UNILY INTERNATIONAL DATA TRANSFER ADDENDUM
(SCC Addendum)

This International Data Transfer Addendum (“SCC Addendum”) with an effective date as of the 27th December 2022 ("Effective Date") is added to that certain agreements made by and between the Client entity that is a party to the Agreement and its Affiliates (“Licensee”, “Client”) and Unily Group and its Affiliates (“Unily”) to which Unily is processing personal data on Licensee’s behalf (collectively, the “Agreement(s)”). Licensee and Unily are together referred to as the “Parties.”

WHEREAS the Parties desire to add to the terms of the Agreement(s) as set out in this SCC Addendum. This SCC Addendum, including all attachments and annexes hereto, adds to the Agreement(s) as follows:

1. **Interpretation.** All capitalized terms that are not expressly defined in this SCC Addendum shall have the meanings assigned to them in the Agreement(s). In the event of any conflict between the SCC Addendum and the Agreement(s), the provisions of this SCC Addendum shall prevail.

2. **Standard Contractual Clauses ("SCCs").** The Parties agree that the Standard Contractual Clauses (Attachment 1) and shall apply to Unily and its respective Affiliates in its role as the “data importer(s),” and to Licensee and its Affiliates established within the European Union, the European Economic Area and/or its member states, Switzerland, in their role as “data exporters.”

3. **UK International Data Transfer Addendum ("UK IDTA").** The Parties agree that the UK International Data Transfer Addendum (Attachment 2) shall apply to Unily and its respective Affiliates in its role as the “data importer(s),” and to Licensee and its Affiliates established within the United Kingdom, in their role as “data exporters.”

4. In connection with the Agreement(s), Licensee and/or its European Affiliates, acting as data exporters, executed (or were required to have executed) with Unily and/or its Affiliates, acting as data importers, certain EU Standard Contractual Clauses to govern the transfer of personal data to processors established in third countries, dated 5 February 2010 (2010/87/EU) in accordance with European Directive 95/46/EC (the “2010 EU SCCs”).

5. In connection with the Agreement(s), Licensee and/or its United Kingdom Affiliates, acting as data exporters, are required to execute with Unily and/or its Affiliates, acting as data importers, the UK IDTA to govern the transfer of personal data to processors established in third countries, dated 1 January 2021.

6. As a result of the recent European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses and Information Commissioners Office (ICO) UK GDPR updates as of 1 January 2021 on the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, the UK GDPR - Data Protection Act 2018, and UK Data Protection Act of 2018 data protection laws applicable to the processing of Customer Personal Data under the agreement(s). The Parties now desire to modify the Agreements(s), any related EU
Standard Contractual Clauses, and UK IDTA provisions consistent with this Amendment.

7. Counterparts. This SCC Addendum may be executed electronically and in counterparts.

NOW and THEREFORE, the Parties agree as follows:

Any previously agreed to SCCs executed between the Parties and/or their respective Affiliates are hereby replaced with the updated Standard Contractual Clauses incorporated by reference, as appropriate: Module 2 of the standard contractual clauses as currently set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj and in Attachment 1 to this Amendment (“EU SCCs”), effective upon execution this Amendment.

The Agreement(s) is hereby amended by addition of the UK IDTA incorporated by reference, as appropriate: the UK IDTA to the EU SCCs as currently set out at https://ico.org.uk/media/for-organisations/documents/4019483/international-data-transfer-addendum.pdf (“UK SCCs”) and set out in Attachment 2 to this Addendum (“UK SCCs”), effective upon execution this Addendum.

The EU SCCs and UK SCCs will be considered part of the Agreement(s) and governed by the terms thereof, provided that in case of contradictions between the EU SCCs and UK SCCs and the terms of the Agreement(s), the terms of the EU SCCs and UK SCCs shall prevail.

All terms of the Agreement(s) not expressly modified by this SCC Addendum shall continue to remain in effect. The Parties agree to amend or supplement the EU SCCs and UK SCCs if necessary to comply with the mandatory provisions of applicable data protection law.

The Parties’ authorized signatories have duly executed this SCC Addendum as of the Effective Date:

Licensee

Signature: __________________________

Name: __________________________

Title: __________________________

Date: __________________________

Unily

Signature: __________________________

Name: Mark Sahal

Title: Chief Operations Officer

Date: 13th December 2022
ATTACHMENT 1
STANDARD CONTRACTUAL CLAUSES
Controller to Processor

The Standard Contractual Clauses attached to the Commission Implementing Decision (EU) 2021/314 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 are incorporated into the Agreement(s) via this Addendum as follows:

SECTION I in fully including:

Clause 7, Docking Clause

SECTION II in full including:

Clause 9(a), Use of sub-processors. Option 2: General written authorization. The data importer has the data exporter’s general authorisation for the engagement of sub-processor(s) The current list of relevant Sub-processors, including a description of their processing activities and countries of location, can be found on Unily’s webpage at https://www.unily.com/legal/sub-processors#request-updates. Client hereby consents to these Sub-processors, their locations and processing activities as it pertains to their Personal Data. The weblink contains a mechanism to subscribe to notifications of new Sub-processors, and if Client subscribes, Unily shall provide written notification of a new Sub-processor(s) thirty (30) 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.

Clause 11 Redress

Clause 13(a), Supervision. 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.

SECTION III in full

SECTION IV in full including:

Clause 17, Governing Law. Option 2 (for Module Two): 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(b), Choice of forum and jurisdiction: (b) The Parties agree that those shall be the courts of the EU Member State set forth in Clause 17.

ANNEX I

A. LIST OF PARTIES

Data exporter:
Name: Licensee
Address: As per the applicable Agreement(s) between the Parties.
Contact person’s name, position and contact details: See the applicable Agreement(s) between the Parties.
Activities relevant to the data transferred under these Clauses: Details of the activities as described in the applicable Agreement(s).
Signature and date: Signed and dated per Addendum above
Role: Controller
### Data Importer(s):
Name: Unily Inc.
Address: 31 Bond Street, New York, 10012, United States
Name: Unily Group Limited and Unily Limited
Address: First Floor, The Granary Abbey Mill Business Park, Lower Eashing, Godalming, Surrey, GU7 2QW, United Kingdom
Co. number: 08804209 (Unily Group Ltd) and 05654147 (Unily Ltd)
Contact person’s name, position and contact details: F.A.O, Data Protection Officer, privacy@unily.com

### Activities relevant to the data transferred under these Clauses:
Data Importer(s) provide an employee experience platform for businesses to communicate, collaborate, and create. Data Importer utilizes digital experiences, integrations with enterprise applications, and connects client personnel. Processing is conducted as part of the services provided and ordered by Data Exporter pursuant to the master Agreement between Data Importer and Data Exporter for the intranet software solution known as Unily. For Hosting Services, ITSM Service Management tool for creating and management of an incident, requests with means of communication and Email SMTP Services, for the Term.

Signature and date: **Signed and dated per Addendum above**
Role: Processor

### B. DESCRIPTION OF TRANSFER

<table>
<thead>
<tr>
<th>Categories of data subjects whose personal data is transferred</th>
<th>Authorized Users (e.g., Employees, Contractors, Personnel) of Data Exporter and its Affiliates as described in the applicable Agreement(s).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Categories of Personal Data Transferred</td>
<td>Personal Data provided by Data Exporter to Data Importer, in order to facilitate services described in the applicable Agreement(s), including but not limited to: names, user email addresses, usernames, photos, IP addresses, phone numbers, physical or mailing addresses, social IDs (e.g. Facebook ID, Google ID), and other info collected via social login (e.g. profile, connections, contact info, interests)</td>
</tr>
<tr>
<td>Sensitive Data transferred:</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis)</td>
<td>Continuous</td>
</tr>
<tr>
<td>Nature and Purpose of Processing</td>
<td>Nature: Processing as part of the Services provided to Data Exporter in the Agreement(s) with Data importer, for the provision of Unily intranet software application. Purpose: The purpose of the Processing of Personal Data by data importer is for the performance of the Services pursuant to the Agreement including Service Level Management and other performances such as granting access and allowing use of software application by authorized users, reporting measurements and development of new or additional services based off client's need. Personal data will be processed through the Unily software application.</td>
</tr>
<tr>
<td>The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period</td>
<td>The Personal Data will be retained pursuant to termination/expiration of the Services under the applicable Agreement(s).</td>
</tr>
</tbody>
</table>
For transfers to sub-processors, also specify the subject matter, nature and duration of the processing

| Subject Matter: Same personal data categories as provided above |
| Nature: Hosting Services, ITSM Service Management tool, Email SMTP Services, software services. |
| Duration: Length of Agreement(s) between Data Importer and Subprocessor |

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority will be the supervisory authority of the data exporter as required by Clause 13.

ANNEX II

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

The following terms describe the technical and organizational measures, internal controls, and information security routines that Unily maintains to safeguard data provided by or on behalf of our clients in connection with a client service engagement ("Client Data"). These security measures are intended to protect Client Data when in Unily’s environments (e.g., systems, networks, facilities) against accidental, unauthorized, or unlawful access, disclosure, alteration, loss, or destruction. When Client Data includes personal data, our implementation of and compliance with these measures (and any additional security measures set out in the applicable client agreement(s)) is designed to provide an appropriate level of security in respect of the processing of the personal data. Unily may change these measures from time to time, without notice, so long as any such revisions do not materially reduce or degrade the protection provided for the Client Data.

STANDARD DATA SAFEGUARDS:

1. Organization of Information Security
   a. Security Ownership. Unily will appoint one or more security officers responsible for coordinating and monitoring the security rules and procedures.
   b. Security Roles and Responsibilities. Unily's personnel with access to Client Data will be subject to confidentiality obligations.
   c. Risk Management Program. Unily will have a risk management program in place to identify, assess and take appropriate actions with respect to risks related to the processing of the Client Data in connection with the applicable agreement(s) between the Parties.

2. Asset Management
   a. Asset Inventory. Unily will maintain an asset inventory of its infrastructure, network, applications, and cloud environments. Unily will also maintain an inventory of its media on which Client Data is stored. Access to the inventories of such media will be restricted to personnel authorized in writing to have such access.
   b. Data Handling. Unily will
      i. Classify Client Data to help identify such data and to allow for access to it to be appropriately restricted.
      ii. Limit printing of Client Data from its systems to what is minimally necessary to perform services and have procedures for disposing of printed materials that contain Client Data.
      iii. Require its personnel to obtain appropriate authorization prior to storing Client Data outside of contractually approved locations and systems, remotely accessing Client Data, or processing Client Data outside the Parties’ facilities.

3. Human Resources Security
   a. Security Training. Unily will
i. Inform its personnel about relevant security procedures and their respective roles.
ii. Inform its personnel of possible consequences of breaching the security rules and procedures.
iii. Only use anonymous data in its training environments.

4. Physical and Environmental Security
   a. Physical Access to Facilities. Unily will implement and maintain procedures to limit authorized access to its facilities where information systems that process Client Data are located.
   b. Physical Access to Components. Unily will maintain records of the incoming and outgoing media containing Client Data, including the kind of media, the authorized sender/recipient, date and time, the number of media, and the types of Client Data they contain.
   c. Component Disposal. Unily will use industry standard (e.g., ISO 27001, Azure CIS 1.3.0, and/or NIST Cyber-Security Framework, as applicable) processes to delete Client Data when it is no longer needed.

5. Communications and Operations Management
   a. Operational Policy. Unily will maintain security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Client Data.
   b. Mobile Device Management (MDM)/Mobile Application Management (MAM). Unily will maintain a policy for its mobile devices that:
      i. Enforces device encryption.
      ii. Prohibits use of blacklisted apps.
      iii. Prohibits enrolment of mobile devices that have been "jail broken."
   c. Data Recovery Procedures. Unily will
      i. Have specific data recovery procedures with respect to its systems in place designed to enable the recovery of Client Data being maintained in its systems.
      ii. Review its data recovery procedures at least annually.
      iii. Log data restoration efforts with respect to its systems, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.
   d. Malicious Software. Unily will have anti-malware controls to help avoid malicious software gaining unauthorized access to Client Data, including malicious software originating from public networks.
   e. Data Beyond Boundaries. Unily will
      i. Encrypt Client Data that it transmits over public networks.
      ii. Protect Client Data in media leaving its facilities (e.g., through encryption).
      iii. Implement automated tools where practicable to reduce the risks of misdirected email, letters, and / or faxes from its systems.
   f. Event Logging.
      i. For its systems containing Client Data, Unily will log events consistent with its stated policies or standards.

6. Access Control
   a. Access Policy. Unily will maintain a record of security privileges of individuals having access to Client Data via its systems.
   b. Access Authorization. Unily will
      i. Maintain and update a record of personnel authorized to access Client Data via its systems.
      ii. When responsible for access provisioning, promptly provision authentication credentials.
      iii. Deactivate authentication credentials where such credentials have not been used for a period of time (such period of non-use not to exceed 30 days).
iv. Deactivate authentication credentials upon notification that access is no longer
needed (e.g., employee termination, project reassignment, etc.) within two
business days.

v. Identify those personnel who may grant, alter, or cancel authorized access to
data and resources.

vi. Ensure that where more than one individual has access to its systems containing
Client Data, the individuals have unique identifiers/logins (i.e., no shared ids).

c. Least Privilege. Unily will

i. Only permit its technical support personnel to have access to Client Data when
needed

ii. Maintain controls that enable emergency access to productions systems via,
temporary ids or ids managed by a Privileged Identity Management System
(PIMS).

iii. Restrict access to Client Data in its systems to only those individuals who
require such access to perform their job function.

iv. Limit access to Client Data in its systems to only that data minimally necessary
to perform the services.

v. Support segregation of duties between its environments so that no individual
person has access to perform tasks that create a security conflict of interest
(e.g., developer/reviewer, developer/tester).

d. Integrity and Confidentiality. Unily will instruct its personnel to disable administrative
sessions when leaving premises or when computers are otherwise left unattended.

e. Authentication. Unily will

i. Use industry standard (e.g., ISO 27001, Azure CIS 1.3.0, and/or NIST Cyber-
Security Framework, as applicable) practices to identify and authenticate users
who attempt to access its information systems.

ii. Where authentication mechanisms are based on passwords, require that the
passwords be renewed every 70 days.

iii. Where authentication mechanisms are based on passwords, require the
password to contain at least eight characters and three of the following four
types of characters: numeric (0-9), lowercase (a-z), uppercase (A-Z), special
(e.g., !, *, &,

iv. Ensure that de-activated or expired identifiers are not granted to other
individuals.

v. Monitor repeated attempts to gain access to its information systems using an
invalid password.

vi. Maintain industry standard (e.g., ISO 27001, Azure CIS 1.3.0, and/or NIST Cyber-
Security Framework, as applicable) procedures to deactivate passwords
that have been corrupted or inadvertently disclosed.

vii. Use industry standard (e.g., ISO 27001, Azure CIS 1.3.0, and/or NIST Cyber-
Security Framework, as applicable) password protection practices, including
practices designed to maintain the confidentiality and integrity of passwords
when they are assigned and distributed, as well as during storage.

f. Multi Factor Authentication. Unily will implement Multi-Factor Authentication for
internal access and remote access over virtual private network (VPN) to its systems or to
cloud hosted applications.


a. At least annually, Unily will perform penetration and vulnerability assessments on Unity’s
IT environments in accordance with Unily’s internal security policies and standard
practices.

b. Perform at least quarterly testing of the Unily Application at the current latest release

c. Unily agrees to share with Client summary level information related to such tests as
conducted by Unily to the extent applicable to the Services.

d. For clarity, as it relates to such penetration and vulnerability testing, Client will not be
entitled to
i. data or information of other customers or clients of Unily;
ii. test third party IT environments except to the extent Unily has the right to allow such testing;
iii. any access to or testing of shared service infrastructure or environments, or
e. any other Confidential Information of Unily that is not directly relevant to such tests and the Services. For any Unily IT systems that are physically dedicated to Client, the Parties may agree to separate, written testing plans and such testing will not to exceed two tests per year.

8. Network and Application Design and Management Unily will
   a. Have controls to avoid individuals gaining unauthorized access to Client Data in its systems.
   b. Use data loss prevention to monitor or restrict movement of sensitive data.
   c. Use network-based web filtering to prevent access to unauthorized sites.
   d. Use Distributed denial of service (DDoS) protection.
   e. Use MFA protected least privilege accounts and PIMs for production access.
   f. Use network intrusion detection and / or prevention in its systems.
   g. Use a cloud native SIEM/SOAR for monitoring, detection, and automation.
   h. Use secure coding standards.
   i. Scan for and remediate OWASP vulnerabilities in its systems.
   j. To the extent technically possible, expect that the Parties will work together to limit the ability of Unily’s personnel to access non-Client and non-Unily environments from the Client systems.
   k. Maintain up to date server, network, infrastructure, application, and cloud security configuration standards
   l. Scan its environments to ensure identified configuration vulnerabilities have been remediated.

9. Patch Management
   a. Unily will have a patch management procedure that deploys security patches for its systems used to process Client Data that includes:
      i. Defined time allowed to implement patches (not to exceed 14 business days) for patches as defined by Unily’s standard); and.
      ii. Established process to handle emergency or critical patches as soon as practicable

10. Workstations
    a. Unily will implement controls for workstations it provides that are used in connection with service delivery/receipt incorporating the following:
       i. MDM/MAM that manages overall compliance of workstation and reports at a minimum on a weekly basis to a central system
       ii. Encrypted OS and Fixed Drives
       iii. Patching process so that workstations are patched within the documented patching schedule
       iv. Ability to prevent blacklisted software from being installed
       v. Antivirus with continuous monitoring and Advanced Threat Detection with a minimum full weekly scan
       vi. Firewalls installed, enabled, and enforced on all profiles

11. Information Security Breach Management
    a. Security Breach Response Process. Unily will maintain a record of its own security breaches in its systems with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the process for recovering data.
    b. Service Monitoring. Unily’s security personnel will review their own logs as part of their security breach response process to propose remediation efforts if necessary.

a. Unily will have processes and programs that are aligned to ISO27001:2013 to enable recovery from events that impact its ability to perform in accordance with the Agreement(s).

SUPPLEMENTARY MEASURES:
In addition, in accordance with regulatory guidance following the European Court of Justice “Schrems II” decision, Unily further commits to maintaining the following additional technical, organizational, and legal/contractual measures with respect to Client Data, including personal data.

Technical Supplementary Measures:
1. The Client Data in transit between Unily’s entities will be strongly encrypted with encryption that:
   a. is state of the art,
   b. secures the confidentiality for the required time period
   c. is implemented by properly maintained software
   d. is robust and provides protection against active and passive attacks by public authorities, including crypto analysis, and
   e. does not contain back doors in hardware or software, unless otherwise agreed with the applicable Client
2. The Client Data at rest and stored by any Unily entities will be strongly encrypted with encryption that:
   a. is state of the art,
   b. secures the confidentiality for the required time period
   c. is implemented by properly maintained software
   d. is robust and provides protection against active and passive attacks by public authorities, including crypto analysis, and
   e. does not contain back doors in hardware or software, unless otherwise agreed with the applicable Client

Organizational Supplementary Measures:
1. The Client Data transfer between Unily entities and the processing by any Unily entities will be in accordance with:
   a. Unily’s internal policies and procedures to manage requests from public authorities to access personal data,
   b. Unily’s internal data access and confidentiality policies and procedures,
   c. Unily’s internal data minimization policies and procedures, and
   d. Unily’s internal data security and data privacy policies and procedures.
2. Unily will maintain a documented log of requests for access to personal data received from public authorities and the response provided, along with the legal reasoning and the involved parties.
3. Unily will regularly provide reports of public authority requests for personal data, if any, to Unily’s Chief Technology Officer and Board.

Legal/Contractual Supplementary Measures:
1. Where such country is not formally recognized as providing a level of protection essentially similar to UK/EU countries, Unily shall endeavour to maintain assessment reports with respect to applicable surveillance laws and privacy practices for the countries in which Unily processes Client Data. Unily will provide copies of applicable reports to clients upon request.
2. The Unily entity/s processing Client Data certify that, unless otherwise agreed with the applicable Client:
   a. it has not purposefully created back doors or similar programming that could be used to access the system and/or personal data
   b. it has not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems, and
   c. to the best of Unily’s knowledge, applicable national law or government policy does not require the Unily entity to create or maintain back doors or to facilitate access to personal data or systems or for the Unily entity to be in possession or to hand over the encryption key without a legally valid order and following an appropriate legal review.
3. To the extent permitted under applicable law the Unily’s entity/s processing Client Data will inform the client of Government Requests relating to Personal Data that Unily is processing on behalf of the client. If, under applicable law, Unily is not permitted to inform the client of a Government...
Request, Unily will take reasonable steps to either
   i. obtain administrative or judicial leave to inform the client at the earliest possible time or
   ii. request that the respective Government Authority directly informs the client. In any event, Unily will take reasonable steps before the courts or in administrative proceedings to challenge Government Requests it deems unlawful.

4. Unily will advise the applicable client of any change in applicable law that would affect Unily’s ability to comply with the data transfer mechanism relied on.

5. The Unily entity’s processing Client Data will allow the applicable client to verify if its personal data was disclosed to public authorities via agreed audit procedures as set out in the applicable client agreement(s).

6. The Unily entity’s processing Client Data will not engage in any onward transfer of Client Data, or suspend ongoing transfers, without the client's approval as required in the applicable client agreement(s) or as otherwise required by law.

7. Nothing herein shall prejudice the rights of the data subject to recover damages from Unily to the extent permitted by applicable law in the event Unily discloses Client Data transferred in violation of its commitments contained under the chosen transfer tool.

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:

**Microsoft:**
See details at: [Protect information subject to data privacy regulation | Microsoft Learn](#)

**ServiceNow UK Limited:**
See Section 2, Physical, Technical and Administrative Security Measures under Data Security Guide. [Microsoft Word - Pre-signed DPA_DSG (Updated 07.17.2020)(CLEAN).docx](servicenow.com) and [ServiceNow Service Privacy Statement – ServiceNow](#)

**Twilio Inc (SendGrid):**
See [Technical and Organizational Measures](#) in Schedule 2: [Data Protection Addendum | Twilio](#) and [Twilio GDPR Program | www.twilio.com](#)

**HubSpot Inc.:**
See details at: [HubSpot Security Program](#) and [HubSpot Privacy Policy](#)

**PlanhatAB:**
See details at: [Planhat: Privacy Policy](#)

**SalesForce:**
See details at: [Trust and Compliance Documentation - Salesforce.com](#)

**FinancialForce UK Limited:**
See details at: [FinancialForce Information Security Program - FinancialForce](#)
ANNEX III
LIST OF SUB-PROCESSORS

The current list of relevant Sub-processors, including a description of their processing activities, countries of location and transfer mechanism (where applicable) can be found on Unily’s webpage at Unily Sub Processors.

ATTACHMENT 2

UK International Data Transfer Addendum (“UK IDTA”, “UK SCCs”)
to the EU Commission Standard Contractual Clauses (“EU SCCs”)

Table 1: Parties

- Licensee is designated a controller and the “data exporter”, and Unily a processor and the “data importer”, Module 2 of the EU SCCs applies.

Table 2: Selected SCCs, Modules and Selected Clauses

- This Attachment 3 and the UK IDTA, as hereby referenced in https://ico.org.uk/media/for-organisations/documents/4019483/international-data-transfer-addendum.pdf is appended to the version of the approved EU SCCs (completed as described above in SCC Attachment 1) following the effective date of this SCC Addendum (including clause 7, 9(a) General authorization with 30 days’ notice, 11 redress, and 17/18(b) governing law and jurisdiction shall be governed by the law of the country of the United Kingdom in which the data exporter is established.

Table 3: Appendix Information

- The Annexes (I, IB, II, and III) are completed as described above for the EU SCCs in Attachment 1 of this SCC Addendum; and

Table 4: Ending this Addendum when the Approved Addendum Changes

- Neither Party may end the UK SCCs as set out under Section 19 of the IDTA.