Data Processing Agreement

This Data Processing Agreement ("**Agreement**") forms part of the Terms of Use ("**Principal Agreement**") between: (i) Overloop SRL ("**Vendor**" or **"Overloop"**) acting on its own behalf and as agent for each Vendor Affiliate; and (ii) _____("**Company**") acting on its own behalf and as agent for each Company Affiliate.

The terms used in this Agreement shall have the meanings set forth in this Agreement. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as set out below, the terms of the Principal Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Agreement to the Principal Agreement. Except where the context requires otherwise, references in this Agreement to the Principal Agreement are to the Principal Agreement as amended by, and including, this Agreement.

1. Definitions

1.1. In this Agreement, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1. "**Applicable Laws**" means any type of legislation to the extent it applies to each party, including the Data Protection Laws;

1.1.2. "**Company Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Company, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.3. "**Company Group Member**" means Company or any Company Affiliate;

1.1.4. "**Company Personal Data**" means any Personal Data Processed by Vendor on behalf of a Company Group Member pursuant to or in connection with the Principal Agreement;

1.1.6. "**Data Protection Laws**" means any privacy and data protection law and regulation to the extent they apply to each party and to the Processing of

Personal Data under the Principal Agreement, including the General Data Protection Regulation (EU) 2016/679 ("**GDPR**");

1.1.7. "**EEA**" means the European Economic Area;

1.1.8. "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Vendor for Company Group Members pursuant to the Principal Agreement; and

1.1.9. "**Vendor Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Vendor, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.2. The terms, "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", "**Sub-Processor**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

1.3. The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Authority

Vendor warrants and represents that, before any Vendor Affiliate Processes any Company Personal Data, Vendor's entry into this Agreement as agent for and on behalf of that Vendor Affiliate will have been duly and effectively authorised (or subsequently ratified) by that Vendor Affiliate.

3. Processing of Company Personal Data

3.1. Vendor and each Vendor Affiliate shall:

3.1.1. comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

3.1.2. not Process Company Personal Data other than on the relevant Company Group Member's documented instructions unless Processing is required by Applicable Laws to which the Vendor or the relevant Vendor Affiliate is subject, in which case Vendor or the relevant Vendor Affiliate

shall to the extent permitted by Applicable Laws inform the relevant Company Group Member of that legal requirement before the relevant Processing of that Company Personal Data.

3.2. Each Company Group Member:

3.2.1. instructs Vendor and each Vendor Affiliate (and authorises Vendor and each Vendor Affiliate to instruct each Sub-Processor) to:

3.2.1.1. Process Company Personal Data as determined in this Agreement; and

3.2.1.2. transfer Company Personal Data to any country or territory, as reasonably necessary for the provision of the Services, consistent with the Principal Agreement and in accordance with Data Protection Laws; and

3.2.2. warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 3.2.1 on behalf of each relevant Company Affiliate.

3.3. Annex 1 to this Agreement sets out certain information regarding the Vendor Processing the Company Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). Company may make reasonable amendments to Annex 1 by written notice to Vendor from time to time as Company reasonably considers necessary.

4. Vendor and Vendor Affiliate Personnel

Vendor and each Vendor Affiliate shall take reasonable steps to ensure the reliability of any of their employees, agents or contractors who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as necessary for the purposes of the Principal Agreement, and to ensure that all such individuals are subject to confidentiality obligations.

5. Security

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Vendor and each Vendor Affiliate shall in relation to the

Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk (see Annex 2).

6. Sub-processing

6.1. Each Company Group Member authorises Vendor and each Vendor Affiliate to appoint (and permit each Sub-Processor appointed in accordance with this section 6 to appoint) Sub-Processors in accordance with this section 6.

6.2. Vendor and each Vendor Affiliate may continue to use those Sub-Processors already engaged by Vendor or any Vendor Affiliate as at the date of this Agreement. The list of current Sub-Processors can be found in Annex 3.

6.3. Vendor shall give Company prior written notice of the appointment of any new Sub-Processor, including full details of the Processing to be undertaken by the Sub-Processor. If, within thirty (30) calendar days of receipt of that notice, Company notifies Vendor in writing of any objections (on reasonable grounds) to the proposed appointment, neither Vendor nor any Vendor Affiliate shall appoint (or disclose any Company Personal Data to) that proposed Sub-Processor until reasonable steps have been taken to address the objections raised by Company and Company has been provided with a reasonable written explanation of the steps taken.

6.4. With respect to each Sub-Processor, Vendor or the relevant Vendor Affiliate shall:

6.4.1. prior to the Sub-Processor Processing Company Personal Data, carry out adequate due diligence to ensure that the Sub-Processor is capable of providing the level of protection for Company Personal Data required by the Principal Agreement;

6.4.2. ensure that the arrangement between the Vendor or the Vendor Affiliate and the Sub-Processor, is governed by a written contract including terms which offer at least the same level of protection for Company Personal Data as those set out in this Agreement;

6.5. Where the Sub-Processor fails to fulfil its data protection obligations, Vendor shall remain liable for the acts and omissions of its Sub-Processor.

7. Data Subject Rights

7.1. Taking into account the nature of the Processing, Vendor and each Vendor Affiliate shall assist each Company Group Member by implementing appropriate

technical and organisational measures, insofar as this is possible, for the fulfilment of the Company Group Members' obligations to respond to requests to exercise Data Subject rights under the Data Protection Laws.

7.2. Vendor shall:

7.2.1. promptly notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

7.2.2. not respond to that request except on the documented instructions of Company or the relevant Company Affiliate.

8. Personal Data Breach

Vendor will notify Company without undue delay upon becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow each Company Group Member to meet any obligations to report or inform Data Subjects or any Supervisory Authority of the Personal Data Breach under the Data Protection Laws.

9. Data Protection Impact Assessment and Prior Consultation

Vendor will reasonably assist Company, upon Company's request, in ensuring compliance with Company's obligations pursuant to Data Protection Laws (in particular articles 32 to 36 of the GDPR, where applicable) taking into account the nature of Processing and the information available to Vendor.

10. Deletion or return of Company Personal Data

10.1. Vendor shall, at the choice of Company, return or delete all (copies of) the Company Personal Data, unless legislation imposed upon Vendor prevents it from returning or destroying all or part of the Company Personal Data.

10.2. Upon request by Company, Vendor shall provide written certification to Company that it has complied with section 10.1.

11. Audit rights

Vendor shall permit Company (or its appointed third-party auditors) to audit Vendor's compliance with this Agreement, and shall make available to Company all information, systems and staff necessary for Company (or its third-party auditors) to conduct such audit. Vendor acknowledges that Company (or its third-party auditors) may enter its premises for the purposes of conducting this audit, provided that Company gives it reasonable prior notice of its intention

to audit, conducts its audit during normal business hours, and takes all reasonable measures to prevent unnecessary disruption to Vendor's operations. Such audit will be subject to any confidentiality terms agreed between the parties.

12. International Transfers

12.1. To the extent Company is located outside the EEA in a country which is not subject to an adequacy decision under the GDPR, the EU Processor-to-Controller Standard Contractual Clauses ("**SCCs**"), set out in Annex 4, shall apply. Annex 1 to the SCCs is deemed to be prepopulated with the names of Company, as data importer, and Vendor, as data exporter, and the Processing operations are deemed to be those described in Annex 1 of this Agreement.

12.2. To the extent Vendor uses Sub-Processors located outside the EEA, in a country which is not subject to an adequacy decision under the GDPR, Vendor shall ensure that such data transfer is subject to the EU Standard Contractual Clauses, the certification under the EU-US Data Privacy Framework, or one of the other transfer mechanisms allowed under Chapter V of the GDPR.

13. General Terms

Governing law and jurisdiction

13.1 The parties to this Agreement hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this Agreement; and

13.2 This Agreement and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

Order of precedence

13.3. Nothing in this Agreement reduces Vendor's or any Vendor Affiliate's obligations under the Principal Agreement in relation to the protection of Company Personal Data or permits Vendor or any Vendor Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement. In the event of any conflict or inconsistency between this Agreement and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

13.4. Subject to section 13.3, with regard to the subject matter of this Agreement, in the event of inconsistencies between the provisions of this Agreement and any other agreements between the parties, including the Principal Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Agreement, the provisions of this Agreement shall prevail.

Severance

13.5. Should any provision of this Agreement be invalid or unenforceable, then the remainder of this Agreement shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this Agreement is entered into and becomes a binding part of the Principal Agreement with effect from the date set out below.

	For Overloop SRL	For Company
Represented by	Vincenzo Ruggiero	_____
Title	CEO	_____
Date of Signature	_____	_____
Signature	_____	_____

ANNEX 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

This Annex 1 includes certain details of the Processing of Company Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Company Personal Data

The subject matter of the Processing of the Company Personal Data is set out in the Principal Agreement and this Agreement. The Processing shall begin upon the commencement of the Principal Agreement and shall continue until the Principal Agreement has been terminated or expires.

The nature and purpose of the Processing of Company Personal Data

The Processing of Company Personal Data is limited to allowing Company to perform lead generation and direct marketing as well as other marketing and sales activities. The Processing of Company Personal Data terminates when Company deletes its account.

Company Personal Data can also be Processed to improve the application, prevent fraud, help with debugging and ease support operations.

The types of Company Personal Data to be Processed

Vendor Processes Company Personal Data supplied when using the service such as: admin contact information, users details, users email template, users emailaddresses, user IP addresses, support ticket data, pre and post sales emails.

The categories of Data Subject to whom the Company Personal Data relates

The categories of Personal Data processed by Vendor may include, without limitation:

- Company employees, contractors or any other person added to the team of the Company.

- Company contacts or leads submitted to Vendor.

- Potential business leads found publicly online that could be used by Company for sales and marketing purposes.

The obligations and rights of Company and Company Affiliates

The obligations and rights of Company and Company Affiliates are set out in the Principal Agreement and this Agreement.

ANNEX 2: SECURITY MEASURES

Overloop is ensuring the state of its security responds to existing and upcoming threats in accordance with industry standards. Those security measures include:

Infrastructure

All of our services run in the cloud. We don't host or run our own routers, load balancers, DNS servers, or physical servers. Our service is built on Heroku (Salesforce, Inc.) which itself is hosted on Amazon Web Services (AWS). They provide strong security measures to protect our infrastructure and are compliant with most certifications. You can read more about their practices here:

- Heroku Security (https://www.heroku.com/policy/security)
- AWS Security (https://aws.amazon.com/security/)

DDoS protection

We use Distributed Denial of Service (DDoS) mitigation services powered by Cloudflare, Inc.

Data encryption

Encryption in transit

All data sent to or from our infrastructure is encrypted in transit via industry best-practices using Transport Layer Security (TLS). You can see our SSLLabs (https://www.ssllabs.com/ssltest/analyze.html?d=Overloop) report here.

Encryption at rest

All our user data (including passwords) is encrypted using battled-proofed encryption algorithms in the database by our database providers Heroku (Salesforce, Inc.) and Redis Labs, Inc.

Data retention and removal

We retain our users data for a period of 60 days after your subscription ends. All data is then completely removed from our servers with the exception of payment and invoices data. Every user can request the removal of usage data by contacting support. Read more about our privacy settings at https://www.overloop.com/privacy.

Business continuity and disaster recovery

We back up all our critical assets and regularly attempt to restore the backup to guarantee a fast recovery in case of disaster. All our backups are encrypted.

Application security monitoring

We use Bugsnag to monitor exceptions, logs and detect anomalies in our applications. We collect and store logs to provide an audit trail of our applications activity.

Application security protection

A Web Application Firewall is set up to filter incoming requests trying to compromise the service. A firewall is systematically used on Overloop's servers to prevent access from non-approved IP addresses. Critical admin interfaces are protected using at least double-authentication. Our software infrastructure is regularly update using automatic update mechanisms when possible. End-to-end encrypted messaging systems are available to Overloop's employees and contractors, and used for most communications.

Secure development

We apply development best practices for your chosen development language and framework to mitigate known vulnerability types such as those on the OWASP Top 10 Web Application Security Risks.

Payment information

All payment instrument processing is safely outsourced to Stripe which is certified as a PCI Level 1 Service Provider. We don't collect any payment information and are therefore not subject to PCI obligations.

Employee access

Our strict internal procedure prevents any employee or administrator from gaining access to user data. Limited exceptions can be made for customer support. All devices (in particular laptops and computers) used by employees and contractors of Overloop are encrypted.

ANNEX 3: LIST OF CURRENT SUB-PROCESSORS

The current list of Sub-Processors can be found in our Privacy Policy by visiting https://www.overloop.com/privacy/.

ANNEX 4: PROCESSOR-TO-CONTROLLER STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1: Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (1) 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 8.1 (b) and Clause 8.3(b);

(iii) Clause 13;

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

(v) Clause 16(e);

(vi) Clause 18.

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

Clause 4: Interpretation

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

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

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

Clause 5: Hierarchy

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

Clause 6: Description of the transfer(s)

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

Clause 7: Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8: Data protection safeguards

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

8.1 Instructions

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

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

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

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

2. Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

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

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

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

Clause 9: Use of sub-processors (N/A)

Clause 10: Data subject rights

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

Clause 11: Redress

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

Clause 12: Liability

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

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

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

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

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

Clause 13: Supervision

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

Clause 14: Local laws and practices affecting compliance with the Clauses

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

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

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[1];

(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).

---

[1] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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

Clause 15: Obligations of the data importer in case of access by public authorities

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

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16: Non-compliance with the Clauses and termination

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

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

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

Clause 17: Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of as set out in the Principal Agreement.

Clause 18: Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of the country as set out in the Principal Agreement.

ANNEX I

A. LIST OF PARTIES

Data exporter: [*Identity and contact details of the data exporter(s) and, where applicable, of its/ their data protection officer and/or representative in the European Union*]

Name: Overloop SRL

Address: Rue des Pères blancs 4, 1040 Etterbeek (Belgium)

Contact person's name, position and contact details: Vincenzo Ruggiero, CEO

Activities relevant to the data transferred under these Clauses: As set out in the Principal Agreement

Signature and date: …

Role (controller/processor): Processor

Data importer: *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*]

Name: Company, as defined in the Principal Agreement

Address: As set out in the Principal Agreement

Contact person's name, position and contact details: As set out in the Principal Agreement

Activities relevant to the data transferred under these Clauses: As set out in the Principal Agreement

Signature and date: …

Role (controller/processor): Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred: As set out in Annex 1 to the Agreement.

Categories of personal data transferred: As set out in Annex 1 to the Agreement.

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: As set out in Annex 1 to the Agreement.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): As set out in Annex 1 to the Agreement.

Nature of the processing: As set out in Annex 1 to the Agreement.

Purpose(s) of the data transfer and further processing: As set out in Annex 1 to the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: As set out in Annex 1 to the Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: As set out in Annex 3 to the Agreement.