal Data protection, business ethics, appropriate use and professional standards; and<br>- Parties make use of password protection and use of passwords and two factor authentications. |
| Technical security minimum requirements | - Encryption of Personal Data;<br>- Use of antivirus;<br>- Use of Anti-Malware Software |

| | |
|---|---|
| Updates to the Security Requirements | - The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to. |

*ANNEX III*

LIST OF SUB-PROCESSORS

5 MODULE TWO: Transfer controller to processor

6 MODULE THREE: Transfer processor to processor

| | |
|---|---|
| List of sub-processors | SECTION B: SERVICE<br><br>SECTION C: SAAS-SERVICE<br><br>Asana, Inc. processes feedback provided by our users. By using Pascal, you acknowledge and agree that your information is subject to Asana. Their privacy statement can be found at the following location: https://asana.com/terms/privacy-statement Processes user feedback, including user email addresses, usernames, organisation names, browser information, and written messages.<br><br>Cloudflare, Inc. provides a proxy services for Pascal. By using Pascal, you acknowledge and agree that your information is subject to Cloudflare. Their privacy statement can be found at the following location: https://www.cloudflare.com/privacypolicy/ Handles all encrypted internet traffic between clients and Pascal.<br><br>DigitalOcean, LLC provides data storage of Pascal. By using Pascal, you acknowledge and agree that your information is subject to DigitalOcean. Their privacy statement can be found at the following location: https://www.digitalocean.com/legal/privacy-policy Stores all Pascal data, including PDF reports and backups of the application's databases.<br><br>Microsoft B.V. provides hosting for our services and processes all our data. By using Pascal, you acknowledge and agree that your information is subject to Microsoft. Their privacy statement can be |

found at the following location: https://privacy.microsoft.com/en-gb/privacystatement Hosts and processes all Pascal data.

Mollie B.V. provides payment services and processes payments made in Pascal. By using Pascal, you acknowledge and agree that your information is subject to Mollie. Their privacy statement can be found at the following location: https://www.mollie.com/privacyProcesses payment details, payment method information, and consumer names for payments made through Pascal.

Twilio Ireland Ltd. provides email services and processes emails send from Pascal. By using Pascal, you acknowledge and agree that your information is subject to Twilio. Their privacy statement can be found at the following location: https://www.twilio.com/en-us/legal/privacy Processes email services, including user email addresses and usernames.

Functional Software, Inc. provides error monitoring for Pascal. By using Pascal, you acknowledge and agree that your information is subject to Functional Software, Inc. Their privacy statement can be found at the following location: https://sentry.io/privacy/ Provides error monitoring, which may include usernames, activity logs, and error-related data from Pascal.

TransIP Group B.V. provides hosting for Pascal and acts as the register for vartion.com. TransIP's privacy policy can be found at the following location: https://www.transip.nl/legal-and-security/privacy-policy/ Provides hosting services and acts as the domain registrar for vartion.com.

Userpilot, Inc. provides onboarding and adoption services for Pascal. By using Pascal, you acknowledge and agree that your information is subject to Userpilot. Their privacy statement can be found at the following location: https://userpilot.com/privacy-policy/ Manages onboarding and adoption services, processing user email addresses, usernames, organisation names, browser information, and account activity logs.

HubSpot, Inc. provides customer services for Pascal. By using Pascal, you acknowledge and agree that your information is subject to

| | |
|---|---|
| | HubSpot. Their privacy statement can be found at the following location: https://legal.hubspot.com/privacy-policy Supports customer service operations by processing user email addresses, usernames, organisation names, and account activity data.<br><br>Eurofiber Cloud Infra B.V. provides hosting for our services and processes all our data. By using Pascal, you acknowledge and agree that your information is subject to Eurofiber Cloud Infra B.V.. Their privacy statement can be found at the following location: https://www.eurofibercloudinfra.com/en/privacy-policy<br><br>Google, LLC provides advertisements and analytics services. Their privacy statement can be found at the following location: https://policies.google.com/privacy Provides advertising services through Google Ads, processing data such as user interactions with advertisements, campaign performance metrics, and device/browser information.<br><br>OVH Groupe SAS provides hosting services. Their privacy statement can be found at the following location: https://www.ovhcloud.com/en/terms-and-conditions/privacy-policy/ Provides hosting services used to collect and store analytics data, including aggregated usage statistics |
| Changes of sub-processors | Processor shall notify Controller of any intended changes concerning the engagement or replacement of a sub-Processor. The Controller shall be given thirty (30) days to object, duly motivated and in writing. Consent shall not unreasonably be withheld. |