DATA PROCESSING ADDENDUM (GDPR)

This Data Processing Addendum ("**DPA**") forms part of the Services Agreement or other written or electronic agreement between CelerisPay B.V. (CP) and Client for the purchase of online services from CP (identified either as "Services" or otherwise in the applicable agreement, and hereinafter defined as "Services") (the "Agreement") to reflect the parties' agreement with regard to the Processing of Personal Data.

In the course of providing the Services to Client pursuant to the Agreement, CP may Process Personal Data on behalf of Client and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

DATA PROCESSING TERMS

DEFINITIONS

"**Adequate Country**" means a country or territory that is recognized under EU Data Protection Laws as providing adequate protection for Personal Data.

"Client" means the entity which signed the CP's Merchant Service Agreement.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Customer Data" means what is defined in the Agreement as "Customer Data" or "Your Data."

"Data Protection Laws and Regulations" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

"Connfido Group" means (i) any direct or indirect holding company of CP and/or (ii) any direct or indirect subsidiary of Connfido B.V. or of any relevant holding company, including, Newgen Payment Gateway Private Limited and/or (iii) any associated company with similar shareholders.

"Data Subject" means the identified or identifiable person to whom Personal Data relates.

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

"Personal Data" means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data.

"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor" means the entity which Processes Personal Data on behalf of the Controller.

"CP" means CelerisPay B.V., a company incorporated in the Netherlands, Chamber of Commerce registration number 75952882.

"Sub-processor" means any Processor engaged by CP or a member of the Connfido Group.

"**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to the GDPR.

2. PROCESSING OF PERSONAL DATA

2.1 Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, Client is the Controller, CP is the Processor and that CP will engage Sub-processors pursuant to the requirements set forth in Section 5 “Sub-processors” below.

2.2 Client’s Processing of Personal Data. Client shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Client’s instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Client shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Client acquired Personal Data.

2.3 CP’s Processing of Personal Data. CP shall treat Personal Data as Confidential Information and shall only Process Personal Data on behalf of and in accordance with Client’s documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Client (e.g., via email) where such instructions are consistent with the terms of the Agreement.

2.4 Details of the Processing. The subject-matter of Processing of Personal Data by CP is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Annex 1 (Details of the Processing) to this DPA.

3. RIGHTS OF DATA SUBJECTS

Data Subject Request. CP shall, to the extent legally permitted, promptly notify Client if CP receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure (“right to be forgotten”), data portability, object to the Processing, or its right not to be subject to an automated individual decision making (“Data Subject Request”). Taking into account the nature of the Processing, CP shall assist Client by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Client’s obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Client, in its use of the Services, does not have the ability to address a Data Subject Request, CP shall upon Client’s request provide commercially reasonable efforts to assist Client in responding to such Data Subject Request, to the extent CP is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Client shall be responsible for any costs arising from CP’s provision of such assistance.

4. CP PERSONNEL

4.1 Confidentiality. CP shall ensure that its (or Connfido Group’s) personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. CP shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2 Reliability. CP shall take commercially reasonable steps to ensure the reliability of any CP

(or Connfido Group's) personnel engaged in the Processing of Personal Data.
4.3 Limitation of Access. CP shall ensure that CP's access to Personal Data is limited to those personnel of CP or Connfido Group performing Services in accordance with the Agreement.
4.4 Data Protection Officer. Members of the Connfido Group have appointed a data protection officer. The appointed person may be reached at support@celerispay.com.

5. SUB-PROCESSORS
5.1 Appointment of Sub-processors. Client acknowledges and agrees that (a) entities within the Connfido Group may be retained as Sub-processors pursuant their involved in the delivery of the Services under the Agreement; and (b) CP and the Connfido Group respectively may engage third-party Sub-processors in connection with the provision of the Services. CP or a Connfido Group member has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this Agreement with respect to the protection of Customer Data to the extent applicable to the nature of the Services provided by such Sub-processor.
5.2 Objection Right for New Sub-processors. Client may object to CP's use of a new Sub-processor by notifying CP promptly in writing within ten (10) business days after receipt of CP's notice in accordance with the mechanism set out in Section 5.2. In the event Client objects to a new Sub-processor, as permitted in the preceding sentence, CP will use reasonable efforts to make available to Client a change in the Services or
recommend a commercially reasonable change to Client's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Client. If CP is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Client may terminate the applicable Order Form(s) with respect only to those Services, which cannot be provided by CP without the use of the objected-to new Sub-processor by providing written notice to CP.
5.3 Liability. CP shall be liable for the acts and omissions of its Sub-processors to the same extent CP would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the CP's Merchant Service Agreement.

6. SECURITY
6.1 Controls for the Protection of Customer Data. CP shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data, as set forth in the Security, Privacy and Architecture Documentation. CP regularly monitors compliance with these measures. CP will not materially decrease the overall security of the Services during a subscription term.
6.2 Third-Party Certifications and Audits. Connfido Group has obtained the third-party certifications and audits set forth in the Security, Privacy and Architecture Documentation. Upon Client's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Connfido Group shall make available to Client that is not a competitor of Connfido Group (or Client's independent, third-party auditor that is not a competitor of Connfido Group) a copy of Connfido's Group then most recent third-party audits or certifications, as applicable.

7. CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION

CP maintains security incident management policies and procedures and shall, notify Client without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by CP or its Sub-processors of which CP becomes aware (a "**Customer Data Incident**"). CP shall make reasonable efforts to identify the cause of such Customer Data Incident and take those steps as CP deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident to the extent the remediation is within CP's reasonable control. The obligations herein shall not apply to incidents that are caused by Client or Client's Users.

8. RETURN AND DELETION OF CUSTOMER DATA

CP shall return Customer Data to Client and, to the extent allowed by applicable law, delete Customer Data and require the Connfido Group to delete, in accordance with the procedures and timeframes specified in the Security, Privacy and Architecture Documentation.

9. LIMITATION OF LIABILITY

Each party's and all of its affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its affiliates (including for CP the Connfido Group) under the Agreement and this DPA. For the avoidance of doubt, CP's and Connfido Group's total liability for all claims from the Client and all of its affiliates arising out of or related to the CP's Merchant Service Agreement and this DPA shall apply in the aggregate for all claims under both the CP's Merchant Service Agreement and this DPA established under the Agreement. The maximum liability of CP under this Agreement shall not exceed in the aggregate an amount equal to the Fees paid by or on behalf of Client to CP for providing Services during the last two (2) months prior to the claim arising. Also, for the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Annexes and Appendices.

10. LEGAL

This Agreement shall be governed by and construed in accordance with the laws of The Netherlands. The Parties agree that the courts of Amsterdam have jurisdiction to settle any disputes in connection herewith and accordingly submit to the jurisdiction of such courts.

11. EUROPEAN SPECIFIC PROVISIONS

11.1 GDPR. CP will Process Personal Data in accordance with the GDPR requirements directly applicable to CP's provision of its Services.

11.2 Data Protection Impact Assessment. Upon Client's request, CP shall provide Client with reasonable cooperation and assistance needed to fulfil Client's obligation under the GDPR to carry out a data protection impact assessment related to Client's use of the Services, to the extent Client does not otherwise have access to the relevant information, and to the extent such information is available to CP. CP shall provide reasonable assistance to Client in the

cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 11.2 of this DPA, to the extent required under the GDPR.

12. COMPLIANCE WITH LAWS AND AUDIT RIGHT

12.1 Each party will comply with all applicable laws and regulations, in the provision of their respective obligations and activities hereunder

12.2 Once every 12 months during the Term of this Agreement, the Client shall have the right, at its own cost and expense, to perform a reasonable audit of CP's performance under and in compliance with the terms of this Agreement (although such audits may be conducted more frequently if required by applicable law, a court order, a regulatory authority with jurisdiction or if a breach is suspected). CP will (a) make (CP or Connfido Group) personnel with knowledge of this Agreement available to the Client; and (b) provide Client with copies of applicable records and other documentation reasonably requested; all as reasonably necessary to carry out such audit. The CP's expenses related to this audit shall be borne by the Client.

13. DATA TRANSFERS

13.1 The Client acknowledges and agrees that CP shall transfer Personal Data outside the EEA, more specifically to a Connfido Group member based in India as required pursuant clause 13.2. The parties agree that the standard contractual clauses approved by the EU authorities under EU Data Protection Laws and set out in Annex 2 will apply in respect of that processing, and CP will comply with the obligations of the 'data importer' in the standard contractual clauses and the Client will comply with the obligations of the 'data exporter'.

13.2 The Client acknowledges and accepts that the provision of the Service under the CP's Merchant Service Agreement may require the processing of Personal Data by sub-processors in countries outside the EEA.

13.3 When CP transfers any Personal Data to a sub-processor located outside of the EEA (without prejudice to clause 4), CP shall in advance of any such transfer ensure that a legal mechanism to achieve adequacy in respect of that processing is in place, such as:

(a) The requirement for CP to execute or procure that the sub-processor execute to the benefit of the Client standard contractual clauses approved by the EU authorities under EU Data Protection Laws and set out in Annex 2;

(b) The requirement for the sub-processor to be certified under the EU-U.S. Privacy Shield Framework; or

(c) The existence of any other specifically approved safeguard for data transfers (as recognised under EU Data Protection Laws) and/or a European Commission finding of adequacy.

13.4 The following terms shall apply to the standard contractual clauses set out in Annex 2:

(a) The Client may exercise its right of audit under clause 12.2 of the standard contractual clauses as set out in; and

(b) CP may appoint sub-processors as set out, and subject to the requirements of, clauses 5 and 13.3 of this DPA.

List of Annexes & Appendix

Annex 1: Details of the Processing

Annex 2: Standard Contractual Clauses

ANNEX 1
DETAILS OF THE PROCESSING
Nature and Purpose of Processing
CP will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Client in its use of the Services.
Duration of Processing
Subject to Section 8 of the DPA, CP will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.
Categories of Data Subjects
Client may submit Personal Data to the Services, the extent of which is determined and controlled by Client in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:
● Prospects, customers, business partners and vendors of Client (who are natural persons)
● Employees or contact persons of Client's prospects, customers, business partners and vendors
● Employees, agents, advisors, freelancers of Client (who are natural persons)
● Client's Users authorized by Client to use the Services
Type of Personal Data
Client may submit Personal Data to the Services, the extent of which is determined and controlled by Client in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:
- First and last name
- Title
- Position
- Employer
- Date of birth
- Address
- Contact information (company, email, phone, physical business address)
- KYC related information (ID data and/or photograph, Company Structure, Board Members, etc.)
- Nationality
- Country of residence
- Bank and/or issuer details

ANNEX 2
STANDARD CONTRACTUAL CLAUSES
2010 EU Model clauses extracted from 2010/87/EU Annex EU Standard Contractual Clauses for the transfer of personal data to data processors established in third countries which do not ensure an adequate level of data protection

INTRODUCTION
Both parties have agreed on the following Contractual Clauses (the "**Clauses**") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

AGREED TERMS

1. Definitions

For the purposes of the Clauses:

a) "**personal data**", "**special categories of data**", "**process/processing**", "**controller**", "**processor**", "**data subject**" and "**supervisory authority**" shall have the same meaning as in EU Data Protection Laws 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

b) the "**data exporter**" means the entity who transfers the personal data;

c) the "**data importer**" means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of EU Data Protection Laws 95/46/EC;

d) the "**sub-processor**" means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

e) the "**applicable data protection law**" means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established; and

f) "**technical and organisational security measures**" means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

3. Third-party beneficiary clause

3.1 The data subject can enforce against the data exporter this Clause, Clause 4.1(b) to (i), Clause 5(a) to (e), and (g) to (i), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

3.2 The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.3 The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub- processor shall be limited to its own processing

operations under the Clauses.
3.4 The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4. Obligations of the data exporter
4.1 The data exporter agrees and warrants:
a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law;
b) that it has instructed and throughout the duration of the personal data-processing services will
instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security;
d) that the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
e) that it will ensure compliance with the security measures;
f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of EU Data Protection Laws
95/46/EC;
g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
h) to make available to the data subjects upon request a copy of the Clauses, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub- processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
j) that it will ensure compliance with Clause 4(a) to (i).

5. Obligations of the data importer
5.1 The data importer agrees and warrants:
a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is
entitled to suspend the transfer of data and/or terminate the contract;

b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of
data and/or terminate the contract;
c) that it has implemented the technical and organisational security measures before processing the personal data transferred;
d) that it will promptly notify the data exporter about:
(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
(ii) any accidental or unauthorised access; and
(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of
the personal data subject to the transfer and to abide by the advice of the supervisory authority with
regard to the processing of the data transferred;
f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
g) that, in the event of sub-processing, it has previously informed the data exporter and obtained its
prior written consent;
h) that the processing services by the sub-processor will be carried out in accordance with Clause 11;
i) to send when requested a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

6. Liability

a) Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to the clauses mentioned in this agreement, and all DPAs between Authorized Affiliates and CP, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Clauses and all DPAs together.
b) The maximum liability of CP under the clauses mentioned in this Agreement shall not exceed in the aggregate an amount equal to the Fees paid by or on behalf of Client to CP for providing Services during the last two (2) months prior to the claim arising.

7. Mediation and jurisdiction

The Clauses shall be governed by and construed in accordance with the laws of The

Netherlands. The Parties agree that the courts of Amsterdam have jurisdiction to settle any disputes in connection herewith and accordingly submit to the jurisdiction of such courts.

8. Compliance with laws and audit right

a) Each party will comply with all applicable laws and regulations, in the provision of their respective obligations and activities hereunder.

b) Once every 12 months during the Term of the Clauses, each party shall have the right, at its own cost and expense, to perform a reasonable audit of performance under and in compliance with the Clauses of this Agreement (although such audits may be conducted more frequently if required by applicable law, a court order, a regulatory authority with jurisdiction or if a breach is suspected).

9. Governing law

The Clauses shall be governed by and construed in accordance with the laws of the Netherlands.

10. Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

11. Sub-processing

11.1 The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5.1(i), which shall be updated at least once a year.

12. Obligation after the termination of personal data-processing services

12.1 The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12.2 The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 2 of Clause 8.

Appendix 1

This Appendix forms part of the Clauses.

Data exporter

The data exporter is: The counterparty agreeing to these terms and all affiliates of such entity established within the EEA, which have purchased services from CP or its Affiliates.

Data importer

The data importer is: CP, which processes Personal Data upon the instruction of the data exporter in accordance with the terms of the agreement between the data exporter and CP.

Data subjects

The personal data transferred concern the following categories of data subjects:

The data exporter may submit Personal Data to CP and its Affiliates, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

• Prospective customers, customers, resellers, referrers, business partners, and vendors of the data exporter (who are natural persons);

• Employees or contact persons of the data exporter's prospective customers, customers, resellers, referrers,
subcontractors, business partners, and vendors (who are natural persons);

• Employees, agents, advisors, and freelancers of the data exporter (who are natural persons); and/or

• Natural persons authorized by the data exporter to use the services provided by CP to the data exporter.

Categories of data

The personal data transferred concern the following categories of data: The data exporter may submit Personal Data to CP and its Affiliates, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to, the following categories of Personal Data:

• Names, titles, position, employer, contact information (email, phone, fax, physical address etc.), identification data, professional life data, personal life data, connection data, or localization data (including IP addresses).

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data: The data exporter may submit special categories of data to CP and its Affiliates, the extent of which is determined and controlled by the data exporter in its sole discretion. Such special categories of data include, but may not be limited to, Personal Data with information revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning an individual's health or sex life.