ANDEA DATA PROCESSING ADDENDUM (DPA) FOR MANUFACTURO

This Andea Data Processing Addendum ("DPA") supplements the Andea Terms of Use available at Terms-of-use.pdf (www.manufacturo.com) and supplements and forms an integral part of the Framework Agreement concluded between Andea and Customer.

BACKGROUND

When providing the Services, Andea (hereinafter also referred to as: "data importer") may collect, process and gain access to personal data of individuals on behalf of Customer. From a data protection perspective, Customer (hereinafter also referred to as: "data exporter") will be the data controller and Andea will be the data processor.

This Data Processing Addendum specifies the data protection obligations of the Parties under the Framework Agreement. It applies to all activities performed by Andea in connection with the Framework Agreement in which Andea, its staff and Affiliates or a third party acting on behalf of Andea comes into contact with personal data of individuals.

1. DEFINITIONS

1. <u>Definitions.</u> Any capitalized terms not otherwise defined in this Addendum shall have the following meaning:

TERM	DEFINITION
Addendum / DPA	this Data Processing Addendum with all Exhibits thereto.
Affiliates	the Andea Group entities other than data importer. An overview of all of the Andea group entities is available on the website: https://www.andea.com/company-entities/.
Agreement/Framework Agreement	the Agreement concluded between the Parties on the basis of Terms of Use and applicable Order.
Andea Security Standard	the part of applicable Documentation; security standards applied to Andea services, including in particular EXHIBIT 2 – Technical and Organizational Measures implemented according to Sec. 10.1 of the Data Processing Addendum.
Controller	the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
Customer's Data	the Personal Data subject to this Addendum.
CCPA	California Consumer Privacy Act as amended by the California Privacy Rights Act (CPRA).
Data Subject	any person whose personal data is being collected, held or processed.
GDPR	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.
Data Protection Laws	means the GDPR, CCPA, any applicable national implementing legislation and all applicable legislation protecting the fundamental

	rights and freedoms of persons and their right to privacy with regard to the Processing of User Personal Data
MS Azure	Microsoft Corporation who provides hosting services on the online platform Azure, engaged as Sub-Processor under this Addendum.
MS Azure Network	MS Azure data center facilities, servers, networking equipment, and host software systems (e.g., virtual firewalls) that are within MS Azure control and are used to perform Andea services on the basis of the Agreement.
MS Azure Security Standards	the security standards applied to MS Azure services accepted by the Customer as described in Security Documentation, available (as of the Effective Date) at https://docs.microsoft.com/en-us/azure/security/.
Personal Data	any information relating to an identified or identifiable natural person; who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing	any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Processor	a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.
Standard Contractual Clauses	standard contractual clauses (module 2: Controller to Processor) as adopted by Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as currently set out at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.
Security Incident	a breach of personal data security leading to the accidental or unlawful loss, destruction, alteration, unauthorized disclosure of, or access to Customer Data processed subject to this Addendum.
Services	services as defined in the Framework Agreement.
Sub-Processor	means any Processor engaged by Andea who agrees to receive from Andea User Personal Data, including Affiliates.

2. <u>Reference.</u> Any capitalized terms used in this Addendum not expressly defined in section "Definitions" above (such as "Services") shall be construed in accordance with the <u>Terms of Use</u>.

2. SUBJECT AND SCOPE OF THE ADDENDUM

1. Andea will collect and process personal data in connection with the Framework Agreement only for the purpose of fulfilling the Framework Agreement. Andea will carry out the data processing operations in accordance with the Framework Agreement as well as any written instructions received from Customer that do not conflict with the provisions of this Data Processing Addendum or the Framework Agreement.

2. <u>Details of Data Processing.</u> Andea is entitled to process personal data on behalf of the Customer according to provisions of this Addendum in order to provide Services and within the material scope of personal data as set in Exhibit 1.

3. <u>Compliance with law.</u> Each Party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this Addendum, including the GDPR and the CCPA.

3. PROCESSING OF PERSONAL DATA

1. <u>Customer Instructions.</u> The Parties agree that this Addendum, the Agreement and the applicable Documentation (particularly Andea Security Standards) constitute Customer's documented instructions regarding Andea's Processing of Customer Data ("Documented Instructions") and covers the entirety of the conditions (in particular technical) for Processing Customer Data by Andea in relation to the provision of Services subject to the Agreement. Andea shall process Customer Data only in accordance with Documented Instructions.

2. <u>Additional instructions.</u> Documented Instructions may not cause any alteration of the this Addendum. Any additional instructions outside the scope of Documented Instructions require prior agreement between the Parties.

4. SECURITY

1. <u>Security.</u> Andea has implemented and will maintain the technical and organizational measures for the Processing of Customer Data subject to this Addendum, as described in the applicable Documentation (particularly in Andea Security Standard). The Customer hereby states that it had made itself acquainted with the technical and organizational measures mentioned above, and agrees those measures constitute appropriate technical and organizational measures.

2. <u>Additional security measures.</u> Any additional security measures to be implemented by Andea, whether technical or organizational, require prior consultation between the Parties on such security measure's scope, form and term of implementation as well as on the share of implementation's costs. A request from the Customer to implement additional technical and organizational measures shall require a written form under pain of being declared null and void. The Parties will agree on any supplementary security measures if such will be required by any provision of law or regulatory decision or official guidelines with regard to transfer of personal data outside of the European Economic Area (EEA).

3. <u>Confidentiality of Customer Data</u>. Andea will not disclose to any third party, any Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as or court order). If a governmental body sends Andea a demand for Customer Data, Andea will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, Andea to the extent legally permitted may provide Customer's basic contact information to the governmental body. If compelled to disclose Customer Data to a governmental body, then Andea will give to the extent legally permitted Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Andea is legally prohibited from doing so.

4. <u>Confidentiality Obligations of Andea Personnel.</u> Andea restricts its personnel from Processing Customer Data without authorisation by Andea as described in the Andea Security Standards. Andea imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security. In particular, Andea warrants that its personnel engaged in the Processing of Personal Data is informed of the confidential nature of the Customer Data, has received appropriate training and is subject to obligations of confidentiality. Andea shall ensure that such confidentiality obligations survive the termination of the personnel engagement. Andea shall ensure that access to Personal Data is limited only to those personnel who require that access in order to fulfil Andea's obligations under the Agreement.

5. DATA SUBJECT RIGHTS

1. Notifications. Andea shall notify Customer, to the extent legally permitted, if Andea receives a request from Data Subject in the subject of access to, correction, amendment, deletion of or objection to the Processing of that Data Subject's Customer Data. Andea shall not respond to any such request.

2. Assistance. Taking into account the nature of the Processing, whenever possible and using commercially reasonable efforts, Andea shall provide the Customer with assistance to meet their obligation to respond to the Data Subject, so that such a Data Subject may exercise their right pursuant to applicable law, including Chapter III of the GDPR (if applicable). To the extent legally permitted, Andea reserves the right to charge additional fees in relation to this cooperation with the Customer.

6. SUB-PROCESSING

1. Appointment of Sub-Processors. Customer acknowledges and agrees that Andea may engage its Affiliates (on the basis of the Andea Group Data Processing Agreement) and third-party Sub-Processors in connection with the provision of the Services. This consent includes Affiliates and the entities indicated below (third-party Sub-processors), as well as other entities (other than Affiliates and third-party Sub-processors), about the involvement of which the Processor will notify the Data Controller (in a written or electronic form), and to which the Data Controller will not object within 7 days of receiving the notification (in a written or electronic form). Andea has entered into (or will enter into in case of future Sub-Processors) an agreement with each Sub-Processor containing data protection obligations not less protective than those in this Addendum with respect to the protection of Customer Data to the extent applicable to the nature of the Services provided by such Sub-Processor. Andea shall engage only Sub-Processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of applicable law and ensure the protection of the rights of the data subject. Andea will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-Processor without unreasonably burdening Customer. If Andea is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the Agreement with respect only to those Services which cannot be provided by Andea without the use of the objected-to new Sub-Processor by providing written notice to Andea. Andea will refund Customer any prepaid fees with respect to such terminated Services.

2. List of Current Sub-Processors. The list of current thirt-party Sub-Processors is as set hereinbelow:

Name of Sub-Processor	Location	Relevant documentation	Service	Transborder transfer of data mechanism
Microsoft Corp.	United States of America	https://www.microsoft.com/en-us/trust-center/privacy Microsoft Privacy Statement – Microsoft privacy	Microsoft Azure cloud hosting services	Standard contractual clauses as adopted by the EU Commission + supplementary measures
Pipedrive OU	Estonia	https://support.pipedrive.com/en/article/pipedrive-and-gdpr	CRM Platform	-
Qwilr Pty Ltd	Australia	https://qwilr.com/privacy-policy/	Proposals & documents preparation tool	*Standard contractual clauses as adopted by the EU Commission + supplementary measures*
Intuit Mailchimp	United States of America	https://www.intuit.com/privacy/statement/ https://mailchimp.com/legal/terms/?_ga=2.82612246.1696356725.1674218671-1795644034.1673527665	Email campaign tool	*Standard contractual clauses as adopted by the EU Commission + supplementary measures*

Version: [_1.3_]
Last updated in: [_2023-04-17__]

GoTo, Inc.	United States of America	https://www.goto.com/company/legal/privacy	Webinar software and virtual conference platform	*Standard contractual clauses as adopted by the EU Commission + supplementary measures*

3. <u>Andea responsibility for Sub-Processors</u>. Where Andea authorizes any Sub-Processor, as described in this section, Andea will:

   a) restrict the Sub-Processor's access to Customer Data only to what is necessary to fulfill the Agreement, and will prohibit the Sub-Processor from accessing Customer Data for any other purpose,

   b) remain responsible for compliance with the obligations of this Addendum and for any acts or omissions of the Sub-Processors that cause Andea to breach any of its obligations under this Addendum, without prejudice to section 6 ("Andea responsibility limitation") and 7 ("MS Azure sole liability") below.

4. <u>Andea responsibility limitation</u>. The Customer agrees that Andea is relieved from any liability for any acts or omissions of the Sub-Processors (including but not limited to liability for personal data breaches), if Andea has done its due diligence in reviewing whether a new Sub-Processor engaged in the Processing of Customer Data provides sufficient guarantees of implementing appropriate technical and organizational measures and the Customer approved the choice of such Sub-Processor pursuant to this section 6.

5. <u>MS Azure sole liability</u> The Customer agrees not to seek redress or claim any damages from Andea in the event of personal data breach regarding or resulting from MS Network or any act or omission on part of MS. The Customer hereby agrees that MS is solely responsible for MS services as well as data protection within MS Network according to the MS Azure terms of service.

7. TRANSBORDER DATA TRANSFER

<u>Transborder transfers of data.</u> Notwithstanding the provisions of section 6, the Customer hereby authorizes Andea to transfer Customer Data outside of the European Economic Area (EEA), in particular USA, including subcontracting the Processing to the Sub-Processors based outside of the European Economic Area (EEA) in particular USA - to the extent necessary to duly perform Services, under the condition that the Sub-Processors will provide sufficient guarantees in relation to the required level of data protection, e.g. through a subcontracting agreement based on the Standard Contractual Clauses, or based on other applicable transborder data transfer mechanisms.

8. LIABILITY AND INDEMNIFICATION

1. <u>Indemnity.</u> Customer shall indemnify and hold Andea, its officers, directors, employees, contractors, and agents harmless from and against all claims, liabilities, administrative fines, suits, judgments, actions, investigations, settlements, penalties, fines, damages and losses, demands, costs, expenses, and fees including reasonable attorneys' fees and expenses, arising out of or in connection with any claims, demands, investigations, proceedings, or actions brought by the Data Subject, legal persons (e.g., corporations and organizations), or supervisory authorities under the data protection laws that apply to Andea in respect of Processing of Customer Data on behalf of Customer in accordance with this Addendum.

2. <u>Limit of liability.</u> Notwithstanding the provisions of section "Indemnity" and section "Sub-Processing" - item 6 and 7, the liability of each Party under this Addendum shall be subject to the exclusions and limitations of liability set out in the <u>Terms of Use</u>.

9. SECURITY BREACH MANAGEMENT AND NOTIFICATION

Version: [_1.3_]
Last updated in: [_2023-04-17__]

1. Security Incident. Andea shall:

   a) notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of Customer's Data; and

   b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

2. Andea Assistance. To assist the Customer in relation to any personal data breach notifications, Andea will include in the notification such information about the Security Incident as Andea is reasonably able to disclose to the Customer, taking into account the nature of the services subject to this Addendum and the Agreement, the information available to Andea, and any restrictions on disclosing the information, such as confidentiality.

10. TECHNICAL MEASURES AND INSPECTIONS

1. Technical measures. Andea will implement the technical and organizational security measures as set forth in Exhibit 2 to this Data Processing Addendum. The technical and organizational security measures will be aimed at protecting the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing.

2. Audit report. Upon Customer's request, but not more frequently than once in any twelve (12) month period, Andea will provide a self-audit report or a third--party report confirming compliance with the technical and organizational security measures before processing or accessing any Personal Data on behalf of Customer.

3. Necessary information. Andea shall provide the Customer without undue delay – on the Customer's demand – with all necessary information proving the obligations set out in the Addendum to be met, and shall enable the Customer access to them, with due respect to professional secrecy and Andea's trade secret.

11. TERM AND TERMINATION

1. Termination Date. This Addendum shall remain in force until the termination of the Agreement (the "Termination Date"), under the conditions of termination stipulated therein.

2. Return or Deletion of Customer Data. Up to the Termination Date, the Customer may export some Customer Data contained in the Platform to the scope indicated in Documentation and in a manner agreed with Andea and only within 3 months after expiration. After a period up to 3 months following such expiry, all the Customer Data will be deleted and no longer available to Customer, which the Customer acknowledges and agrees to it.

12. MISCELLANEOUS

1. Representations. Each Party represents and warrants that it has validly entered into this Addendum and has the legal power to do so.

2. Governing law. The Data Processing Addendum is governed by the law indicated as the governing law in the respective provisions of the Framework Agreement.

3. Manner of giving notice. All notices, notifications, requests, additional agreements and consultations between the Parties shall be made in accordance with the terms set forth in the Agreement.

EXHIBIT 1 - DETAILS OF DATA PROCESSING

Subject matter and nature of the Processing

Performance of the Andea Services pursuant to the Agreement, particularly compute, storage and such other Services as described in the Documentation.

Categories of data subjects

Customer may submit Customer Data in the course of its use of the Services (particularly by uploading them to the Platform), the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

a) *Customer's directors, officers, employees, interns, trainees, agents, contractors, job applicants, customers, suppliers, subcontractors, business contacts, vendors, users;*

b) *Customer clients' directors, officers, employees, interns, trainees, agents, contractors, customers or business contracts;*

c) *Any third party with whom Andea interacts or is requested to interact in connection with the provision, operation, or maintenance of the Services on behalf of Customer;*

d) *Any other individuals for which Company enters personal data or information into the Service*

   Andea will not have any knowledge or control over the categories or identities of the Data Subjects whose Personal Data Company may elect to record or upload into the Service, except as provided in the Framework Agreement

Categories of personal data

Customer may submit Customer Data in the course of its use of the Services (particularly by uploading them to the Platform), the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Personal Data:

a) *First name and last name, , email address, phone number, username, password, cookies, IP address, company name, title, role, skills and assignment to organization structure, SSH public key;*

b) *Customer history;*

c) *Contract billing and bank data;IP Addresses;*

d) *References, meeting notes; and*

e) *Such categories of personal data pertaining to an identified or identifiable individual as Company or Company's representative may enter or upload from time to time into the Service.*

Andea will not have any knowledge or control over the categories or identities of the Personal Data that Customer may elect to record or upload into the Service, except as provided in the Framework Agreement

EXHIBIT 2 – Technical and Organizational Measures implemented according to Sec. 10.1 of the Data Processing Addendum:

Clause 1

Organizational and Security measures

1. Andea has internal personal data processing policies in place. Every employee of Andea is obliged to get familiar with the policies before accessing personal data.
2. Every employee of Andea is obliged to sign an NDA before commencing work at Andea.
3. The policies are reviewed annually to keep them up-to-date in accordance with the industry standards.
4. Violation of the policies by an employee may cause penalties varying from written notice to dismissal.
5. Security breaches are reported to the company's senior management.
6. Andea runs security audits.
7. Andea maintains a personal data processing policy.
8. Andea ensures the compliance of Subprocessors and data processing partners with applicable data protection regulations.

Clause 2

Data access

1. Physical access to production environment:

   a) Andea uses Microsoft Azure or other hosting providers as identified in this list https://www.Andea.com/legal/privacy/third-parties.html for hosting of data.
   b) Employed hosting providers utilize secure premises for storage and encrypted physical communications channels compliant with recent security standards.

2. Availability

   a) Andea uses scalable services for business-critical functionality to provide high availability of its applications to users.
   b) Andea employs third-party hosting providers' stable infrastructure to improve the availability of its products and services.
   c) Employed hosting providers provide Andea with the functionality of restoring from backups for business-critical processes and restoring the availability of and access to personal data in a timely manner in the event of a physical or technical incident.

3. System access

   a) Access to production systems is limited to authorized employees who require the access to perform their duties.
   b) Accounts used for access to production systems are terminated when an employee leaves Andea.

4. Permissions management

   a) Access to data or systems is provided on a "need-to-know" basis.
   b) Employees involved in development do not have access to production infrastructure unless it is required for the support or provision of services.

Version: [__]
Last updated: [__]

5. Andea keeps track of (logs) the most important data processing activities, i.e., amendment, deletion, etc., in order to enable Andea and Customer to demonstrate due protection of personal data processed and compliance with data protection regulations in general.

Clause 3

Data security

1. Andea makes commercially reasonable efforts to protect processed personal data from unauthorized access and to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services.
2. Data storages are encrypted when the encryption noticeably improves data security.
3. The transfer of data outside Andea premises or premises Andea maintains is secured with certificates of actual TLS versions, in order to prevent any unauthorized subject from capturing and reading the personal data that are subject to the transfer.

Clause 4

Incident management

1. To respect the privacy of its users and protect the business from risks imposed by security incidents, Andea:

   i.   Maintains breach response and breach notification policies.
   ii. Maintains a data breach registry.
   iii. Shall notify the controller (and, if the controller so wishes, the corresponding authority or data subjects, the latter being subject to limitations according to Art. 34 paragraph 3 of the GDPR) of an incident without undue delay and in accordance with the GDPR.

EXHIBIT 3

INTERNATIONAL DATA TRANSFER MECHANISMS

1. The Parties enter into and incorporate into this DPA Standard Contractual Clauses as amended and completed as follows:
    (1) Applicable Module: Module 2 – Controller to Processor.
    (2) In clause 7 of the Standard Contractual Clauses, the optional docking clause will not apply.
    (3) In clause 9 of the Standard Contractual Clauses, Option 2 (general authorisation) will apply. The data importer shall specifically inform the data exporter of any intended changes to that list through the addition or replacement of sub-processors at least 7 days in advance.
    (4) In clause 17 of the Standard Contractual Clauses, Option 1 is selected and the Standard Contractual Clauses will be governed by the law of Poland.
    (5) In clause 18 (b) of the Standard Contractual Clauses disputes will be resolved before the courts in Krakow-Śródmieście, Poland.
    (6) In Annex I, Part A "List of the Parties" of the Standard Contractual Clauses:

Data exporter:

a) The entity indicated in the Framework Agreement (Manufacturo Order Form) as the Client/Customer.
b) Contact person's name, position and contact details as indicated in the Framework Agreement (Manufacturo Order Form/ section Coordinators).
c) Activities relevant to the data transferred under these Clauses: Delivery or granting access to data necessary for the performance of the Andea Services pursuant to the Agreement, particularly to compute, store and such other activities within the Services as described in the Documentation.
d) Signature and date: By entering into this DPA, data exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the DPA.
e) Data exporter role: controller.

Data importer:

a) The Andea Group company indicated in the Framework Agreement (Manufacturo Order Form) as the service provider.
b) Contact person's name, position and contact details: rodo@andea.com.
c) Activities relevant to the data transferred under these Clauses: Performance of the Andea Services pursuant to the Agreement, particularly to compute, store and such other activities within the Services as described in the Documentation.
d) Signature and date: By entering into this DPA, data exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the DPA.
e) Data importer role: processor.

    (7) In Annex I, Part B of the Standard Contractual Clauses (Description of transfer):
    a) Categories of data subjects whose personal data is transferred: As described in Exhibit 1 to the DPA.
    b) Categories of personal data transferred: As described in Exhibit 1 to the DPA.
    c) The frequency of the transfer: On continuous basis.
    d) Nature of the processing: As described in Exhibit 1 to the DPA.
    e) Purpose(s) of the data transfer and further processing: To fulfil obligations under the Frame Agrement (e.g. to provide Services).
    f) The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: For the duration of provision of Services.
    g) For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: As described in section 6.1 and 6.2 of the DPA.

    (8) In Annex I, Part C of the Standard Contractual Clauses: Prezes Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa, Poland will be the competent supervisory authority.
    (9) Exhibit 2 (Technical and Organizational Security Measures) of this DPA serves as Annex II of the Standard Contractual Clauses.

Version: [__]
Last updated: [__]

(10) Annex III (List of sub-processors) of the Standard Contractual Clauses: The controller has authorised the use of the sub-processors as provided in section 6.1 and 6.2 of the DPA.

2. To the extent that UK Personal Data is transferred to countries which are not covered by UK adequacy regulations issued under Section 17A UK Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the UK Data Protection Act, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, as issued by the UK Information Commissioner's Office, version B1.0 as in force as of 21 March 2022 as currently set out at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf (hereinafter referred to as: "UK SCC") as amended or completed as follows:

    (1) In Table 1 of the UK SCC tha parties' details and key contact information is located in point 1 (6) of this Exhibit 3.

    (2) In Table 2 of the UK SCC 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 is Module 2 (see: this Exhibit 3).

    (3) In Table 3 of the UK SCC: List of Parties, Description of Transfer are located in point 1(6) of this Exhibit 3, Technical and organizational measures – in Exbibit 2, List of sub-processors – in clauses 6.1 and 6.2 of the DPA.

    (4) In the Table 4 of the UK SCC both exporter and importer may end the UK SCC in accordance with the terms of the UK SCC.

3. To the extent that Personal Data is processed in accordance with the Main Agreement, which Personal Data is within the scope of the California Consumer Privacy Act (CCPA), 1) Andea and Customer act as a CCPA Service Provider; and 2) make the following additional commitments to Customer: Andea will not retain, use, or disclose that data for any purpose other than for the purposes set out in this DPA and as permitted under the CCPA, including under any "sale" exemption. In no event will Andea sell any such data; and 3) will not combine Customer's Data with personal data that it receives from, or on behalf of, another person or entity than Customer. These CCPA terms do not limit or reduce any data protection commitments Andea make in this DPA or the Frame Agreement.