Recurly Personal Data Processing Addendum

This Personal Data Processing Addendum ("Addendum") forms a part of the Master Services Agreement (the "Agreement") entered into by and between the merchant who executed the Agreement ("Merchant") and Recurly, Inc. ("Recurly"). By executing the Addendum in accordance with Section 11 herein, Merchant enters into this Addendum on behalf of itself and, to the extent required under applicable Data Protection Laws (defined below), in the name and on behalf of its Affiliates (defined below), if and to the extent Recurly processes Personal Data for which such Affiliates qualify as the Controller (defined below). Any terms not defined in this Addendum shall have the meaning set forth in the Agreement. In the event of a conflict between the terms and conditions of this Addendum and the Agreement or any other agreement between the parties (including any prior data processing addenda), the terms and conditions of this Addendum shall supersede and control. In the event of a conflict between the Standard Contractual Clauses (as defined below and where applicable) with any provision of this Addendum, the Standard Contractual Clauses shall prevail to the extent of such conflict.

1. Definitions

1.1 "Affiliate" means (i) an entity of which a party directly or indirectly owns fifty percent (50%) or more of the stock or other equity interest, (ii) an entity that owns at least fifty percent (50%) or more of the stock or other equity interest of a party, or (iii) an entity which is under common control with a party by having at least fifty percent (50%) or more of the stock or other equity interest of such entity and a party owned by the same person, but such entity shall only be deemed to be an Affiliate so long as such ownership exists.

1.2 "Anonymous Data" means Personal Data that has been processed in such a manner that it can no longer be attributed to an identified or identifiable natural person.

1.3 "Authorized Employee" means an employee of Recurly who has a need to know or otherwise access Personal Data to enable Recurly to perform their obligations under this Addendum or the Agreement.

1.4 "Authorized Sub-Processor" means a third-party who has a need to know or otherwise access Personal Data to enable Recurly to perform its obligations under this Addendum or the Agreement, and who is either (1) listed at https://recurly.com/legal/privacy/subprocessors or (2) authorized by Merchant to do so under Section 4 of this Addendum.

1.5 "Controller" (or "data controller") means 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, including as applicable any "business" as defined under the CCPA (as defined below).

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

1.7 "Instruction" means a direction, either in writing, in textual form (e.g., by e-mail) or by using a software or online tool, issued by Merchant to Recurly and directing Recurly to Process Personal Data.

1.8 "Personal Data" means any information relating to Data Subject which is subject to Data Protection Laws (defined below) and which Recurly Processes on behalf of Merchant other than Anonymous Data.

1.9 "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data in Recurly's possession or control.

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

1.11 "Processor" means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of a Controller, including as applicable any "service provider" as defined under the CCPA (defined below).

1.12 "Services" shall have the meaning set forth in the Agreement.

1.13 "Standard Contractual Clauses" means the standard contractual clauses module for the transfer of Personal Data by Controllers to Processors as approved by the European 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 as such Model Clauses may be subsequently updated by the European Commission, attached as [**Annex C**] and forming part of this Addendum executed by and between Merchant and Recurly .

1.14 "Supervisory Authority" means an independent public authority with jurisdiction over the Processing subject to this Addendum.

2. Processing of Data

2.1 The rights and obligations of Merchant with respect to this Processing are described herein. As between Recurly and Merchant, except as otherwise provided herein, Merchant is the Controller of Personal Data and Recurly shall process Personal Data only as a Processor acting on behalf of Merchant. In the event that, during the course of the Agreement, in response to emerging guidance or legislation Recurly considers that its categorization for any Processing carried out under the Agreement should change from Processor to Controller, Recurly shall provide written notice of this change to Merchant and the parties agree that the terms under this Addendum relating to the new status shall apply to all Processing from the date of receipt of such notice.

2.2 Merchant shall, in its use of the Services, at all times Process Personal Data, and provide instructions for the Processing of Personal Data, in compliance with the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR"), the California Consumer Privacy Act (the "CCPA"), and any other applicable legislation relating to data protection and privacy (together with the GDPR and CCPA, "Data Protection Laws"). Merchant shall ensure that its Instructions comply with all laws, rules and regulations applicable in relation to the Personal Data, and that the Processing of Personal Data in accordance with Merchant's Instructions will not cause Recurly to be in breach of the Data Protection Laws. Merchant is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Recurly by or on behalf of Merchant, (ii) the means by which Merchant acquired any such Personal Data, and (iii) the Instructions it provides to Recurly regarding the Processing of such Personal Data, including providing notice and obtaining all consents and rights necessary for Recurly to process Personal Data pursuant to the Agreement and this Addendum. Merchant shall not provide or make available to Recurly any Personal Data in violation of Data Protection Laws or the Agreement or otherwise inappropriate for the nature of the Services, and shall indemnify Recurly from all claims and losses in connection therewith.

2.3 Recurly, in its capacity as the Processor, shall not (a) retain, use, sell, or otherwise disclose Personal Data outside of its relationship with Merchant other than as required by law, as stated in the Agreement or in this Addendum, or as necessary to provide the Services or (b) Process Personal Data (i) for purposes other than those set forth in the Agreement and/or **Annex I**, and (ii) in a manner inconsistent with the terms and conditions set forth in this Addendum or any other documented Instructions provided by Merchant, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by any law or regulation to which Recurly is subject. Merchant hereby instructs Recurly to Process Personal Data in accordance with the foregoing and as part of any Processing initiated by Merchant in its use of the Services.

2.4 Following completion of the Services, at Merchant's choice, Recurly shall return or delete the Personal Data, unless further storage of Personal Data is required or authorized by applicable law. If Merchant and Recurly have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the certification of deletion of Personal Data that is described in Clause 8.5 of the Standard Contractual Clauses shall be provided by Recurly to Merchant only upon Merchant's request.

3. Authorized Employees

3.1 Recurly shall ensure that all Authorized Employees have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality in relation to any Personal Data.

3.2 Recurly shall take commercially reasonable steps to limit access to Personal Data to only Authorized Employees.

4. Authorized Sub-Processors

4.1 Merchant acknowledges and agrees that Recurly may, as specified in **Annex B**, (1) engage its affiliates and the Authorized Sub-Processors listed at https://recurly.com/legal/privacy/subprocessors to access and Process Personal Data in connection with the Services and (2) from time to time engage additional third parties for the purpose of providing the Services, including without limitation the Processing of Personal Data. By way of this Addendum, Merchant provides general written authorization to Recurly to engage sub-processors as necessary to perform the Services.

4.2 A list of Recurly's current Authorized Sub-Processors (the "List") is available at https://recurly.com/legal/privacy/subprocessors. Such List may be updated by Recurly from time to time. Merchant acknowledges and agrees that it is solely responsible for subscribing to notifications of changes, which notification mechanism will be available through the List, in order to be notified of new Authorized Sub-Processors. Merchant also acknowledges and that, aside from updating the List and informing Merchant that the List has been updated, Recurly shall have no obligation to inform Merchant of any additional Authorized Sub-Processors. If the parties have entered into the Standard Contractual Clauses, the notification requirements set out in Clause 9 will control. Merchant acknowledges that certain sub-processors are essential to providing the Services and that objecting to the use of a sub-processor may prevent Recurly from offering the Services to Merchant.

4.3 If Merchant reasonably objects to an engagement in accordance with Section 4.2, and Recurly cannot provide a commercially reasonable alternative within a reasonable period of time, Recurly may terminate the Agreement or this Addendum. Termination shall not relieve Merchant of any fees owed to Recurly under the Agreement.

4.4 If Merchant does not object to the engagement of a third party in accordance with Section 4.2, that third party will be deemed an Authorized Sub-Processor for the purposes of this Addendum.

4.5 Recurly will enter into a written agreement with the Authorized Sub-Processor imposing the same data protection obligations on the Authorized Sub-Processor as those imposed on Recurly under this Addendum and by applicable Data Protection Laws with respect to the protection of Personal Data.

(i)The above authorizations will constitute Merchant's prior written consent to the subcontracting by Recurly of the processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the parties agree that the copies of the agreements with Authorized Sub-Processors that must be provided by Recurly to Merchant pursuant to Clause 9(c) of the Standard Contractual Clauses may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, and that such copies will be provided by Recurly only upon request by Merchant.

5. Security of Personal Data

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Recurly has implemented and will maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of Processing Personal Data ("Security Measures"). The Security Measures applicable to the Recurly Services are set forth in **Annex A**, as updated or replaced from time to time in accordance with Section 5.2.

5.2 Merchant is responsible for reviewing the information made available by Recurly relating to data security and making an independent determination as to whether the Recurly Services meet Merchant's requirements and legal obligations under Data Protection Laws. Merchant acknowledges that the Security Measures are subject to technical progress and development and that Recurly may update or modify the Security Measures from time to time.

5.3 Notwithstanding the above, Merchant agrees that except as provided by this Addendum, Merchant is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Personal Data when in transit to and from the Recurly Services and taking any appropriate steps to securely encrypt or backup any Personal Data uploaded to the Recurly Services.

6. Transfers of Personal Data

6.1 Merchant acknowledges and agrees that Recurly will process Personal Data in the United States as necessary to provide the Services. Recurly may also transfer and process Personal Data anywhere in the world where Recurly, its Affiliates or its Sub-processors maintain data processing operations.

6.2 To the extent any Personal Data originates from the European Economic Area ("EEA"), the United Kingdom or Switzerland, Recurly will take measures to confirm that appropriate safeguards have been implemented for the transfer of such Personal Data to a jurisdiction that the European Commission has not determined provides an adequate level of protection for Personal Data in accordance with Data Protection Laws.

6.3 Where required, any transfer of Personal Data made subject to this Addendum to any countries which do not ensure an adequate level of data protection shall be undertaken by Recurly pursuant to the Standard Contractual Clauses. The parties acknowledge that Recurly shall be deemed to provide adequate protection (within the meaning of applicable Data Protection Law) for any such Personal Data by complying with the Standard Contractual Clauses attached hereto at **Annex C**. Recurly agrees that it is a "data importer" and the Company is the "data exporter" under the Standard Contractual Clauses.

7. Rights of Data Subjects

7.1 Recurly shall, to the extent permitted by law, notify Merchant upon receipt of a request by a Data Subject to exercise the Data Subject's privacy rights ("Data Subject Request(s)"). If Recurly receives a Data Subject Request in relation to Personal Data, Recurly will advise the Data Subject to submit their request to Merchant and Merchant will be responsible for responding to such request, including, where necessary, by using the functionality of the Services.

7.2 Recurly shall, at the request of the Merchant, and taking into account the nature of the Processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Merchant in complying with Merchant's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, *provided that* (i) Merchant is itself unable to respond without Recurly's assistance and (ii) Recurly is able to do so in accordance with all applicable laws, rules, and regulations. Merchant shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Recurly.

8. Actions and Access Requests

8.1 Recurly shall, taking into account the nature of the Processing and the information available to Recurly, provide Merchant with reasonable cooperation and assistance where necessary for Merchant to comply with its obligations under the GDPR (or equivalent provision of other applicable Data Protection Laws) to conduct a data protection impact assessment and/or to demonstrate such compliance, *provided that* Merchant does not otherwise have access to the relevant information. Merchant shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Recurly.

8.2 Recurly shall, taking into account the nature of the Processing and the information available to Recurly, provide Merchant with reasonable cooperation and assistance with respect to Merchant's cooperation and/or prior consultation with any Supervisory Authority, where necessary and where required by the Data Protection Laws. Merchant shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Recurly.

8.3 Recurly shall maintain records sufficient to demonstrate its compliance with its obligations under this Addendum. Upon Merchant's request, Recurly shall, no more than once per calendar year and provided the parties have an applicable non-disclosure agreement in place, make available for Merchant's review copies of certifications or reports demonstrating Recurly's compliance with prevailing data security standards applicable to the Processing of Merchant's Personal Data. If Merchant and Recurly have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the audits described in Clause 8.9 and Clause 13(b) of the Standard Contractual Clauses shall be carried out in accordance with this Section 8.3.

8.4 Recurly shall immediately notify Merchant if an Instruction, in Recurly's opinion, infringes the Data Protection Laws.

8.5 In the event of a Personal Data Breach, Recurly will inform Merchant of the Personal Data Breach and will provide information relating to the Personal Data Breach as it becomes known or as is reasonably requested by Merchant. Recurly will also take such steps as Recurly in its sole discretion deems necessary and reasonable to remediate such incident (to the extent that remediation is within Recurly's reasonable control).

8.6 In the event of a Personal Data Breach, Recurly shall, taking into account the nature of the Processing and the information available to Recurly, provide Merchant with reasonable cooperation and assistance necessary for Merchant to comply with its obligations under the Data Protection Laws with respect to notifying (i) the relevant Supervisory Authority and (ii) Data Subjects affected by such Personal

Data Breach without undue delay.

8.7 The obligations described in Sections 8.5 and 8.6 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Merchant. Recurly's obligation to report or respond to a Personal Data Breach under Sections 8.5 and 8.6 will not be construed as an acknowledgement by Recurly of any fault or liability with respect to the Personal Data Breach.

8.8 If a law enforcement agency or supervisory authority sends Recurly a demand for Personal Data (for example, through a subpoena or court order), Recurly will attempt, as permitted by applicable law, to redirect the law enforcement agency or supervisory authority to request that data directly from Merchant . As part of this effort, Recurly may provide Merchant's basic contact information to the law enforcement agency or supervisory authority. Recurly shall make commercially reasonable challenges to requests for Personal Data from law enforcement agencies by (i) demanding that all such requestors provide proof of a request's legal authorization and validity, and (ii) responding only to requests that are legally binding. If compelled to disclose Personal Data to a law enforcement agency or supervisory authority, then Recurly will use commercially reasonable efforts to give Merchant reasonable notice of the demand to allow Merchant to seek a protective order or other appropriate remedy unless Recurly is legally prohibited from doing so. Recurly's legal department may make a record of all such supervisory authority and law enforcement requests.

9. Limitation of Liability. The total liability of each of Merchant and Recurly (and their respective employees, directors, officers, affiliates, successors, and assigns), arising out of or related to this Addendum, whether in contract, tort, or other theory of liability, shall not, when taken together in the aggregate, exceed the limitation of liability set forth in the Agreement. Merchant further agrees that any regulatory penalties incurred by Recurly in relation to the Personal Data that arise as a result of, or in connection with, Merchant's failure to comply with its obligations under this Addendum or any applicable Data Protection Laws shall be subject to Merchant's indemnification obligations under the Agreement.

10. General

10.1 Any claims against Recurly or its Affiliates under this Addendum shall be brought solely against the entity that is a party to the Agreement. In no event shall any party limit its liability with respect to any individual's data protection rights under this Addendum or otherwise.

10.2 No one other than a party to this Addendum, their successors and permitted assignees shall have any right to enforce any of its terms.

10.3 This Addendum 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. For Merchants located in the EEA, the governing law and jurisdiction provisions set out in Clause 18 of the Standard Contractual Clauses will control.

10.4 This Addendum may be executed simultaneously in any number of counterparts, each of which may be deemed an original but all of which together constitute one and the same agreement. The parties may execute and deliver signatures to this Addendum electronically, including by facsimile or portable document format file (PDF).

10.5 The provisions of this Addendum are severable. If any phrase, clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision, and the rest of this Addendum shall remain in full force and effect.

10.6 This Addendum is intended for use with Merchants located both within and outside of the EEA. As such, for clarification, the following sections apply only in the event that the Merchant is located within the EEA, unless otherwise specified: 2.5, 3.1, 4.2-4.5, 5.1, 6.2, 6.3, 8.1-8.4, 8.6 and 8.8.

11. Execution of this Addendum. Recurly has pre-signed this Addendum. To complete this Addendum, Merchant must: (i) complete the information requested in the signature block below and add the signatures there and (ii) send the completed and signed Addendum to Recurly by email to legal@recurly.com. Upon receipt of the validly completed Addendum by Recurly at this email address, this Addendum will become legally binding.

Merchant

Signature:

Merchant Legal Name:

Print Name:

Title:

Recurly, Inc.

Signature:

Print Name: James R Palmer

Title: Head of Information Security, DPO

Date: September 23, 2021

Date:

Annex A – Technical and organisational security measures implemented by Recurly:

Organisational safeguards:

- Recurly has a full-time team dedicated to our security, compliance, and privacy program. Recurly's security program is based on NIST 800-53 and we annually review our security program along with our policies and standards. Recurly has appointed one or more officers responsible for coordinating and monitoring the information technology rules and procedures.
- Recurly maintains SOC 1, SOC 2 Type II, and PCI DSS Level 1 certifications to demonstrate our security posture and commitment to security. These are audited annually by an external third-party.

Data security:

- Recurly maintains and enforces various policies, standards, processes, and controls to secure data, based on the NIST 800-53 framework.
- Access is limited to data, and in some cases, such as credit card numbers, no employee has routine access.
- Recurly has data security controls in place to do the following:
    - Prevent unauthorized persons from gaining access to data processing systems (physical access control).
    - Prevent data processing systems from being used without authorization (logical access control).
    - Ensure that persons entitled to use data processing systems gain access only to such data as they are entitled to access in accordance with their access rights (data access control).
    - Ensure that data cannot be read, copied, modified, or deleted without authorization during electronic transmission, transport or storage and that the target entities for any transfer of data by means of data transmission facilities can be established and verified (data transfer control).
    - Ensure the establishment of an audit trail to document whether and by whom data has been entered into, modified in or removed from processing (entry control).
    - Ensure that data is processed solely in accordance with the Instructions of the Data Controller (control of instructions).
    - Ensure that data is protected against accidental destruction or loss (availability control).
    - Ensure that data collected for different purposes can be processed separately (separation control).
- Recurly conducts annual risk assessments to review and revise its information security practices and whenever there is a material change in Recurly's business practices.

Physical security:

- Recurly maintains commercially reasonable security at all of our facilities, including badged access and cameras. Note that we do not store Merchant data in any of our facilities, including backups. Recurly reasonably restricts access to such Personal Data appropriately.

Security controls:
Recurly's security program consists of many security policies, procedures, and controls. The following list highlights many of them:

- Application Security. Recurly utilizes a Secure Development Lifecycle based on the OWASP Software Assurance Maturity Model (SAMM). (Formerly known as OpenSAMM)
- Bug Bounty Program. Recurly offers a bug bounty program to aid in the detection and remediation of application vulnerabilities.
- Vendor Security. Recurly reviews and approves all vendors and sub-contractors that handle Personal Data to ensure they have appropriate security controls and reviews them periodically to ensure ongoing compliance.
- Media Destruction. When media are to be disposed of or reused, procedures have been implemented to prevent any subsequent retrieval of any Personal Data stored on them before they are withdrawn from the inventory. When media are to leave the premises at which the files are located as a result of maintenance operations, procedures have been implemented to prevent undue retrieval of Personal Data stored on them.
- Risk Rated Assets. Recurly has security policies and procedures to classify sensitive information assets, clarify

security responsibilities and promote awareness for employees.

- Incident Response. All Security Incidents are managed in accordance with appropriate incident response procedures.
- Network Security. Recurly maintains network security using commercially available equipment and industry standard techniques, including firewalls, intrusion detection and/or prevention systems, access control lists and routing protocols.
- Access Control. Recurly will maintain appropriate access controls, including, but not limited to, restricting access to Personal Data to the minimum number of Recurly personnel who require such access.
- Least Privilege. Access rights are implemented adhering to the “least privilege” approach. Only authorized staff can grant, modify or revoke access to an information system that uses or houses Personal Data.
- User Roles. User administration procedures define user roles and their privileges, and how access is granted, changed and terminated; address appropriate segregation of duties and define the logging/monitoring requirements and mechanisms.
- Unique Logins. All employees of Recurly are assigned unique User-IDs.
- Secure Passwords. Recurly implements commercially reasonable physical and electronic security to create and protect passwords.
- Encryption. Recurly encrypts, using industry-standard encryption tools, all Personal Data in transit and at rest. Recurly safeguards the security and confidentiality of all encryption keys associated with encrypted Sensitive Information / Personal Data.
- Virus and Malware Controls. Recurly utilizes anti-virus and malware protection software to protect Sensitive Data from anticipated threats or hazards and protect against unauthorized access to or use of Personal Data.
- Training. Recurly requires personnel to comply with its Information Security Program prior to providing personnel with access to Personal Data. Recurly implements a security awareness program to train personnel about their security obligations. This program includes training about data classification obligations; physical security controls; security practices and security incident reporting.
- Business Continuity. Recurly implements appropriate disaster recovery and business continuity plans. Recurly regularly reviews and updates its business continuity plan to ensure it is current and effective.

Annex B – List of Recurly Sub-processors

Recurly uses its Affiliates and a range of third party Sub-processors to assist it in providing the Recurly Services (as described in the Agreement). These Sub-processors are set out at the following link: https://recurly.com/legal/privacy/subprocessors.

Annex C – Standard Contractual Clauses

Commission Decision (EU) 2021/914
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)[1] for the transfer of personal data to a third country.

(b) The Parties:

  (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

  (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in 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.

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

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

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

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

SECTION II - OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

(a) The data 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 its 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[2] (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,

---

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

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 ten (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.[3] 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 authorised 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

---

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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) 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.

(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

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

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

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(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

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

15.1 Notification

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

---

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

(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 one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

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 Netherlands.

(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.

APPENDIX

Annex I:

A. LIST OF PARTIES

Data exporter(s): *Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*
Name:
Address:
Contact person's name, position and contact details:
Activities relevant to the data transferred under these Clauses: ...
Authorised Signature ……………………
Name: ……………………
Title: ……………………
Date: ……………………
Role (controller/processor): controller

Data importer(s): *Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*
Name: Recurly Inc., a Delaware Corporation, USA
Address: 400 Alabama St., Suite 202, San Francisco, CA 94110, USA
Contact person's name, position and contact details: James R. Palmer, Vice President, Information Security
Activities relevant to the data transferred under these Clauses: Recurly provides recurring billing and payments management and such other services.
Name: James R. Palmer
Title: Head of Information Security, DPO
Date: September 23, 2021
Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
Merchant's employees, customers, and authorized users in connection with the Services.

Categories of personal data transferred
Identification and contact data (name, address, title, company name, VAT number, contact details, including phone number, address and email address); account details (username; account code (can include email addresses), notes on an account, invoice or transaction, account number last four); financial information (payment card details, account details, payment information); employment details (employer, job title, geographic location, area of responsibility); personal interests or preferences (including marketing preferences); IT information (IP addresses, usage data, cookies data, location data).

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.
Not applicable.

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

Nature of the processing
Recurly provides recurring billing and payments management and such other services, as described in the Agreement.

Purpose(s) of the data transfer and further processing
Recurly provides recurring billing and payments management and such other services, as described in the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
Only so long as Recurly has an ongoing legitimate business need to process the personal data (for example, to provide the Services requested or to comply with an applicable legal requirement).

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

EU:
Dutch Data Protection Authority Autoriteit Persoonsgegevens
PO Box 93374
2509 AJ DEN HAAG
https://autoriteitpersoonsgegevens.nl/en

UK:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone: 0303 123 1113
Fax: 01625 524510
https://ico.org.uk/global/contact-us/

Annex II:

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

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Those listed in **Annex A** above.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.