Data Processing Addendum

This DPA is entered into between the Customer and Prodly, Inc., a California corporation (**Prodly**), and is incorporated into and governed by the terms of the Subscription Services Agreement between the parties.

DEFINITIONS.

Any capitalized term not defined in this DPA will have the meaning given to it in the Agreement (defined below).

a. **Affiliate** *means* any entity that directly or indirectly controls, is controlled by, or is under common control of a party. "Control" for purposes of this definition *means* direct or indirect ownership or control of more than 50% of the voting interests of a party.

b. **Agreement** *means* the Subscription Services Agreement between the Customer and Prodly for the provision of the Services.

c. **CCPA** *means* the California Consumer Privacy Act of 2018, along with its regulations, and as amended.

d. **Controller** *means* the Customer, the entity which determines the purposes and means of the process of Personal Data.

e. **Customer Data** *means* data, which may include Personal Data, and the categories of data submitted, stored, sent, or received via the Services by the Customer, its Affiliates, or end users.

f. **Data Protection Laws** *means* all laws and regulations applicable to the processing of Personal Data under the Agreement, including, but not limited to, the GDPR and the CCPA.

g. **Data Subject** *means* (i) the identified or identifiable person to whom Personal Data relates; or (ii) a "Consumer" as the term is defined in the CCPA.

h. **DPA** *means* this data processing addendum and its schedules (together).

i. **GDPR** *means* 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.

j. **Model Contract Clauses** *means* the standard contractual clauses for personal data transfer from controllers to processors adopted by the European Commission pursuing to its Implementing Decision (EU) 2021/914 of 4 June 2021 as set out in Schedule 4 of this DPA.

k. **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), which is provided as Customer Data.

l. **Processor** *means* Prodly, the entity which Processes Personal Data on behalf of Controller, including as applicable any "Service Provider" as that term is defined by the CCPA.

m. **Sub-processors** *mean* any person or entity engaged by Prodly or an Affiliate to process Personal Data in the provision of the Services to Customer.

n. **Services** *means* the web subscription services provided by Prodly.

1. **PURPOSE.**

a. Prodly has agreed to provide the Services to the Customer in accordance with the terms of the Agreement. In providing the Services, Prodly will process Customer Data on behalf of the Customer. Customer Data may include Personal Data. Prodly will process and protect such Personal Data in accordance with the terms of this DPA and the Data Protection Laws.

b. With respect to Customer Data under this DPA, the parties agree that the Customer is the “data controller” and Prodly is the “data processor.” The Customer will comply with its obligations as a controller and Prodly will comply with its obligations as a processor under the DPA.

c. Where a Customer Affiliate or a Customer client is the controller with respect to certain Customer Data, the Customer represents and warrants to Prodly that it is authorized to instruct Prodly and otherwise act on behalf of such

Customer Affiliate or Customer client in relation to the Customer Data in accordance with the Agreement and this DPA.

2. SCOPE.

In providing the Services to the Customer pursuant to the terms of the Agreement, Prodly will treat Personal Data as confidential and only process Personal Data on behalf of the Customer, and only to the extent necessary to provide Services and in accordance with the Customer's instructions as documented in the Agreement and this DPA.

3. PRODLY OBLIGATIONS.

a. Prodly may collect, process, or use Personal Data only in accordance with the scope of the Agreement, this DPA, and the Customer's instructions. This DPA is the Customer's complete and final documented instruction to Prodly in relation to Personal Data. Additional instructions outside the scope of this DPA (if any) require prior written agreement between Prodly and the Customer, including agreement on any additional fees payable by the Customer to Prodly for carrying out such instructions.

b. Prodly will ensure that all employees, agents, officers, and contractors involved in the handling of Personal Data: (i) are aware of the confidential nature of the Personal Data and are contractually bound to keep the Personal Data confidential; (ii) have received appropriate training on their responsibilities as a data processor; and (iii) are bound by terms materially no less restrictive than the terms of this DPA.

c. Prodly must maintain appropriate managerial, operational, and technical safeguards designed to preserve the integrity and security of Customer Data while in its possession and control hereunder, while taking into account the state of the art, 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.

d. Prodly must maintain appropriate measures to ensure a level of security appropriate to the risk, as further set forth in Schedule 2.

e. Customer agrees that, in the course of providing the Services to the Customer, it may be necessary for Prodly to access the Personal Data to respond to any technical problems, Customer queries, security monitoring, and to ensure the proper working of the Services. All such access by Prodly will be limited to those purposes and performed by authorized personnel.

f. Where Personal Data relating to an EU Data Subject is transferred outside of the European Economic Area (EEA), it will be processed in accordance with the provisions of the Model Contract Clauses, unless the processing takes place: (i) in a third country or territory recognized by the EU Commission to have an adequate level of protection; or (ii) by an organization located in a country which has other legally recognized appropriate safeguards in place, such as the Binding Corporate Rules. Where Personal Data relating to a United Kingdom (UK) Data Subject is transferred outside of the UK, it will be processed in accordance with the provisions of the standard contractual clauses adopted by European Commission Decision C(2010)593 or any successor standard contractual clauses approved by the UK Information Commissioner's Office.

g. Prodly will reasonably assist the Customer in meeting its obligation to carry out Data Protection Impact Assessments (DPIAs), taking into account the nature of processing and the information available to Prodly.

h. The Customer and Prodly and, where applicable, their representatives, will cooperate, upon request, with a supervisory data protection authority in the performance of their respective obligations under this DPA.

i. Prodly may not (i) sell Personal Data; (ii) retain, use, or disclose Personal Data for commercial purposes other than providing the Services under the terms of the Agreement; or (iii) retain, use, or disclose Personal Data outside of the Agreement. Prodly understands these restrictions.

4. CUSTOMER OBLIGATIONS.

a. The Customer represents and warrants, in its use of the Services, that it will comply with the terms of the Agreement, this DPA, and the Data Protection Laws. All Affiliates of Customer that use the Services will comply with the obligations of the Customer set out in this DPA.

b. The Customer represents and warrants that, having sole responsibility for Customer Data quality, legality, and accuracy, it has obtained any and all necessary permissions and authorizations necessary to permit Prodly, its Affiliates, and Sub-processors, to execute their rights or perform their obligations under this DPA.

c. The Customer represents and warrants that: (i) its instructions comply with Data Protection Laws; and (ii) some instructions from the Customer, including assisting with audits, inspections, or DPIAs (defined below) by Prodly, beyond the reasonable assistance Prodly generally provides to its customers during an audit, inspection, or DPIA), may result in additional fees. Prodly will notify the Customer in advance of its fees for providing such assistance.

d. The Customer must inform Prodly of any notice, inquiry (including any notice, investigation, complaint, or request) relating to Processor's processing of Personal Data and provide Processor with a copy thereof within 48 hours of receipt. Notices should be sent to privacy@prodly.co.

5. **NOTIFICATION OF SECURITY BREACH.**

a. Prodly will notify the Customer without undue delay after becoming aware of (and in any event within 72 hours of discovering) any confirmed accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access to the Customer's Personal Data ("Data Breach").

b. Prodly will take all commercially reasonable measures to secure the Personal Data, to eliminate the Data Breach, and to assist the Customer in meeting the Customer's obligations under applicable law. In the event of a Data Breach, Prodly's System Administration Team and Security Team will perform a risk-based assessment of the situation and develop appropriate strategies in accordance with Prodly incident response procedures, which include contacting the Customer and to contact the Customer's primary (technical or business) point of contact or Security Operation Center (SOC) to brief them on the situation and provide resolution status updates.

6. **AUDIT.**

a. Prodly will make available to the Customer all information reasonably necessary to demonstrate compliance with its processing obligations and allow for and contribute to audits and inspections.

b. Any audit conducted under this DPA will consist of examination of the most recent reports, certificates, and/or extracts prepared by an independent auditor bound by confidentiality provisions similar to those set out in the Agreement. In the event that provision of the same is not deemed sufficient in the reasonable opinion of the Customer, the Customer may conduct a more extensive audit which will be: (i) at the Customer's expense; (ii) limited in scope to matters specific to the Customer and agreed in advance; (iii) carried out during business hours and upon reasonable notice which must be not less than 4 weeks unless an identifiable material issue has arisen; and (iv) conducted in a way which does not interfere with Prodly's day-to-day business. This clause does not modify or limit the rights of audit of the Customer, instead it is intended to clarify the procedures in respect of any audit undertaken pursuant thereto.

7. **DATA SUBJECTS.**

a. Prodly must, to the extent legally permitted, promptly notify the Customer if Prodly receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of processing, erasure, data portability, object to the processing (Data Subject Request).

b. Taking into account the nature of the processing, Prodly must assist the Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Customer's obligation to respond to a Data Subject Request under the Data Protection Laws.

c. To the extent the Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Prodly must upon the Customer's request, and to the extent possible, provide commercially reasonable efforts to assist the Customer in responding to such Data Subject Request, to the extent Prodly is legally permitted to do so and the response to such Data Subject Request is required under data protection laws. To the extent legally permitted, the Customer must be responsible for any costs arising from Prodly's provision of such assistance.

8. **SUB-PROCESSORS.**

a. The Customer agrees that: (i) Affiliates of Prodly may be used as Sub-processors; and (ii) Prodly and its Affiliates respectively may engage Sub-processors in connection with the provision of the Services. The current list of Sub-processors is available at https://prodly.co/legal/subprocessors/.

b. All Sub-processors that process Personal Data in the provision of the Services to the Customer will comply with the obligations of Prodly set out in this DPA.

c. Where Sub-processors are located outside of the EEA, Prodly confirms that such Sub-processors: (i) are located in a third country or territory recognized by the EU Commission to have an adequate level of protection; (ii) have entered

into the Model Contract Clauses or other duly approved standard contractual clauses with Prodly; or (iii) have other legally recognized appropriate safeguards in place, such as the Binding Corporate Rules.

d. During the term of this DPA, Prodly will provide the Customer with prior notification, via email, of any changes to the list of Sub-processors who may process Personal Data before authorizing any new or replacement Sub-processors to process Personal Data in connection with the provision of the Services. Notification to Customer will be provided to the email address(s) provided in the Order Form for the Service. Additionally, Customer may sign up for notification at https://prodly.co/legal/subprocessors/.

e. The Customer may object to the use of a new or replacement Sub-processor, by notifying Prodly promptly in writing within 10 days after receipt of Prodly's notice. If the Customer objects to a new or replacement Sub-processor, and that objection is not unreasonable, the Customer may terminate the Agreement or applicable order with respect to those Services which cannot be provided by Prodly without the use of the new or replacement Sub-processor. Prodly will refund the Customer any prepaid and unused fees covering the remainder of the term of the applicable order following the effective date of termination with respect to such terminated Services.

9. **LIABILITY.**

a. The parties agree that Prodly will be liable for any breaches of this DPA caused by the acts and omissions of its Sub-processors to the same extent Prodly would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

b. The parties agree that the Customer will be liable for any breaches of this DPA caused by the acts and omissions of its Affiliates and users as if such acts and omissions had been committed by the Customer itself.

c. Any liabilities arising under this DPA are subject to the limitations of liability in the Agreement.

10. **TERM AND TERMINATION.**

a. This DPA will automatically terminate upon the termination of the Agreement.

b. Prodly will, upon written request: (i) make the Services available to the Customer for the return of Customer Data to the Customer at the expiration of the order within the time periods set out in the Agreement; (ii) securely delete all Customer Data after such time period unless applicable law with respect to Prodly prevent destruction of the Customer Data; and (iii) provide a certification of deletion of Customer Data.

c. Where any Customer Data is retained for such reasons, the Customer Data must be treated as Confidential Information and will no longer be actively processed.

11. **GENERAL.**

a. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

b. This DPA sets out the entire understanding of the parties, and supersedes all prior and contemporaneous agreements and understandings, with regards to the subject matter. No modification or waiver of any term in this DPA is effective unless both parties sign it.

c. Should a provision of this DPA be invalid or become invalid, then the legal effect of the other provisions will be unaffected. A valid provision is deemed to have been agreed upon, which comes closest to what the parties intended commercially and will replace the invalid provision. The same will apply to any omissions.

d. To the extent of any conflict or inconsistency between the terms of this DPA, the Model Contract Clauses, and the Agreement, the following order of precedent applies: The Model Contract Clauses; the Agreement, including without limitation the disclaimer of damages and limitation of liability in the Agreement; and this DPA. Subject to the amendments in this DPA, the Agreement remains in full force and effect.

e. Customer may send any questions or concerns regarding this DPA to privacy@prodly.co.

_____ **(Customer)**	**Prodly, Inc.** **(Prodly)**
Signature:	**Signature:** Daniel Rudman

Printed Name:	**Printed Name:** Daniel Rudman
Title:	**Title:** Founder & CTO
Date:	**Date:** 8/17/2022
Address:	**Address:** 3101 Park Boulevard Palo Alto, CA 94306

Schedules Attached

Schedule 1 - Categories of Data

Schedule 2 - Technical and Organizational Security Measures

Schedule 3 - EU Model Contract Clauses

Schedule 1

Categories of Data

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Schedule.

Data exporter

- The data exporter is the Customer and its end users.

Data importer

- The data importer is Prodly, Inc., a provider of a software service.

Categories of Data

- The personal data transferred concern the following categories of data:
    - Email
    - First and Last Name
    - Salesforce Org IDs and Names
    - Salesforce Record IDs

Data Subjects:

- The personal data transferred concern the following categories of data subjects (please specify):
    - Website end-users
    - Application end-users
    - Customers (contact persons/representatives)
    - Prospects (contact persons/representatives)

Processing Operations:

- With respect to Customer's data, the parties acknowledge and agree that Customer is the 'data controller' (as defined in the Data Protection Legislation) and Prodly is a 'data processor' (as defined in the Data Protection Legislation). Customer will comply with its obligations as a 'data controller' and Prodly will comply with its obligations as a 'data processor' under the agreement.

- Prodly will only process Customer data in the performance of the Services in accordance with Customer's written instructions as documented in this DPA.

Schedule 2

Technical and Organizational Security Measures

Prodly shall have in place security safeguards designed to conform to or exceed industry best practices regarding the protection of the confidentiality, integrity and availability of customer data. These information security safeguards shall be materially consistent with, or more stringent than, the safeguards described in this Schedule.

Prodly is ISO 27001 standard aligned.

- Asset Management Policy
- General information security policy
- Data classification policy
- Access control policy
- Remote access policy
- Acceptable use policy
- General password policy
- Incident response, business continuity and disaster recovery policy
- Data backup, retention and disposal policy
- Policy governing storage of data on mobile devices (corporate and personal)
- Security awareness policy
- Change management policy
- Configuration management policy
- Vulnerability and patch management policy
- Data media security policy
- Physical access policy
- Breach notification policy
- Risk management policy
- Third party risk management policy
- Logging and monitoring policy

Schedule 3

Model Contract Clauses

STANDARD CONTRACTUAL CLAUSES (CONTROLLER TO PROCESSOR)

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) for the transfer of 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), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time,

the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

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

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that

list through the addition or replacement of sub-processors at least 10 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorized to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

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

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 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) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) 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 and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) 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.

(f) The Parties agree that if one Party is held liable under paragraph (e), 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.

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

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

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

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

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

Clause 15

Obligations of the data importer in case of access by public authorities

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 non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of France.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the EU Member State in which the data exporter is established.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

See Schedule 1 to this DPA.

B. DESCRIPTION OF TRANSFER

See Schedule 1 to this DPA.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority in the EU Member State in which the data exporter is established.

ANNEX II

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

See Schedule 2 to this DPA.

ANNEX III

LIST OF SUB-PROCESSORS

See https://prodly.co/legal/subprocessors/.