SERVING AUTHORS WORLDWIDE
AU SERVICE DES AUTEURS DANS LE MONDE
AL SERVICIO DE LOS AUTORES EN EL MUNDO

ISWC AUTOMATED LOOKUP SERVICE: TERMS AND CONDITIONS

SG23-0244

CISAC
www.cisac.org
info@cisac.org
+33 (0)1 55 62 08 50
20-26 boulevard du Parc
92200 Neuilly-sur-Seine, France

Confédération Internationale des Sociétés d'Auteurs et Compositeurs
SIRET : 784 668 667 00024 - APE : 913E - TVA FR 22 784 668 667

BETWEEN

[Name of company], a company incorporated in [*to be completed*] with registered number [*to be completed*] whose registered office is at [*to be completed*], represented by [*Name*], [*Function*], duly authorised to do so,

(Hereinafter called the "**Licensee**")

AND

Confédération Internationale de Sociétés d'Auteurs et Compositeurs (CISAC), a French Association governed by the French Law on Association of July 1st, 1901, whose head office is at 20 - 26 Boulevard du Parc 92200 Neuilly-sur-Seine France, represented by Gadi ORON, Director General, duly authorised to do so,

(Hereinafter called "**CISAC**")

In the following, CISAC and the Licensee are also referred to jointly as the "**Parties**" and individually as the "**Party**".

WHEREAS

1. CISAC, as the ISWC Registration Authority, operates the International Standard Musical Work Code (ISWC) and associated system, services and databases, i.e., the ISWC System, the ISWC Network, etc. The ISWC is a unique, permanent, and internationally recognized reference number for the identification of musical works. The ISWC standard has been approved by the International Organization for Standardisation ("ISO") and is currently assigned by CISAC societies through the ISWC System.

2. In order to improve the adoption and use of the ISWC as an identifier of musical works by stakeholders of the music industry, CISAC makes available a specific tool interfaced with the ISWC System allowing various stakeholders, such as Licensee, to access and perform automated searches and to retrieve in bulk the ISWC Data (hereafter, "**ISWC Automated Lookup Service**").

3. The Parties thus wish to enter into these Terms and Conditions and appendices (hereafter the "**Agreement**"), to govern the access and use of the ISWC Automated Lookup Service, and associated use of ISWC Data, by the Licensee.

1. Definitions

Each term that starts with a capital letter and is not otherwise defined in this Agreement has the meaning set forth in this article 1.

1.1 Additional Terms means additional terms and conditions that may be provided by CISAC in connection with Licensee's access and use of the ISWC Automated Lookup Service, and associated use of the ISWC Data, including, without limitation, in connection with related technology and additional features, functionality, products and/or services that CISAC may make available as part of, or in connection with, the ISWC Automated Lookup Service.

1.2 "CISAC Society/ies" means any organisation providing ISWC Data to the ISWC System (e.g. CISAC member societies and client rights management entities).

1.3 "Confidential Information" means all data and information (written or oral) provided pursuant to or in accordance with this Agreement or concerning the business and affairs of CISAC or Licensee, which either of them shall have obtained or received as a result of the discussions leading up to, or the entering into, or the performance of this Agreement. It is understood that Confidential Information notably includes reporting survey results performed in accordance with Article 8.

1.4 "Controller" shall have the meaning specified in the applicable Data Protection Law.

1.5 "Data Protection Law" means any law, rule or regulation relating to the processing, privacy, and use of Personal Data, as applicable to CISAC, the Licensee, and/or the ISWC Automated Lookup Service and ISWC Data, including, without limitation, the General Data Protection Regulation (EU) 2016/679 ("GDPR"), and/or any applicable corresponding or equivalent national laws.

1.6 "Data Subject" shall have the meaning specified in the applicable Data Protection Law.

1.7 "Fees" means the fees described in Article 9.1.

1.8 "Force Majeure Event" means any event beyond the control of the will of either Party, and which prevents the fulfillment, in whole or in part, of a Party's contractual obligations, including, without limitation, any act of war, act of God or nature, earthquake, hurricanes, tornados, flood, fire or other similar casualty, embargo, riot, terrorism, sabotage, strike or labor difficulty, governmental act, law or regulation, insurrections, terrorism, epidemic, quarantine, inability to procure materials or transportation facilities, failure of power, court order, condemnation, failure of the Internet, failure of a supplier or other cause, whether similar or dissimilar to the foregoing, not resulting from the actions or inactions of such Party.

1.9 "Intellectual Property Rights" means any and all (i) copyright, database rights, rights in unregistered trademarks, unregistered design rights, and any other similar rights in any part of the world; and (ii) patents, registered trademarks, registered designs, and any other registered rights in any part of the world, and all related goodwill, applications for registration for any such rights as may exist anywhere in the world, and the right to make such applications.

1.10 "ISWC" means the unique, permanent, and internationally recognized reference number for the identification of musical works.

1.11 "ISWC Data" means, collectively, the ISWC and ISWC Related Metadata.

1.12 "ISWC Related Metadata" means a musical work's title, creators' (composers, authors, arrangers, translators etc.) names, roles, IP name numbers.

1.13 "**ISWC System**" means the system operated by CISAC and containing the ISWC Data.

1.14 "Permitted Purpose" means the purpose(s) in relation to the Licensee's authorized access and use of the ISWC Automated Lookup Service, and associated use of ISWC Data, described in Article 5.1 of this Agreement.

1.15 "Personal Data" shall have the meaning specified in applicable Data Protection Law and shall include for the purpose of this Agreement a musical work's creators' (composers, authors, arrangers, translators etc.) names, roles, and IP name numbers.

1.16 "Personal Data Breach" shall have the meaning specified in applicable Data Protection Law.

1.17 "Preferred ISWC" means the ISWC retrieved from the ISWC Automated Lookup Service (as opposed to an "archived ISWC", which shall not be used anymore by the Licensee). The Preferred ISWC should be used by the Licensee in accordance with Article 6.

1.18"Subscription Key" means the code provided by CISAC to the Licensee, after the execution of the Agreement by the Parties, for accessing the ISWC Automated Lookup Service.

1.19 "Supervisory Authorities" shall have the meaning specified in applicable Data Protection Law.

1.20 "Term" means the duration of the Agreement as specified in Article 18 of this Agreement.

1.21 "Third Party" means any person other than the Licensee, a User or CISAC.

1.22 "**Update**" means any improvement, modification, update, made by CISAC, at its sole discretion, on the ISWC Automated Lookup Service during the Term of this Agreement.

1.23 "User" means each employee of the Licensee who is authorized by the Licensee to access and use the ISWC Automated Lookup Service, and associated ISWC Data, in accordance with the Agreement for the Permitted Purpose.

2. Affirmation of authorization

2.1. Licensee (1) declares and represents that it is fully able and competent to enter into the terms, conditions, obligations, affirmations, representations, and warranties set forth in this Agreement, and to abide by and comply with this Agreement; (2) acknowledges that it has read and understood the limitations and restrictions set forth in this Agreement; and (3) accepts and agrees to abide by this Agreement at all times when accessing or using the ISWC Automated Lookup Service and ISWC Data.

2.2. This Agreement applies to all Users accessing or using the ISWC Automated Lookup Service, and ISWC Data, on Licensee's behalf or using Licensee's Subscription Key. Licensee represents and warrants that (1) only Users can access and use the ISWC Automated Lookup Service and that (2) such Users accessing or using the ISWC Automated Lookup Service and ISWC Data on its behalf have been advised of and agree to be bound by this Agreement, including its appendices, before accessing the ISWC Automated Lookup Service.

3. Purpose of the Agreement

The purpose of the Agreement is to define the terms under which CISAC provides the Licensee, in consideration of the payment of the Fees by the latter, with the right to access and use the ISWC Automated Lookup Service (and associated use of ISWC Data) solely for the Permitted Purposes specified in Article 5.1 below.

This Agreement applies whether the Licensee accesses and uses the ISWC Automated Lookup Service via a personal computer, a wireless or mobile device or any other IP-enabled technology.

4. Contractual documentation and order of precedence

Unless otherwise specified in the Agreement, the Agreement includes the following documents which are ranked by order of precedence:

i. This document and any amendment thereto.
ii. The Annex to this document and any amendment thereto.
iii. Any additional document, including Additional Terms, incorporated by reference.

5. Licence

5.1. Scope of the Licence

Subject to compliance by the Licensee with all provisions of the Agreement, CISAC hereby grants the Licensee, for the Term, a limited, non-exclusive, non-transferable, worldwide license to access and use the ISWC Automated Lookup Service and ISWC Data, pursuant to the terms and conditions of this Agreement, with no right to sublicense to a Third Party, for the following Permitted Purposes, (hereafter, the "**License**"):

- To look up the ISWC Data related to a given musical work so as to (i) identify musical works using ISWC Data within Licensee's documentation systems and (ii) ensure data consistency as well as accurate identification of a musical work for the benefit of the author(s), composer(s) and publisher (s).

- To incorporate and/or display ISWC Data in Licensee's own services or derivative dataset that it provides to Third Parties but solely for the purpose of uniquely identifying a musical work, and subject to (i) compliance with Article 12 and (ii) acknowledgement of the source of the ISWC Data with the following wording: "based on data provided by CISAC", whether the ISWC Data is used "AS IS" or in a derivative dataset.

- To use ISWC Data in data exchanges with all its partners, solely for the purpose of improving the identification of works throughout the value chain subject to (i) compliance with Article 12 and (ii) acknowledgement of the source of the ISWC Data with the following wording: "based on data provided by CISAC", whether the ISWC Data is used "as is" or in a derivative dataset.

Other than the temporary and limited License granted above for the Permitted Purposes in accordance with the Agreement, the Licensee does not obtain any right or interest in all or any part of the ISWC Automated Lookup Service, and ISWC Data.

5.2. License limitations

The Licensee shall not access, and/or use the ISWC Automated Lookup Service, and ISWC Data for any other purpose than the Permitted Purposes (such other purposes, "Prohibited Purposes").

For the avoidance of doubt, all uses other than the Permitted Purposes, as strictly and expressly authorized above in Article 5.1, shall constitute Prohibited Purposes, and include, but are not limited to:

- Commercializing in any way, ISWC Data (on a standalone basis), including selling, offering for sale, marketing, promoting, advertising, or using for any other purpose ISWC Data than for the Permitted Purpose. By way of example and not of limitation, such commercialization may include the use of ISWC Data as a basis for the creation, directly or indirectly, of a derivative dataset, in any manner and for any purpose, other than to uniquely identify a musical work, and/or to improve the identification of works throughout the value chain.

- Copying, distributing, manufacturing, adapting, downloading, modifying, reformatting, creating derivative works from, displaying , publishing, disseminating, broadcasting or circulating, translating, extracting, scraping, linking, incorporating into other software, databases or online platform, website or material, or otherwise appropriating the ISWC Automated Lookup Service, and/or all or any part of ISWC Data obtained by using the ISWC Automated Lookup Service.

- Embedding the ISWC Automated Lookup Service (or parts thereof) in "frames" or other pages offered from other sites, and "mirroring" content from the ISWC Automated Lookup Service on a server other than that operated by CISAC or on its behalf by its service provider.

- Developing or running scripts or any tools other than the ISWC Automated Lookup Service in order to generate queries or capture and/or download and/or store the results automatically. In particular, Licensee may not systematically or automatically collect, scrape, harvest, or use other means than the ISWC Automated Lookup Service to extract, copy or use, in any manner, data from the ISWC System.

- Using the ISWC Automated Lookup Service and/or the ISWC Data and/or the ISWC System, in each case in whole or in part, to develop a similar or competing product intended to substitute, or capable of substituting, for the ISWC Automated Lookup Service and the ISWC System.

- Reverse engineering, i.e., decompiling, disassembling, reverse compiling, reverse assembling, or reverse translating or otherwise modifying the content of the ISWC Automated Lookup Service and the ISWC System, or using any means to discover the source code of or trade secret in the ISWC Automated Lookup Service and the ISWC System or otherwise circumvent any technological measure that controls access to the ISWC Automated Lookup Service and the ISWC System.

- Accessing, displaying and using the ISWC Automated Lookup Service in any manner that interferes with its normal operation, its availability, or with any other User's use and enjoyment of the ISWC Automated Lookup

Service and including but not limited to the following acts: (i) modify, disrupt, impair or interfere with the use, features, function, operation or maintenance of the ISWC Automated Lookup Service; (2) impersonate any person or entity or represent the Licensee's affiliation with a person or entity; or (3) solicit the Subscription Key or Personal Data from Third Parties.

- Not to make available to any Third Party, either directly or indirectly, any part of the ISWC Automated Lookup Service or the ISWC Data, except as permitted in Section 5.1 hereof.

- Not enable any Third Party to engage in any of the acts coming within any of the limitations above.

Every act not expressly authorized under this Agreement is strictly forbidden.

6. Licensee's obligations

The Licensee shall take all reasonable steps to use for the Permitted Purpose, the Preferred ISWC and its ISWC Related Metadata instead of any other ISWC in its possession and/or made otherwise available to it.

In addition, the Licensee undertakes the following:

- To make best efforts to prevent access to the ISWC Automated Lookup Service, and/or to the ISWC Data, by any person except Users. Licensee shall be responsible and liable to CISAC for any act or omission of its Users and shall be responsible for each User's compliance with the Agreement.
- Where Licensee wishes to outsource to a Third Party the performance of any part of its business which requires total or partial access and use of the ISWC Automated Lookup Service, and ISWC Data, Licensee shall obtain CISAC's express prior written consent. In any case, Licensee shall be responsible and liable to CISAC for any act or omission of such Third Party under this Agreement.
- To pay the Fees as set forth in Article 9.1.

7. Access to the ISWC Automated Lookup Service

Licensee acknowledges and agrees that, in order to access and use the ISWC Automated Lookup Service, it may be required to use devices, hardware or technology meeting certain system requirements, determined by CISAC in its sole discretion, and that it is solely responsible for ensuring that the Licensee's devices, hardware or other technology meet all such requirements.

To access and use the ISWC Automated Lookup Service, the Licensee will receive a Subscription Key from CISAC.

The Licensee:

- Acknowledges and understands that the right to access and use the ISWC Automated Lookup Service is granted to the Licensee, on an *intuitu personae* basis, and that such right of access and use is not transferrable or assignable to any Third Party;
- Agrees to take all appropriate measures to ensure that Users will not share the Subscription Key with any Third Party;
- Undertakes to promptly notify CISAC, if it knows or has reason to believe that the security of the Subscription Key has been compromised in any way;
- Is liable for any access to the ISWC Automated Lookup Service with its Subscription Key; and
- Will not circumvent or attempt to circumvent any programs, applications, or processes that CISAC may employ to track, control or limit access to the ISWC Automated Lookup Service, the ISWC System or ISWC Data.

8. Reporting

In consideration of the License given herein, CISAC may from time to time, at its sole discretion, send a survey to the Licensee on usage of the data. The survey is intended to help understand the usage, help improve the data offerings and to give an indication of the innovation and services created downstream. The Licensee shall make its best efforts to

provide to CISAC complete and timely answers to the survey. Anonymized and aggregated results of such survey may be published by CISAC from time to time at CISAC's discretion .

9. Financial Conditions

9.1. Fees and invoicing

In consideration of the grant of the License by CISAC to the Licensee, the Licensee shall pay to CISAC the Fees applicable to the option chosen by the Licensee and which are specified in Annex 2 "Financial Conditions", together with all applicable taxes thereon. The Licensee acknowledges and agrees that the Fees may be modified from time to time by CISAC.

CISAC shall invoice Fees annually in advance.

9.2. Payment terms

All payments are to be made in euros (€). All invoices shall be due and payable in full thirty (30) calendar days from the date of invoice. In the event that any payment remains unpaid at the due date of payment, interest will accrue on the relevant unpaid amount at a per annum rate of three times the applicable legal interest rate until payment is made in full.

9.3. Non-Payment

In the event of a non-payment of any Fee by the Licensee, CISAC shall be entitled, seven (7) days after notification to Licensee to this effect and provided that payment has not been received within that period, to:

(i) Suspend the access to and use of the ISWC Automated Lookup Service until payment is made, and/or
(ii) Terminate this Agreement, without prejudice to any other rights and remedies it may have at law or under the Agreement, in particular the right to commence proceedings for the payment of the amounts still owing and to any damages.

10. Intellectual Property rights

10.1. General

The Licensee acknowledges that all the Intellectual Property Rights regarding or in connection with the ISWC Automated Lookup Service, and ISWC Data, including any Update thereto, as well as the manner in which they are presented or appear and all information relating thereto are the property of CISAC and/or CISAC Societies.

10.2. Trademarks

The Licensee agrees that it will not remove any copyright, trademark, logos or other proprietary notices of CISAC affixed to or displayed on the ISWC Automated Lookup Service. In addition, the Licensee shall not during or after the expiry or termination of this Agreement, without the prior written consent of CISAC use or adopt any trademark, trade name, or commercial designation that includes or is similar to or may be mistaken for the whole or any part of any trademark, trade name or commercial designation used or owned by CISAC.

10.3. Updates

CISAC may, at its sole discretion, make available Updates to the ISWC Automated Lookup Service, notably as it may be required to comply with Data Protection Law. Subject to provisions of Article 16.1, the Licensee shall always use the then-current version of the ISWC Automated Lookup Service.

The Licensee shall be entitled to use any such Updates under the same terms and conditions as for the ISWC Automated Lookup Service as provided under this Agreement, unless otherwise specified in Additional Terms in accordance with Article 21.1.

11. Intellectual Property Rights Indemnities

11.1. CISAC Indemnity

Provided that the Licensee complies with the Agreement, CISAC shall, within the terms of this Agreement, indemnify the Licensee against damages awarded by a competent Court by way of a final decision arising from or incurred by reason of any Third Party claim that the ISWC Automated Lookup Service licensed by CISAC under this Agreement infringes a Third Party's Intellectual Property Rights (hereafter "**Claim**"). In any event, CISAC's liability shall not exceed the total amount of fees paid or payable under the Agreement within the 6 months preceding the event that has given rise to liability.

11.2. Remedies

If the ISWC Automated Lookup Service is adjudged to have infringed or if, in the CISAC's reasonable judgment, is likely to infringe a Third Party's Intellectual Property Rights, then CISAC may, at its option:

i) Procure for Licensee the right to continue using the ISWC Automated Lookup Service or the alleged infringing part thereof;

ii) Replace or modify the ISWC Automated Lookup Service or the alleged infringing part thereof to make it non-infringing; or

iii) Terminate this Agreement immediately by notice in writing to the Licensee.

11.3. Requirements

CISAC indemnification obligation under Article 11 is subject to the following conditions:

- The Licensee shall promptly notify CISAC in writing of any Claim brought against it;
- The Licensee shall give CISAC full and complete authority to conduct the defense of the Claim and CISAC will have complete freedom to compromise, settle or proceed with any procedure;
- The Licensee shall provide CISAC with all reasonable assistance and information in order to enable CISAC to perform its defense;
- The Licensee shall not make any admission of liability, agreement or compromise in respect of a Claim without CISAC's prior written consent.

11.4. Exclusions

The indemnity given by CISAC under this Article 11 shall not cover a Claim arising from:

i) The combination of the ISWC Automated Lookup Service, with material not provided by CISAC or that was not approved by CISAC.

ii) The use of the ISWC Automated Lookup Service, otherwise than in accordance with the terms of this Agreement.

11.5. Sole remedy

Notwithstanding anything in this Agreement to the contrary, this Clause 11 is Licensee's sole and exclusive remedy for any intellectual property infringement claims.

12. Data protection

The Licensee acknowledges and agrees that its access and use of the ISWC Automated Lookup Service, and ISWC Data will lead to the collection and processing of Personal Data which is governed by Data Protection Laws and CISAC's Privacy Policy (https://www.cisac.org/cisac/Privacy-Policy). It is understood that each Party acts in this context as independent Controller.

Regarding the use of the Personal Data, the Licensee as independent Controller is accountable for ensuring compliance with applicable Data Protection Laws and the provisions of this Agreement. Therefore, the Licensee undertakes:

- To comply with all requirements imposed on it by applicable Data Protection Laws;
- To process Personal Data fairly and lawfully in all circumstances;
- To maintain so long as necessary, all permissions, authorizations, or prior advice from Supervisory Authorities where such permissions, authorizations or prior advice are required for the processing of Personal Data by the Licensee;
- Not to use Personal Data for any other Purpose than the Permitted Purpose;
- Not to disclose or allow access to Personal Data to any Third party other than those authorized under the Permitted Purpose;
- To ensure that Data Subjects are informed by any appropriate means of the processing of Personal Data by the Licensee for the Permitted Purpose and that their rights as provided by Data Protection Law are complied with;
- To keep Personal Data accurate and up to date, taking into account the provisions of Article 10.3 of the Agreement;
- Not to retain Personal Data for longer than necessary to achieve the Permitted Purpose taking notably into account the provisions of Article 19.3;
- Taking into account the nature and risks associated with its use of the Personal Data, to have in place appropriate technical and organisational measures, to protect Personal Data against unauthorised or unlawful processing and against accidental loss or destruction of, or damage to it, including, without restriction, when accessing to and using the ISWC Automated Lookup Service;
- To implement measures as required under Data Protection Laws if Personal Data is to be transferred to a recipient outside of the European Economic Area (EEA);
- Upon request by CISAC, to refrain from using Personal Data.

Where the Licensee is located outside the EEA and that its access and use of the ISWC Automated Lookup Service, and ISWC Data leads to a transfer of Personal Data outside of the EEA, such transfer can only be carried out provided that one of the following conditions is met : i) the Licensee is located in a country benefitting from an adequacy decision from the European Commission, or, ii) the Parties execute the Controller-to-Controller Standard Contractual Clauses (SCCs) provided in Annex 1, or iii) another appropriate transfer mechanism as provided by the GDPR is implemented. Where the SCCs are chosen, it is agreed that the signature by the Parties of the Agreement, incorporating the SCCs, shall be deemed as signature of the SCCs.

Each Party undertakes to assist the other in complying with applicable requirements under Data Protection Law including, but not limited to, answering requests from Data Subjects in relation to their rights as provided by Data Protection Laws, and, notifying Personal Data Breaches.

The Licensee shall indemnify and hold CISAC harmless against any loss, damage, or expense (including reasonable legal costs) which CISAC incurs or becomes liable for as a result of a breach by the Licensee of its obligations set out in this Article 12.

13. Confidentiality

13.1. Use of Confidential Information

A Party receiving Confidential Information (the **"Receiving Party"**) from the other Party (the **"Disclosing Party"**) shall keep all such Confidential Information with the same degree of care with which it maintains the confidentiality of its own confidential information, but in no event less than a reasonable degree of care. Neither Party shall use such Confidential Information for any purpose other than in performance of this Agreement and shall not disclose the same to any Third Party (other than those expressly authorized) and such of its and their employees or agents who have a

need to know such Confidential Information to implement the terms of this Agreement. Each Party shall advise any employee or agent who receives such Confidential Information of the confidential nature thereof and of the obligations contained in this Agreement relating thereto, and such Party shall ensure that all such employees and agents comply with such obligations as if they had been a Party hereto. Upon termination or expiration of this Agreement, upon written notice from a Disclosing Party, the Receiving Party shall destroy all documents, tapes or other media containing Confidential Information of the Disclosing Party that remains in such Party's or its agents' or employees' possession and upon request shall confirm in writing such destruction.

Notwithstanding anything to the contrary in this Agreement, Confidential Information shall not include any information or materials that the Receiving Party can demonstrate by documentary evidence:

i) were already legitimately known to the Receiving Party (other than under an obligation of confidentiality), at the time of disclosure by the Disclosing Party;

ii) were generally available to the public or otherwise part of the public domain at the time of its disclosure to the Receiving Party without any breach of confidentiality;

iii) became generally available to the public or otherwise part of the public domain after its disclosure or development, as the case may be, and other than through any act or omission of a Party in breach of such Party's confidentiality obligations under this Agreement;

iv) were disclosed to a Party, other than under an obligation of confidentiality, by a Third Party who had no obligation to the Disclosing Party not to disclose such information to others; or

v) were independently discovered or developed by or on behalf of the Receiving Party without any breach of confidentiality and without the use of the Confidential Information belonging to the other Party.

13.2. Permitted Disclosure

Each Party shall further be entitled to disclose Confidential Information, to the extent required to comply with an order of a judicial body or Regulatory Authority (provided always that, where reasonably practicable and without breaching any legal or regulatory requirements, the Party disclosing the Confidential Information of the other Party will inform such other Party of such disclosure a reasonable period of time before such disclosure actually takes place) or the rules of the stock exchange rules.

Each Party shall (without limiting either Party’s rights under the Agreement or at law) promptly notify the other Party of any unauthorised possession, use or knowledge, or attempt thereof, of the other Party’s Confidential Information by any Third Party of which it becomes aware.

13.3. Survival

The obligations and prohibitions contained in this Clause shall survive the expiration or termination of this Agreement for a period of five (5) years.

13.4. Injunctive relief

In the event of any breach of this Article by either Party, each Party acknowledge that the other Party would suffer irreparable harm and shall therefore be entitled to seek injunctive relief.

14. Verification

CISAC and its agents shall have the right to implement tools to monitor the usage by the Licensee and its Users of the ISWC Automated Lookup Service, and ISWC Data to ensure compliance with this Agreement by the Licensee and its Users.

15. Liability

This Article 15 sets out the entire liability of the Parties to each other arising whether as a result of any breach of their obligations under the Agreement.

Any access and use by Licensee of the ISWC Automated Lookup Service, and ISWC Data other than for the Permitted Purpose shall constitute a breach of this Agreement for which CISAC may, in addition to any other remedies it may have, immediately terminate the Licensee's License.

The Licensee agrees that it will indemnify, defend, and hold CISAC and/or a CISAC Society harmless from any and all claims, liabilities, damages, losses, costs, and expenses (including reasonable attorneys' fees), arising in any way out of or in connection with its (i) use of the ISWC Automated Lookup Service and ISWC Data, and (ii) breach or violation of this Agreement.

The Licensee understands and agrees that its use of the ISWC Automated Lookup Service (and associated use of the ISWC Data) is under its sole responsibility. To the fullest extent permissible by applicable law, CISAC shall not be liable for any loss or damage of any kind, direct or indirect, including, without limitation, compensatory, consequential, incidental, indirect, special or punitive damages, in connection with, or arising from : (i) the Licensee's use of the ISWC Automated Lookup Service and ISWC Data and/or otherwise processing thereby, including any Licensee's preferences or instructions made or given in conjunction with a Licensee's use of the ISWC Automated Lookup Service and ISWC Data or (ii) the Licensee's inability to use the ISWC Automated Lookup Service and ISWC Data, or (iii) the implementation of this Agreement. These include damages relating to errors, omissions, down time, interruptions, defects, delays, computer viruses, Licensee's loss of profits, loss of data, unauthorized access to and alteration of Licensee's transmissions and data, and other tangible and intangible losses. This limitation applies regardless of whether the damages are claimed under the terms of a contract, as the result of negligence or otherwise, and even if CISAC or its service providers or their representatives have been negligent or have been advised of the possibility of such damages. In any event, CISAC's liability shall not exceed the total amount of fees paid or payable under the Agreement within the 6 months preceding the event that has given rise to liability.

16. Disclaimer of warranties

16.1. Accuracy of the data

CISAC does not warrant the quality, accuracy, timeliness or completeness of any information or data contained in the ISWC Automated Lookup Service. Such information and data are provided on an "AS IS" and "AS AVAILABLE" basis without warranty or condition of any nature. The Licensee accepts that CISAC makes no guarantees, warranties, or representations of any kind with respect to the completeness, quality, reliability, adequacy, security, or accuracy of ISWC Data and does not take over responsibility nor warranty or indemnification of the Licensee for any damage, which may result either directly or indirectly from information, which the Licensee retrieved from using the ISWC Automated Lookup Service.

16.2. Availability of the ISWC Automated Lookup Service

CISAC does not warrant that access to or use of the ISWC Automated Lookup Service will be uninterrupted or error-free, that defects will be corrected, that the ISWC Automated Lookup Service, or the server that makes it available are free of viruses or other harmful components.

CISAC reserves the right at any time and from time to time to modify, suspend, or discontinue, temporarily or permanently, the access and use of the ISWC Automated Lookup Service (or any part thereof) with or without notice. The Licensee agrees that CISAC shall not be liable to the Licensee or to any Third Party for any modification, suspension, or discontinuation of the access and use of the ISWC Automated Lookup Service.

17. Force Majeure

If a Force Majeure Event occurs that prevents, hinders or delays a party (the "**Affected Party**") from performing any of its obligations under this Agreement, the Affected Party shall not be liable to the other party and shall be released from its obligation to perform the relevant obligations to the extent that its ability to perform those obligations has been directly affected by the Force Majeure Event.

The Affected Party shall notify the other party in writing as soon as reasonably practical of the occurrence of the Force Majeure Event and the nature and likely duration of its impact upon the other party and the Affected Party takes all reasonable steps to mitigate the impact of the Force Majeure Event.

Upon cessation of the Force Majeure Event, the Affected Party must promptly notify the other party of such cessation and resume performance of the affected obligations.

If the impact of the Force Majeure Event upon the Affected Party continues for a period of thirty (30) calendar days in relation to any obligation under this Agreement, either Party may terminate this Agreement in whole (but not in part) with immediate effect without liability to the other Party by giving notice in writing to the other Party and without having to file any claim in accordance with Article 21.8.

18. Term

This Agreement will enter into force at the date of its signature by the last Party and shall remain in effect for twelve (12) months ("Initial Term"). Unless either Party notifies the other Party of the non-renewal of the Agreement at least three (3) months before the expiration of the term or otherwise terminated earlier in accordance with the terms of this Agreement, the Initial Term (and any renewal term, if any) will automatically renew for successive terms of twelve (12) months.

19. Termination

19.1. Termination for cause

Without prejudice to any other rights and remedies a Party may have at law or under the Agreement, either Party (the "**Non-defaulting Party**") may terminate, as of right, the Agreement, by giving written notice to the other Party (the "**Defaulting Party**") if the Defaulting Party commits a breach of the Agreement and fails to remedy that breach within seven (7) calendar days after receipt of written notice from the Non-defaulting Party. Except as otherwise provided under the Agreement and to the extent permitted by applicable law, will constitute a breach allowing CISAC to immediately terminate the Agreement as specified in article 15, the Licensee's access or use of the ISWC Automated Lookup Service and ISWC Data for any other purpose than the Permitted Purpose.

19.2. Receivership and bankruptcy

To the extent permitted by law, CISAC may terminate this Agreement, as of right, by giving written notice to the Licensee, if the Licensee ceases conducting business in the normal course, makes a general assignment for the benefit of creditors, suffers or permits the appointment of a receiver for its business or assets, or becomes subject to a proceeding relating to insolvency or the protection of creditor's rights.

19.3. Consequences of termination

Immediately upon termination or expiry of this Agreement (howsoever occasioned), the Licensee shall cease accessing and using the ISWC Automated Lookup Service and ISWC Data, including for all Permitted Purposes. The Licensee agrees and acknowledges that in any event, CISAC may immediately terminate the access by the Licensee to the ISWC Automated Lookup Service.

Within thirty (30) days from the effective date of termination or expiration , the Licensee shall (i) irrevocably destroy and delete all ISWC Data and copies of the ISWC Data, including backup and archival copies from its systems, documentation, services and databases (ii) and certify it in writing to CISAC .

Without prejudice to any other rights CISAC may have at law or under the Agreement, any amounts owed to CISAC under this Agreement before or as of such termination or expiration become immediately due and payable.

20. Modification

Licensee acknowledges and agrees that CISAC reserves the right to change, modify or otherwise alter this Agreement at any time. In such a case, CISAC will notify the Licensee of any major change in the best appropriate way (e.g., e-mail, notice in the ISWC Automated Lookup Service, etc.), with reasonable notice, prior to the effective date of such major change. If Licensee disagrees with the changes made by CISAC to the Agreement, Licensee retains the right to terminate the Agreement by providing written notice within one (1) month of CISAC's notification. If CISAC does not receive timely notice, Licensee is deemed to have accepted the change.

21. Miscellaneous

21.1. Additional terms and conditions

Licensee acknowledges and agrees that Additional Terms may be provided in connection with Licensee's access and use of the ISWC Automated Lookup Service and ISWC Data. The Additional Terms will be incorporated into this Agreement by reference as though fully set forth herein.

21.2. Language

Should this Agreement be translated into a foreign language, the English versions shall be the only valid and admissible version.

21.3. Notifications

All notifications, requests, claims or other communications relating to this Agreement (including for the purpose of the SCCs included in Annex 1) shall be made in writing and sent with acknowledgment of receipt or an internationally recognized courier with a record of delivery at the following addresses:

- For CISAC : 20-26 Boulevard du Parc, 92200 Neuilly-sur-Seine, France.
- For Licensee : [Indicate address]
  [Indicate email address]

21.4. Transfer - subcontracting

The Licensee may not assign or transfer, by operation of law or otherwise, any of its rights under this Agreement to any Third Party, or transfer any of the license rights granted hereunder, without the prior written consent of CISAC. Any attempted assignment or transfer in violation of the foregoing will be void.

CISAC may freely assign this Agreement, or subcontract or otherwise delegate its obligations hereunder, in whole or in part, to any Third Party. Any assignment of the Agreement by CISAC releases CISAC for the future.

21.5. Severability

If one or more provisions of this Agreement are deemed invalid or cannot be enforced pursuant to a law or regulation or as the result of the final judgement of a court of jurisdiction, the validity of the remaining clauses and their enforceability shall not be affected or compromised in any way. The Parties shall discuss and use their best efforts to agree upon a valid and enforceable provision that is a reasonable substitute for such invalid or unenforceable provision in view of the intent of this Agreement.

21.6. No waiver

Failure to claim breach by either Party to any provision of this Agreement shall not be construed as acquiescence to the breach nor will it affect the right to invoke such a breach in the future.

21.7. Survival

Any provision of the Agreement which by its nature shall survive expiry or termination of the Agreement shall remain in full force after such expiry or termination. In particular, all provisions relating to proprietary rights, restrictions, liabilities, indemnifications, and warranties shall survive the termination of the Agreement.

21.8. Applicable law and dispute resolution

This Agreement shall be construed in accordance with the laws of France. In case of a dispute relating to this Agreement, the Parties hereto shall each use their best efforts to reach an amicable solution. In the event that the Parties hereto are unable to reach an amicable solution within 6 months after notification of the dispute by the initiating Party, the matter shall be submitted to mediation in accordance with the Centre for Mediation and Arbitration of Paris ("CMAP") Mediation Rules. The sole seat of mediation shall be Paris, France and the proceedings shall be conducted in English; provided that the Parties shall also be authorized to present evidence, testimonies, or submissions in French, in which case a certified translation shall be supplied. If any such dispute has not been settled pursuant to the mediation within 90 days of the commencement of the mediation, it shall be submitted to the courts of Paris which shall have exclusive jurisdiction to adjudicate it, without regard to conflict of law provisions.

21.9. Counterparts

This Agreement may be executed in counterparts, each of which counterparts, when so executed and delivered, shall be deemed to be an original, and both of which counterparts, taken together, shall constitute one and the same instrument even if both Parties have note executed the same counterpart.

IN WITNESS WHEREOF, the Parties hereto have caused this Agreement to be executed by their duly authorized representatives.

LICENSEE	**CISAC**
NAME:	NAME:
TITLE:	TITLE:
DATE:	DATE:
SIGNATURE:	SIGNATURE:

Annex 1 - Standard Contractual Clauses for the transfer of Personal Data from an EU Controller to a Controller located outside the EU (Module 1)

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 - Clause 8.5 (e) and Clause 8.9(b);

(iv) Clause 12 - Clause 12(a) and (d);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Clause 18(a) and (b);

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 (Docking clause) is not applicable

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 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. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix 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 the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation[1] of the data and all back-ups at the end of the retention period.

8.5 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 personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they 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 subject. 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.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

[1] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) 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 personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 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 or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter "onward transfer") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it 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 of Regulation (EU) 2016/679 with respect to the processing in question;

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

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

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

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9 (Use of sub-processors) is not applicable for controller to controller transfers

Clause 10

Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.[3] The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge :

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the

[3] That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter "automated decision"), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under Regulation (EU) 2016/679.

(c) 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.

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

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

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

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

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

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

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

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

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

Clause 15

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

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

---

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

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

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

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

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of France.

Clause 18

Choice of forum and jurisdiction

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

(b) The Parties agree that those shall be the courts of France.

(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 I

A. LIST OF PARTIES

Data exporter:

Name: **Confédération Internationale des Sociétés d'Auteurs et Compositeurs (CISAC)**

Address: **20-26 boulevard du Parc, 92 200 Neuilly sur Seine, France**

Contact person's name, position and contact details: **as provided under article 21.3 Notifications of the Agreement**

Activities relevant to the data transferred under these Clauses: **operator of the ISWC-Net platform**

Role : **Controller**

Data importer :

Name: **The entity identified as "Licensee" under the Agreement entered into with CISAC**

Contact person's name, position and contact details: **as provided under article 21.3 Notifications of the Agreement**

Activities relevant to the data transferred under these Clauses: **digital service provider and aggregators within the music industry**

Role : **Controller**

The signature by the Parties of the Agreement in which these Clauses are incorporated shall be deemed as signature of the present Clauses.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

- Creators of musical works i.e., composers, authors, arrangers, translators

Categories of personal data transferred:

- Creator's first name, last name, and IP number

Sensitive data transferred

- None

The frequency of the transfer:

- Continuous basis

Nature of the processing

- Access, searching, retrieval

Purpose(s) of the data transfer and further processing

- Access to and use by Importer of the International Standard Musical Work (ISWC) code and associated metadata related to a given musical work so as to identify musical works within Importer's documentation systems

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

- Access for the duration of the ISWC Tool agreement signed by Importer

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

- Not applicable

C. COMPETENT SUPERVISORY AUTHORITY

French Data Protection Authority (CNIL).

APPENDIX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

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

Choice to be made by Importer :

☐ 1. The Importer will implement the security measures set out in the annex provided by Importer and attached to these Clauses

☐ 2. The Importer will implement the security measures referenced online at [*insert link to publicly available security procedure, schedule or other document describing Importer security measures*]

☐ 3. The Importer will implement the security measures as selected in the table below.

∞∞

Table to be completed by Importer if it selects choice 3:

TOPIC	MEASURE	
1. Access control to premises and facilities	Unauthorized access is prohibited	☐
	Access control system	☐
	ID reader, magnetic card, chip card	☐
	Door locking (keys, electric door openers etc.)	☐
	Surveillance of facilities	☐
	Alarm system, CCTV monitoring	☐
	Logging exits/entries into facilities	☐
2. Workstation security	Automatic session locking	☐
	Use of regularly updated antivirus software	☐
	Use of regularly updated firewall software	☐
3. Security of mobile equipment	Implementation of encryption on mobile equipment	☐
	Regular back-ups and synchronization	☐
	Locking with password/confidential information	☐
4. Access control to systems	Unauthorized access to IT systems is prevented	☐
	Technical and organizational measures for the identification and authentication of users	☐
	Password compliant with up to date recognized industry and regulatory standards	☐
	Password change in case of reset (different from previous ones)	☐
	Unsuccessful account access attempts are limited	☐
	Captchas are used for access control	☐
	No access for guest users, no anonymous accounts	☐
	Access to systems is centrally managed and restricted to approval by both personnel management and system owner	☐
5. Access control to data	Differentiated access rights (profiles, roles, transactions and objects) are defined	☐
	Access rights defined according to duties and least privilege principle	☐
	Measures to remove obsolete permissions	☐
	Annual review of authorizations granted	☐
6. Logging / incident management	Logging of user access on IT systems	☐
	Users are informed on logging and controls	☐

TOPIC	MEASURE	
	Security of access logs is ensured	☐
	Procedures for security incidents, including data breach, detection and management	☐
7. Network / Disclosure control	Transmission and disclosure of personal is controlled, including electronic transfer, data transportation, transmission control, etc.	☐
	All data is transferred via wholly owned private network	☐
	Encryption/tunnelling (VPN = Virtual Private Network) for remote access, transport and communication of data	☐
	Prohibition of use of portable media	☐
	Wi-Fi network is protected (WPA2 or WPA2-PSK protocol is implemented)	☐
8. Input control	Full documentation of data management and maintenance	☐
	Measures for subsequent checking whether data have been entered, changed, deleted and by whom	☐
	Systems log user activities according to the Importer's security logging standard	☐
9. Security of servers	Access to servers and administration interfaces limited to qualified personnel and is logged	☐
	Procedures are implemented for the installation without delay of critical updates	☐
	Availability of data is ensured	☐
	Measures to check at a later stage if data has been entered, modified or deleted, and by whom:	☐
	Systems that record user activity in accordance with the logging policy of the data importer	☐
10. Job control	The Importer has defined selection criteria for processors/sub-contractors in consideration of guarantees presented for the implementation of security measures/sensitivity of the processing it has been entrusted with	☐
	Measures to allocate the responsibilities between the Importer and its processor/sub-contractor for the implementation of security measures set out in this annex and related to the processing subject to sub-processing	☐
	Use of processor/sub-contractor is formalized (e.g., contract) using unambiguous wording on the service to be provided by processor/sub-contractor	☐
	Process for monitoring contract performance by processor/sub-contractor (e.g., audit)	☐
11. Business Continuity/Availability control	Regular backups	☐
	Uninterruptible power supply (UPS)	☐
	Remote storage of backup medium	☐
	Regular testing of business continuity measures	☐
12. Segregation control	Data collected for different purposes are processed separately.	☐
	Restriction of access to data stored for different purposes according to business function of staff.	☐
	Segregation of systems and/or data	☐
	Segregation of testing and production environments	☐

TOPIC	MEASURE	
13. Archiving control	Specific access methods are implemented to control access to archived data	☐
	Obsolete archives are destroyed securely	☐
14. Website security	TLS protocol is used	☐
	Payment systems are PCI DSS compliant	☐
	No password or identifiers are transmitted via URLs	☐
	Controls are in place to check that user input is as expected	☐
15. Software development	Development environments are separated from production environments	☐
	Supervision only grants mechanisms that offer privacy compliant settings	☐
	The use of free text zones is limited and controlled	☐
	Tests are carried out on anonymous data or synthetic data only	☐
16. User awareness	Users authorized to access and further process personal data are regularly trained on application of data protection legislation and on the precautions and measures to follow when handling personal data	☐
	Users follow a security/data protection policy which is made binding according to Importer's internal rules	☐
17. Control and audits	Importer has a regular audit program covering personal data processing operations	☐
	Audit mechanism: internal and/or external	☐
18. Certifications	Importer hold appropriate security certifications: *specify*	☐

Annex 2 - Financial Conditions

Fees do not include taxes. The Licensee acknowledges and agrees that the Fees may be modified from time to time by CISAC.

Subscription Key	**High Band**	**Medium Band**
Queries per minute	230	115
Queries per month equivalent	**10 million**	**5 million**
Onboarding (One Off)	**10,000 €**	**10,000 €**
Recurring Costs (Annual)		
Business and Technical Support	6,000 €/year	6,000 €/year
ISWC Service Provision costs	30,000 €/year	20,000 €/year
Year 1 Total	**46,000 €**	**36,000 €**
Year 2+ Recurring (Annual) Total	**36,000 €/year**	**26,000 €/year**