DATA PROCESSING ADDENDUM

This Data Processing Addendum (**"DPA"**) forms part of the Master Services Agreement or other written or electronic agreement (the "**Agreement**") between SevenRooms and Client for the purchase of Services from SevenRooms and reflects the parties' agreement with regard to the Processing of Client Personal Data.

By signing the Agreement, Client enters into this DPA on behalf of itself and, to the extent required under Data Privacy Law, in the name and on behalf of its Affiliates, if and to the extent SevenRooms Processes Personal Data for which such Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Client" shall include Client and its Affiliates. All capitalized terms used but not defined herein shall have the meanings ascribed to such terms in the Agreement.

In the course of providing the Services to Client pursuant to the Agreement, SevenRooms will Process Client Personal Data, and the Parties agree to comply with the following provisions with respect to Processing of Client Personal Data, each acting reasonably and in good faith. For the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Schedules.

1. DEFINITIONS

"Affiliate" means with respect to a party an entity that (i) controls, (ii) is controlled by, or (iii) is under common control with such party. An entity will be deemed to control another entity if it has the power to direct or cause direction of the management or policies of such entity, whether through the ownership or voting securities, by contract, or otherwise.

"**Client Personal Data**" means all Personal Data Processed by SevenRooms or its Sub-processors on behalf of Client or its Affiliates pursuant to or in connection with the Agreement. For the avoidance of doubt, information that has been anonymized (as defined in the GDPR) or deidentified (as defined in the CCPA) shall not be Client Personal Data hereunder.

"**CCPA**" means the California Consumer Privacy Act of 2018.

"Data Privacy Law" means, as applicable, EU Data Protection Laws, the CCPA and all other applicable laws, rules and regulations relating to the Processing of Personal Data and data privacy or data protection that may exist in any relevant jurisdiction.

"**EU Data Protection Laws**" means (i) EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR; (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; (iii) in respect of the United Kingdom, any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the United Kingdom leaving the European Union ("**UK GDPR**") (with references to specific GDPR provisions in this DPA understood to refer to substantially equivalent provisions, if any, in the UK GDPR); and (iv) the Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance; in each case, as may be amended, superseded or replaced.

"**European Data**" means Client Personal Data that is subject to the protection of EU Data Protection Laws.

"**GDPR**" means the EU General Data Protection Regulation 2016/679.

"Services" means the Services (as defined in the Agreement) and access to and use of the Platform and any other services provided by SevenRooms pursuant to the Agreement, including pursuant to any related Order Form (as defined therein).

"Sub-processor" means any person (including any third party and any Affiliate of SevenRooms, but excluding an employee of SevenRooms or any of its Sub-processors) appointed by or on behalf of SevenRooms or any of its Affiliates to Process Client Personal Data.

The terms, **"Commission"**, **"Controller"**, **"Data Subject"**, **"Data Protection Impact Assessment"**, **"Member State"**, **"Personal Data"**, **"Personal Data Breach"**, **"Processing", "Processor"**, and

"Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. PROCESSING OF PERSONAL DATA

2.1 Details of the Processing. The parties acknowledge and agree that with regard to the Processing of Client Personal Data, Client is the Controller, SevenRooms is the Processor and that SevenRooms or its Affiliates engaged in the Processing of Client Personal Data will engage Sub-processors to Process Client Personal Data on their, and ultimately the Controller's, behalf subject to the requirements set forth in Section 5 "Sub-processors" below. The subject matter, duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 (Details of the Processing) to this DPA.

2.2 Client's Processing of Personal Data. Client shall in its use of the Services Process Personal Data, including through its engagement of SevenRooms as Processor, in accordance with the requirements of Data Privacy Law. For the avoidance of doubt, Client's instructions for the Processing of Client Personal Data shall comply with Data Privacy Law. This DPA and the Agreement are, at the time of signature of the Agreement, Client's complete and final documented instructions to SevenRooms for the Processing of Client Personal Data, and Client's configuration of the Services shall constitute an additional documented instruction to SevenRooms. The parties agree that a Client instruction shall be deemed to have been given by Client to SevenRooms for any act or omission of SevenRooms within the framework of the Agreement and any Order Form or this DPA, including any anonymization or deidentification of Client Personal Data as a consequence of which such data is no longer Client Personal Data. Any additional or alternate instructions must be agreed upon and documented separately. Client shall have sole responsibility for the accuracy and quality of Client Personal Data, and the legality of (a) the content of such Client Personal Data, (b) the means by which Client acquired such Client Personal Data and (c) the Processing of such Client Personal Data.

2.3 SevenRooms's Processing of Client Personal Data. SevenRooms shall treat Client Personal Data as Confidential Information and, subject to the last two sentences of this paragraph, shall only Process Client Personal Data on behalf of Client and in accordance with Client's documented instructions, including with regard to transfers of Client Personal Data to a third country or an international organization, for the following purposes: (i) Processing in accordance with the Agreement and any applicable Order Form(s) thereunder; (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Client (e.g., via email) where such instructions are consistent with the terms of the Agreement. SevenRooms will Process Client Personal Data in compliance with Data Privacy Law, provided however that SevenRooms shall not be in violation of this contractual obligation in the event that SevenRooms's Processing of Client Personal Data in breach of Data Privacy Law is attributable to the documented instructions of Client or is otherwise due to acts or omissions of Client; provided further, that SevenRooms shall inform Client if in SevenRooms's opinion any instruction given by the Client violates or is otherwise non-compliant with Data Privacy Law. SevenRooms's obligation to Process Client Personal Data only on the instructions of Client in accordance with this Section 2.3 shall be subject to an exception for any Processing by SevenRooms in contravention of, or additional to, such instructions that is required by Data Privacy Law. Where SevenRooms is compelled by Data Privacy Law to Process Client Personal Data, SevenRooms shall promptly notify Client before performing the Processing so compelled unless Data Privacy Law prohibits SevenRooms from so notifying Client.

2.4 General. Taking into account the nature of the Processing of Client Personal Data and information available to SevenRooms, subject to the specific provisions of this DPA, SevenRooms shall assist Client in its efforts to comply with its obligations under Data Privacy Law, including obligations relating to responding to Data Subject Requests, and in ensuring compliance with its obligations with respect to records of processing, security of Processing, notifications of Personal Data Breaches to Data Subjects and Supervisory Authorities, Data Protection Impact Assessments, and consultations with Supervisory Authorities. SevenRooms shall make available to the Client all information, to the extent SevenRooms is in possession of such information, necessary for Client, as Controller, to meet its obligations under Data Privacy Law, and allow for and contribute to audits, including inspections, conducted by the Client or another auditor mandated by the Client in all cases subject to and in the manner provided for in Section 6 hereof and in compliance with Clause 8..9 of the Standard Contractual Clauses (defined below).

2.5 Use of Data by SevenRooms. For avoidance of doubt, with respect to Client Personal Data that has been deidentified, anonymized, pseudonymized, masked and/or aggregated (referred to as "**Deidentified Data**", but for (i) Client Personal Data subject to EU Data Protection Laws, includes only Client Personal Data that has been anonymized in accordance with the EU Data Protection Laws and for (ii) Client Personal

Data subject to the CCPA, includes only Client Personal Data that has been deidentified in accordance with the CCPA), as well as data which is created, generated, organized, formatted, derived, trained, ensembled, or based from or on Deidentified Data, SevenRooms has the right to use such Deidentified Data in any manner consistent with Data Privacy Law including the right to (a) use all of the foregoing for its own internal business purposes, (b) modify the Deidentified Data, (c) aggregate or combine the Deidentified Data with other data, (d) disclose Deidentified Data to third parties, (e) use the Deidentified Data in demonstrations of products and services to third parties, and (f) license, assign, convey and/or transfer ownership of Deidentified Data and any or all of SevenRooms's rights thereto to third parties.

3. SEVENROOMS PERSONNEL

3.1 Confidentiality. SevenRooms shall ensure that its personnel engaged in the Processing of Client Personal Data are informed of the confidential nature of the Client Personal Data, have received appropriate training on their responsibilities and have either executed written confidentiality agreements committing them to holding the Client Personal Data in confidence or are under an appropriate statutory obligation of confidentiality. SevenRooms shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

3.2 Reliability. SevenRooms shall take commercially reasonable steps to ensure the reliability of any SevenRooms personnel engaged in the Processing of, or that has access to, Client Personal Data.

3.3 Limitation of Access. SevenRooms shall ensure that its employees' access to Client Personal Data is strictly limited to those personnel requiring such access to perform the Services in accordance with the Agreement.

4. DATA SUBJECT REQUESTS

4.1 Data Subject Requests. Taking into account the nature of the Processing, SevenRooms shall assist Client by providing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Client's obligation to respond to requests from Data Subjects to exercise their rights under applicable Data Privacy Law ("**Data Subject Requests**").

4.2 Client Controls. The Services provide Client with a number of controls that Client may use to retrieve, correct, delete or restrict Client Personal Data which Client may use to assist it in connection with its obligations under Data Privacy Law, including its obligations relating to responding to Data Subject Requests. To the extent that Client is unable to independently address a Data Subject Request through the Services, then upon Client's written request SevenRooms shall provide reasonable assistance to Client to respond to any Data Subject Requests.

4.3 Data Subject Requests to SevenRooms. If a Data Subject Request is made directly to SevenRooms, it shall, to the extent legally permitted and to the extent SevenRooms is able to identify that the request comes from a Data Subject whose Personal Data was submitted to the Services by or on behalf of Client, promptly notify Client. SevenRooms shall not respond to a Data Subject Request without Client's prior written instruction to do so except (a) to confirm that such request relates to Client, to which Client hereby agrees and (b) as required by law applicable to SevenRooms, in which case SevenRooms shall to the extent permitted by applicable law inform Client of that legal requirement before SevenRooms responds to the request. Client shall be solely responsible for responding substantively to any such Data Subject Requests or communications involving Client Personal Data.

5. SUB-PROCESSORS

5.1 Use of Sub-processors. Client acknowledges and agrees that (a) SevenRooms's Affiliates may be retained as Sub-processors; and (b) SevenRooms and SevenRooms's Affiliates, respectively, may engage third-party Sub-processors for the provision of the Services and related Processing of Client Personal Data. Where SevenRooms engages any Sub-processor as described in this Section 5:

(i) SevenRooms will restrict the Sub-processor's access to Client Personal Data only to what is necessary to maintain the Services or to provide the Services to Client and its Users in accordance with the Documentation and SevenRooms will prohibit the Sub-processor from accessing Client Personal Data for any other purpose;

(ii) SevenRooms will enter into a written agreement with the Sub-processor and, to the extent that the Sub-processor is performing the same Processing services that are being provided by SevenRooms under this

DPA, SevenRooms will impose on the Sub-processor the same contractual obligations that SevenRooms has under this DPA; and

(iii) SevenRooms will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processors that cause SevenRooms to breach any of SevenRooms's obligations under this DPA.

5.2 List of Current Sub-processors and Notification of New Sub-processors. A list of Sub-processors is available at https://www.sevenrooms.com/en/subprocessors/ as well as a mechanism that Client hereby agrees to subscribe to in order to receive notifications of new Sub-processors. Such Sub-processor list includes the identities of such Sub-processors, their country of location as well as the type of processing they perform. Client may object to SevenRooms's use of a new Sub-processor by notifying SevenRooms in writing within ten (10) business days after receipt of a notification in accordance with the mechanism set out in the preceding sentence. SevenRooms shall work with Client in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Sub-processor; and where such a change cannot be made within thirty (30) calendar days from receipt by SevenRooms of Client's notice, notwithstanding anything in the Agreement, Client may by written notice to SevenRooms with immediate effect terminate those Services which require the use of the proposed Sub-processor objected to by Client.

6. SECURITY

6.1 Controls for the Protection of Client Personal Data. 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, SevenRooms shall maintain appropriate technical and organizational measures for protection of the security (including protection against Personal Data Breach), confidentiality and integrity of Client Personal Data, including (without limitation) those measures set out in Article 32 of the GDPR, and as described in Schedule 2 to this DPA ("**Security Measures**"). Notwithstanding any provision to the contrary, SevenRooms may modify or update the Security Measures at its discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures, and provided those Security Measures comply with Data Privacy Law. SevenRooms regularly monitors compliance with such measures. In assessing the appropriate level of security, SevenRooms shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach. Client is responsible for reviewing the information made available by SevenRooms relating to data security and making an independent determination as to whether the Services meet Client's requirements and legal obligations under Data Privacy Law.

6.2 Third Party Certifications. Upon Client's written request at reasonable intervals (as provided below), and subject to the confidentiality obligations set forth in the Agreement, SevenRooms shall allow for and contribute to audits and inspections ("**Audits**") conducted by Client (or Client's independent, third-party auditor that is not a competitor of SevenRooms and that is subject to confidentiality obligations at least as restrictive as those set forth in the Agreement) by providing any information reasonably necessary to demonstrate SevenRooms's compliance with the obligations set forth in this DPA in the form of a copy of SevenRooms's then most recent third-party audits or certifications, as applicable, that SevenRooms makes available to its clients generally.

6.3 Right to Audit. SevenRooms shall maintain complete and accurate records and information to demonstrate its compliance with this DPA, and Client (or its permitted third-party auditor as provided above) may perform an Audit remotely or on-site, up to one (1) time per year, with at least three (3) weeks' advance written notice, unless otherwise required by Client's regulators or applicable law. If Client requests an on-site Audit, the following terms shall apply: (a) such Audit shall be limited to facilities operated by SevenRooms and shall not exceed one (1) business day; (b) before the commencement of any such on-site Audit, Client and SevenRooms shall mutually agree upon the scope and timing of, and procedures relating to, the Audit with a view towards minimizing the disruption of SevenRooms's business; (c) Client shall reimburse SevenRooms for actual expenses and costs incurred in connection with such Audit; and (d) Client shall promptly notify SevenRooms with reasonably detailed information regarding any non-compliance discovered during the course of an Audit.

6.4 Audits Pursuant to Standard Contractual Clauses. The parties agree that the audits described in Clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with the foregoing Section 6.2 and 6.3.

6.5 Personal Data Breaches. SevenRooms will notify Client without undue delay after it becomes aware of any Personal Data Breach and shall provide timely information relating to the Personal Data Breach as it

becomes known or reasonably requested by Client. At Client's request, SevenRooms will promptly provide Client with such reasonable assistance as necessary to enable Client to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if and to the extent Client is required to do so under Data Privacy Law.

7. DATA TRANSFERS

7.1 Transfers Generally. Client acknowledges and agrees that SevenRooms may access and Process Client Personal Data on a global basis as necessary to provide the Services in accordance with the Agreement, and in particular that Client Personal Data will be transferred to and Processed by SevenRooms in the United States and to other jurisdictions where SevenRooms Affiliates and Sub-processors have operations. SevenRooms shall ensure such transfers are made in compliance with the requirements of Data Privacy Law.

7.2 Transfer Mechanisms for European Data. SevenRooms shall not transfer European Data to any country or recipient not recognized as providing an adequate level of protection for Personal Data (within the meaning of EU Data Protection Laws) unless it first takes all such measures as are necessary to ensure the transfer is in compliance with applicable EU Data Protection Laws. Such measures may include (without limitation) transferring such data to a recipient that has achieved binding corporate rules authorization in accordance with EU Data Protection Laws, to a recipient that has executed appropriate standard contractual clauses adopted or approved by the European Commission or transferring data in accordance with certain derogations under the GDPR.

7.3 Transfer of Client Personal Data to SevenRooms. Client acknowledges that in connection with the performance of the Services, SevenRooms may be a recipient of European Data in the United States. The parties agree that SevenRooms agrees to abide by and process European Data in compliance with the Standard Contractual Clauses attached hereto as Schedule 3 and forming part of this DPA pursuant to the 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, or any set of clauses approved by the European Commission or a Supervisory Authority which subsequently amends, replaces or supersedes the same (the "**Standard Contractual Clauses**"). If and to the extent the Standard Contractual Clauses (where applicable) conflict with any provision of this DPA, the Standard Contractual Clauses shall prevail to the extent of such conflict.

8. LIMITATIONS OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement including this DPA.

9. TERMINATION

The term of this DPA will end simultaneously and automatically at the later of (i) the date of expiration or termination of the Agreement and (ii) the first date when all Client Personal Data is deleted from SevenRooms's systems. After the termination of this DPA, SevenRooms will delete or return all Client Personal Data (including copies thereof) promptly upon its receipt of written notice from Client specifying whether it chooses for such Client Personal Data to be deleted or returned, save that this requirement shall not apply to the extent SevenRooms is required by applicable law to retain some or all of the Client Personal Data.

10. CALIFORNIA CONSUMER PRIVACY ACT OF 2018

The following applies to any Personal Information (as defined under the CCPA) Processed on behalf of Client:

10.1. All references to Data Privacy Law in this DPA shall be deemed to include a reference to the CCPA;

10.2 All references to Personal Data in this DPA shall be deemed to include Personal Information, as defined in the CCPA;

10.3 All references to "Controller" in this DPA shall be deemed to be references also to "Business," as defined in the CCPA;

10.4 All references to "Processor" in this DPA shall be deemed to be references also to "Service Provider," as defined in the CCPA;

10.5 Any capitalized term used in this Section 10 but not defined herein, shall have the meaning set forth in the CCPA.

10.6 SevenRooms shall not Sell any Personal Information.

10.7 SevenRooms will Process Personal Information solely to the extent required to perform the Services as set forth in Section 2 (the "**Business Purpose**"), and shall not further collect, retain, use, or disclose the Personal Information for any purpose (including a commercial purpose) other than the Business Purpose.

10.8 SevenRooms does not receive any Personal Information from Client as consideration for SevenRooms's provision of the Services.

10.9 SevenRooms certifies that it understands the restrictions set forth in this DPA, and in particular this Section 10, and will comply with them.

11. GENERAL

a. This DPA may only be amended with the written consent of both parties.

b. For the purposes of this DPA the contact information of each party are set forth the below but may be updated by either party upon written notice to the other:

For SevenRooms:	For Client:
privacy@sevenrooms.com	See Order Form.

c. This DPA represents the entire understanding of the parties relating to the Agreement arising out of the Processing of Personal Data and their relationship under Data Privacy Law.

d. The parties to this DPA hereby submit to the choice of law and jurisdiction stipulated in the Agreement with respect to any disputes or claims that arise under this DPA, subject to the Standard Contractual Clauses.

SCHEDULE 1

PERSONAL DATA PROCESSING DETAILS

INFORMATION REGARDING SEVENROOMS'S PROCESSING OF CLIENT PERSONAL DATA AS REQUIRED BY ARTICLE 28(3) OF THE GDPR (AND EQUIVALENT REQUIREMENTS OF OTHER DATA PROTECTION LAWS)

SUBJECT MATTER:	The subject matter of the Processing under this DPA is Client Personal Data.
DURATION OF PROCESSING:	As between SevenRooms and Client the duration of the Processing under this DPA is determined by Client; provided that, generally the duration of the Processing of Client Personal Data shall be for the duration of the Agreement and for the minimum period thereafter required to wind-down the parties' relationship under the Agreement and properly return or dispose of Client Personal Data.
NATURE OF THE PROCESSING:	Computing, storing and such other Services as described in the Agreement.

CATEGORIES OF DATA SUBJECTS, TYPES OF CLIENT PERSONAL DATA AND PURPOSE OF PROCESSING ORGANIZED BY SEVENROOMS SERVICE

SevenRooms Service	Categories of Data Subjects	Type of Client Personal Data	Purpose of the Processing
Concierge	Venue Guests Concierge Staff	First Name Last Name IP Address (of user) Email Address (optional) Phone Number (optional) Special Occasion (optional) Occupation (optional)	• Booking and fulfilling reservations as requested by the guest • User account definition, privilege level, and access to use the platform
Contactless Order and Pay	Venue Guests Venue Staff	First Name Last Name Email Job/Title (optional) IP Address (Activity logs)	• Capture Guest's order for Venue fulfilment • User account definition, privilege level, and access to use the platform
CRM	Venue Guests Venue Staff	First Name Last Name IP Address (of user) Email Address (optional) Phone Number (optional) Membership Number Dietary Restrictions (optional) Birthday (optional) Special Occasion (optional) Address (optional) Occupation (optional) Social ID (optional) Picture (optional) Free Form Data Entry	• Managing Client profile data (CRM) • Correcting information as requested by the guest, and capturing Guest preferences or special requests • Building a profile for Guests at the inception of our Clients' use of the platform
Guest Satisfaction	Venue Staff	First Name Last Name Email Job/Title (optional) IP Address (Activity logs)	• User account definition, privilege level, and access to use the platform.

Marketing Automation	Venue Staff	First Name Last Name Email Job/Title (optional) IP Address (Activity logs)	• User account definition, privilege level, and access to use the platform.
Online Ordering	Venue Guests Venue Staff	First Name Last Name Email Address (optional) Phone Number (optional) Address (optional)	• Capture Guest's order for Venue fulfilment
Reservations	Venue Guests Venue Staff	First Name Last Name Email Address Phone Number Membership Number IP Address (of API user) Dietary Restrictions (optional) Birthday (optional) Social ID (optional) Special Occasion (optional) Picture (optional) Server Full Name	• Booking and fulfilling reservations and requests as requested by the Guest • Transactional messaging • Confirming an in-advance booking • Guest may supply more details about their party or themselves for Venue accommodation • Building a profile for Guests at the inception of our Clients' use of the platform • Managing server rotations during Venue operation • Capturing POS server during Venue operation • User account definition, privilege level, and access to use the platform.
Table Management	Venue Guests Venue Staff	First Name Last Name IP Address (of user) Email Address (optional) Phone Number (optional) Dietary Restrictions (optional) Birthday (optional) Address (optional) Occupation (optional) Spend (optional) Server Full Name	• Booking and fulfilling reservations and requests as requested by the Guest • Transactional messaging • Confirming an in-advance booking • Guest may supply more details about their party or themselves for Venue accommodation • Building a profile for Guests at the inception of our Clients' use of the platform • Managing server rotations during Venue operation • Capturing POS server during Venue operation • User account definition, privilege level, and access to use the platform.
Waitlist	Venue Guests Venue Staff	First Name Last Name Email Address Phone Number IP Address (of guest) Dietary Restrictions (optional) Birthday (optional) Social ID (optional)	• Booking and fulfilling reservations and requests as requested by the Guest • Transactional messaging • User account definition, privilege level, and access to use the platform.

		Special Occasion (optional) Picture (optional)	
Support Requests (Email)	Venue Staff Concierge Staff	First Name Last Name Email	Venue/Concierge Staff emailing into Support@sevenrooms.com for assistance with the platform

SCHEDULE 2

Security Measures

SevenRooms is committed to the protection of Personal Data and employs industry standards of technological internet and web application security to prevent security incidents from occurring. SevenRooms also maintains organizational and physical policies and procedures to enforce these standards.

SevenRooms maintains organizational policies and standards in the following areas:

- Access Management and Entitlements (only provide access on a need to know basis and scope)
- Change Management (document and follow all changes to systems and process)
- Physical Security (maintain appropriate safeguards for physical locks, security cameras and sensors, check-in, scope/role-based access, and telecom security)
- Clear Desks / Clear Screens
- Password and MFA requirements for company systems
- Data decommissioning and Archival Policy (disposal and destruction of hardware, data, and software using US DoD standards)
- Information Security (training, awareness, encryption, anti-virus, risk assessments)
- Acceptable Use Policy for hardware and software
- Production system vulnerability threat assessments, penetration testing, configuration standards
- Data Backups
- Business Continuity and Disaster Recovery Process
- Software Development Process, environment isolation, and application security review (OWASP design principles)
- Secure Handling of Client Data
- Incident Response Process
- Employee Background Check and Termination Procedures
- General Code of Conduct (conflict of interest, employment practices, anti-bribery, etc.)
- Privacy Law adherence and GDPR awareness / readiness

SevenRooms technical infrastructure follows best practices for data protection and security:

- Cloud datacenter with strict physical safeguards, cameras, power redundancy, role-based access and keycards, and sensors
- Utilizing cloud infrastructure with SOC-1, SOC-2, SOC-3, ISO 27001, CSA Star, and other standards (see https://cloud.google.com/security/compliance/#/)
- We assess ourselves for CSA Star Criteria for cloud configuration
- PCI DSS 3.2+ Compliance
- Proper use of encryption in transit and at rest
- Network-level intrusion detection and monitoring with automated alerting
- OWASP design principles for secure application coding

- Effective use of firewalls and network isolation via Google Cloud
- Role-based access
- Multi-factor authentication for production system access
- Regular penetration testing and vulnerability scanning (black box / grey box testing)
- Other information security best practices

Technical and organisational measures by which assistance shall be provided by SevenRooms to Client in respect of Data Subject Requests

- SevenRooms provides Client with a number of controls that it may use to retrieve, correct, delete or restrict Client Personal Data
- SevenRooms will comply with the procedures set forth in Section 4 of the DPA with respect to Data Subject Requests
- Other measures that SevenRooms will employ to assist Client with Data Subject Requests

SCHEDULE 3

STANDARD CONTRACTUAL CLAUSES

(Module 2)

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 personal data to a third country.

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

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

(ii) Clause 8.1(b), 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 – Not included.

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.

MODULE TWO: Transfer controller to processor

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 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 theredacted 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. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with itsobligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and theaffected 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 restrictionsand/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

MODULE TWO: Transfer controller to processor

(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 leastten (10) business days in advance, thereby giving the data exporter sufficient time to be able to object to such changesprior 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. 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 confidentialinformation, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(c) 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.

(d) 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

MODULE TWO: Transfer controller to processor

(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.

MODULE TWO: Transfer controller to processor

(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

MODULE TWO: Transfer controller to processor

(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

MODULE TWO: Transfer controller to processor

(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 behaviour 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

MODULE TWO: Transfer controller to processor

(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

MODULE TWO: Transfer controller to processor

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 deletionof 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 underRegulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

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 Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(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 Ireland.

(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 TO STANDARD CONTRACTUAL CLAUSES

ANNEX I

A. **LIST OF PARTIES**

MODULE TWO: Transfer controller to processor

Data exporter(s):

1. Name: See Order Form and Agreement

Address: See Order Form and Agreement

Contact person's name, position and contact details: See Order Form and Agreement

Activities relevant to the data transferred under these Clauses: Data processing for the performance of the Agreement as described in Schedule 1 to the DPA.

Signature and date: See Order Form and Agreement

Role (controller/processor): Controller

2. ……

Data importer(s):

1. Name: SevenRooms, Inc., a Delaware corporation

Address: 228 Park Avenue South, PMB 33706, New York, New York 10003-1502, US

Contact person's name, position and contact details: Jessica Kramer, jessica.kramer@sevenrooms.com

Activities relevant to the data transferred under these Clauses: Data processing for the performance of the Agreement as described in Schedule 1 to the DPA.

Signature and date: See Order Form and Agreement

Role (controller/processor): Processor

2. ……

B. **DESCRIPTION OF TRANSFER**

MODULE TWO: Transfer controller to processor *Categories*

of data subjects whose personal data is transferred

Please see Schedule 1 of the DPA, which describes the data subjects.

Categories of personal data transferred

Please see Schedule 1 of the DPA, which describes the categories of 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.

The parties do not anticipate the transfer of special categories of data.

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

The transfers are on a continuous basis.

Nature of the processing

Please see Schedule 1 of the DPA, which describes the processing operations.

Purpose(s) of the data transfer and further processing

SevenRooms, Inc. shall process personal data as necessary to provide the Services to data exporter in accordance with 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

Please see Schedule 1 of the DPA, which describes the processing operations.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

With respect to any transfers to sub-processors, the subject matter, nature and duration of the processing shall be substantially the same as described on Schedule 1 of the DPA.

C. **COMPETENT SUPERVISORY AUTHORITY**

MODULE TWO: Transfer controller to processor

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

The Irish Supervisory Authority - The Data Protection Commission, unless the data exporter notifies the data importer of an alternative competent supervisory authority from time to time in accordance with Section 11 of the DPA.

ANNEX II

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

MODULE TWO: Transfer controller to processor

Please see Schedule 2 of the DPA, which describes the technical and organizational security measures implemented by SevenRooms.

ANNEX III

LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

Subject to Clause 9, paragraph (a) and Section 5 of the DPA, the data importer has the data exporter's general authorisation for the engagement of sub-processor(s).

The list of sub-processors is located here:

https://sevenrooms.com/en/subprocessors/

ANNEX IV

This Annex IV forms part of the Clauses.

This Annex IV sets out the parties' interpretation of their respective obligations under specific terms of the Clauses. Where a party complies with the interpretations set out in this Annex IV, that party shall be deemed by the other party to have complied with its commitments under the Clauses; provided that, in the event of any conflict between the Clauses and this Appendix IV, the Clauses shall control.

For the purposes of this Appendix, "DPA" means the Data Processing Agreement in place between Client and SevenRooms into which these Clauses are incorporated and "Agreement" shall have the meaning ascribed to such term in the DPA.

Clauses 8.1 and 8.2: Instructions; Purpose

a. The parties acknowledge that data importer may process the personal data only on behalf of the data exporter and in compliance with its instructions as provided by the data exporter and the Clauses. For the purposes of Clauses 8.1 and 8.2, the processing described in Section 2 of the DPA is deemed an instruction by data exporter to process personal data, subject to data importer's compliance with applicable Data Privacy Law.

Clause 8.3: Disclosure of these Clauses

a. Data exporter agrees that these Clauses constitute data importer's Confidential Information as that term is defined in the Agreement and may not be disclosed by data exporter to any third party without data importer's prior written consent unless permitted pursuant to Agreement or so required by applicable law. This shall not prevent disclosure of these Clauses to a data subject pursuant to Clause 8.3.

Clauses 8.5 and 16(d): Obligation after the termination of personal data-processing services

a. Data importer agrees that it will fulfil its obligation to return or destroy all the personal data on the termination of the provision of data-processing services by complying with Section 9 "Termination" of the DPA.

Clauses 8.9(d) and (c): Audit

a. Data exporter acknowledges and agrees that it exercises its audit right under Clauses 8.9(d) and (c) by instructing data importer to comply with the audit measures described in Sections 6.2, 6.3 and 6.4 of the DPA.

Clause 9: Sub-processing

a. Pursuant to Clause 9, data exporter agrees that data importer may continue to use those sub-processors already engaged by data importer as at the date of the DPA identified as set forth in Section 5 of the DPA, and otherwise in accordance with Section 5 of the DPA.

Clause 12: Liability

a. Any claims brought under the Clauses shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement; provided that, in no event shall any party limit its liability with respect to any data subject rights under these Clauses.