DIDOMI

STANDARD TERMS

In order to comply with the Regulation, the Client decided to rely on several solutions published by Didomi:

Didomi publishes:

- an online solution for collecting consents ("CMP"), managing preferences ("PMP"), processing requests to exercise rights ("DSAR"), accessible remotely.
- the Didomi Advanced Compliance Monitoring ("ACM") platform, a tech stack for monitoring, identifying, managing and assessing the activities of actors (or "Vendors") in the open web.

Didomi is selling this access through AWS Marketplace, where the Client has agreed to execute these Standard Terms.

Article 1 : Definitions

The following definitions shall apply to the entire Agreement, for the below capitalized terms, in both singular and plural:

- *Account*: means the Client's online account allowing for access to the Platform.
- *Agreement*: means all the Standard Terms, the appendix and the Purchase Order(s), excluding the Documentation.
- *Beneficiary*: means the company(ies) or entity(ies) belonging to or affiliated with the Client (as defined under Article L233-3 of the French Commercial Code), or any such compan(ies) or entit(ies) as may be referred to in the Purchase Order, and who have access to the Services and the Platform.
- *Client*: means the company referred to in the Purchase Order that executes the Agreement with Didomi.
- *Confidential(s) Information(s)* : means any information disclosed to either Party by the other Party, or obtained by either Party from the other Party that is confidential or designated as such by either Party (e.g., the Agreement and the information contained therein, Documentation that is not public, trade secrets, the operation of the Platform or Services, or commercial information circulating under the Agreement).
- *Didomi:* means (1) if the Client is US or Canadian entity, DIDOMI CORP, C/O Orbiss Inc, 1411 Broadway FL16, New York, NY 10018, USA, Company n°: 6223654, or (2) if the Client is incorporated in any other country, DIDOMI SAS, a French SAS with capital of 42.853 euros, registered with the Paris Trade and Companies Registry under number 831 722 756, whose registered office is at 137 Boulevard Sébastopol, 75002 PARIS, France.
- *Documentation*: means the documentation supplied by Didomi, as accessible at https://developers.didomi.io. The Parties agree that the Documentation has no contractual value or legal effect.
- *Effective Date*: means, in order (1) the Agreement's effective date specified in the Purchase Order, or (2) the Agreement's signature date by the Client.
- *Party:* means individually Didomi or the Client.
- *Platform*: means the online privacy, personal data and preferences consent management service, accessible at https://console.didomi.io.
- *Purchase Order*: means the purchase order for the Services and the Platform, emitted by Didomi and signed by the Client through AWS Marketplace - specific Purchase Orders can be signed for the CMP, the PMP, DSAR and ACM - they are of identical value as they govern different Services.
- *Regulation*: means (i) if the Client is a Canadian company or uses the Services in Canada, any Canadian privacy legislation, (ii) if the Client is a US company or uses the Services in the US, any United States Privacy Laws, including but not limited to the Californian Consumer Privacy Act on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, (iii) if the Client also uses the Services in the European Economic Area, means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter the "GDPR") as well as Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) and the implementation recommendations of the competent supervisory authorities within the European Economic Area (iv) if the Client is located in the United Kingdom or uses the Services in the United Kingdom, means instead the Data Protection Act 2018, and all applicable subordinate legislation, statutory instruments and implementing legislation (including without limitation relevant provisions of the European Union (Withdrawal) Act 2018 (EUWA) and the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019/419) implementing, modifying, merging or otherwise relating to the GDPR as retained under UK law. Any reference to GDPR in the Agreement refers instead to the provisions replacing GDPR in the United Kingdom.
- *Services:* means the services supplied by Didomi as detailed in the Purchase Order.
- *Standard Terms:* means these standard terms.
- *Support*: means the site(s), mobile application(s) and/or online interface(s) on which the Services are deployed, as may be specified in the Purchase Order.
- *Monthly Unique Visitors:* means an approximation of the monthly volume of visitors on the Client's Supports via the pageview and app session events. The volume of visitors is the approximate number of distinct user IDs (UUID generated locally by Didomi's SDK on the device) divided by the sampling rate (number of ID/rate). The sampling for the web pageviews is 0.03 (3%) and the sampling for the app sessions is 0.10 (10%). For more details: https://support.didomi.io/understand-your-monthly-unique-visitors-muvs
- *User:* means the individual(s) authorized by the Client or the Beneficiaries, who has access to the Platform and the Services.
- The terms "Controller", "Processor", "Personal Data", "Data Subject" and "Processing" shall be understood in accordance with the meaning assigned to them in the Regulation.
- When referring to retention of Client data in the Agreement, each year means 365 days and in case of custom retention, every 6 months increment means 183 days.

Unless the context otherwise requires, the terms and definitions used in the singular form refer to the plural form and vice versa.

DIDOMI

Article 2 : Services

Didomi shall ensure that the Platform and the Services detailed in the Purchase Order are available to the Client, the Beneficiaries and the Users, in compliance with the terms set out in the Agreement. Didomi shall be solely responsible for its technical and human resources in order to ensure that the Services and the Platform are available.

The Services and the Platform shall be standard, shall be accessible from a remote location and shall not require any services in order to be integrated into the IT systems of the Client or the Beneficiaries, except where provisions are made in the Purchase Order for the supply of additional professional services. If onboarding is included in the Purchase Order, the terms of Annex 2 "Onboarding" apply, and Didomi will provide the contact details and availability schedule of a specialist when the Agreement enters into force. The Client must then schedule an onboarding meeting with the specialist, which must take place within a maximum of forty-five (45) days from the date of entry into force of the Agreement. If such a meeting has not been scheduled, the Client will be considered to have waived the onboarding Service and will not be able to use it. Onboarding at a later date may be subject to additional fees.

This paragraph describes the basic SLA - the SLA terms may vary if the Purchase Order includes a higher tier SLA. Didomi agrees that the Platform shall operate in compliance with the following features: (i) access shall be provided 24/7, and Didomi shall provide reasonable efforts to ensure ninety-nine percent (99%) availability on a monthly basis, subject to any testing or installation phase, and further subject to any interruptions required for the repair and technical maintenance of its hardware or software; (ii) Didomi shall set up the access controls necessary to ensure that any person accessing the Platform is actually in possession of an access code; (iii) Didomi reserves the right to change its hardware or software environment; and (iv) the Client acknowledges and agrees that Didomi may not be held liable for any such interruptions, failure or altered access to the Services or to the Platform as may result from the network itself, the features of the Internet, the Client's internet connection or any other external cause. The Client is informed of the technical issues that may affect the said network and may cause any slowdown or unavailability making the connection difficult or impossible. Didomi may not be held liable for any difficulty in accessing the Platform and the Services due to perturbations of the Internet. Technical support is available at: support@didomi.io from Monday to Friday, except on legal holidays (9:00 a.m./6:00 p.m. UTC+1). Didomi shall send to the Client an acknowledgement of receipt within two (2) business days from receipt by Didomi of a support request detailing the relevant issue, and agrees to provide its best efforts to provide appropriate technical support within a reasonable period after sending an acknowledgement of receipt, according to the difficulty and nature of the request. The technical support shall be provided in French or in English.

If the Client uses the Didomi API, Didomi may limit the quantity of requests that the Client can send through the API, as described on https://developers.didomi.io/api/introduction/rate-limiting, in order to avoid overloading the Services.

Article 3 : Didomi "Advanced Compliance Monitoring" Service

This Article applies only to the Didomi "Advanced Compliance Monitoring" (ACM) Service. In the context of ACM, "Support" means only the site(s) and excludes applications as well as online interfaces.

3.1. Description of the Didomi "Advanced Compliance Monitoring" Service

1. The Platform allows the retrieval of indicators and information related to the "Vendors" detected on the Client's Supports, including compliance scores with the regulations applicable to personal data; and according to the following three scenarios:

- End-user accepts all vendors and cookies,
- End-user declines all vendors and cookies,
- End-user makes no choice.

2. The Platform allows the retrieval of indicators and information related to the Client's trackers detected on the targeted domains in compliance with the regulations applicable to personal data in the following three scenarios

- End-user accepts all vendors and cookies,
- End-user declines all vendors and cookies,
- End-user makes no choice.

3. Only for Didomi notices - The Platform analyzes the implementation of the CMP and, in particular, the list of Vendors declared in the CMP. The Platform compares the declared Vendors with the active ones. The Platform also allows the Client to monitor the activity of certain Vendors.

4. A "weekly privacy report" sent on a weekly basis including the dimensions described below:

A - Vendor and trackers ecosystem evolution

1 - New trackers identification

2 - New Vendor identification

2.1 - Vendor breach

B - Last week privacy breaches

3 - Last week trackers activated without explicit choice

3.1 - 1st party trackers without explicit choice

3.2 - 3rd party trackers without explicit choice

4 - Last week trackers activated despite refusal

4.1 - 1st party trackers despite refusal

4.2 - 3rd party trackers despite refusal

"*Vendors*" means advertisers, third-party programmatic technologies that place cookies or other tracking devices on the end-user's browser in order to display relevant ads to potential customers. "Other Trackers" means pixels, web or local storage solutions.

3.2. Service Level Agreement "Advanced Compliance Monitoring"

In addition to those set in Section "Services", Didomi commits to the following service levels for the Advanced Compliance Monitoring Service:

- [Data collection]: As far as the collection of web related data is concerned, Didomi guarantees that the daily collections will be provided on a ninety-nine point nine (99,9) % monthly basis. In the event that this level of daily sampling is not met, Didomi will proceed to reimburse the amount paid in advance by the Client in proportion to the period during which the collection is unavailable.

- [Advanced Compliance Monitoring availability]: Didomi guarantees the availability of the Platform on a basis of ninety-nine (99) % on a monthly basis subject to any test or installation phase, and interruptions made necessary to ensure the repair or technical maintenance of hardware or software.

Article 4 : Payments and invoicing

In consideration for the Services and the Platform, the Client agrees to pay Didomi the amounts specified in the Purchase Order in compliance with the terms set out therein.

The price of the subscription may be revised according to the Monthly Unique Visitors grid set in the Purchase Order if the applicable threshold is exceeded during three (3) consecutive months. The revised price will apply from the fourth month. For clarification purposes, the price of the subscription can be reviewed upwards as set above, but if the Monthly Unique Visitors then drop after this change, the revised price will remain in force.

The initial period is invoiced on the Agreement Effective Date. In case of renewal of the Agreement, unless otherwise agreed by the Parties, invoices shall be issued each year at the beginning of the renewal period. Prices are firm for the first contractual period, and may be raised by a maximum of ten (10) % of the price of the previous contractual period at each annual renewal of the Agreement. As an exception to the above, Didomi may change the prices beyond this ceiling if the increase is notified to the Client in writing at least fifteen (15) days before the deadline for notification of tacit non-renewal by the Client as set out in the Article "Term and Termination". In case of renewal, Didomi shall issue an invoice within fifteen (15) business days from the anniversary date of the Effective Date. The Client agrees to settle any invoice within thirty (30) days from issuance. Any payment shall be made by the Client via AWS Marketplace.

In addition, if Client does not make payment when due, in addition to Didomi's rights herein, Didomi may charge interest on the unpaid amount, without any need to send any follow-up letter, as follows: (1) if the Client is a US or Canadian entity, at the lesser of 1.5% per month or the maximum rate allowed by law, or (2) if the Client is incorporated in the UK, the penalties for late payment as set out in the Late Payments of Commercial Debts (Interest) Act apply, or (3) if the Client is incorporated in any other country, in accordance with Article L. 441-10 of the French Commercial Code, penalties equal to three (3) times the statutory interest rate as well as an indemnity equal to forty (40) euro in collection expenses, without prejudice to any damages that might be claimed by Didomi on account of such late payment.

In the event Didomi incurs any costs (including reasonable attorney's fees) from efforts collecting overdue fees from Client, Client agrees to pay such costs.

If Client is a US entity, Client further agrees to pay all foreign, federal, states, and local taxes, if applicable, to Client's access to, use, or receipt of the Service. Didomi is only considered as having a sales tax nexus in the following States: Florida, New York, Utah and Colorado. Therefore, in all other States, Didomi is not considered as having a sales tax nexus in the Client's or User's State and is therefore not required to collect and remit sales tax on sales made to clients located or using the Services outside of the States aforementioned. Certain clients are required to file a sale and use tax return remitting any unpaid taxes. The Client is advised to refer to its tax advisor and to the regulations of the State where the Services are used, consumed, distributed, or stored to determine if it is required to file such returns. By default, invoices will be issued based on the assumptions that the Client does not have a Sales Tax Exemption Certificate nor a Sales Tax Multiple Points of Use Certificate, nor any other equivalent certificates. Therefore, Didomi will issue its invoices with the sales tax amount based on the invoicing address indicated on the Order Form. If the Client has a Sales Tax Exemption Certificate, a Sales Tax Multiple Points of Use Certificate, or any other equivalent certificate ("the Certificates"), it must provide it to Didomi before the starting date of the performance of the Services (the "Dates"). If Certificates are not provided before the Dates, the invoices will still be issued based on the invoicing address indicated on the Order Form.

All payments shall be made in US dollars, unless agreed otherwise in the Agreement.

Article 5 : Term - Termination

The Agreement shall enter into force on the Effective Date for the term stipulated in the Purchase Order. If no termination notice is sent by registered mail with return receipt requested at least three (3) months prior to the anniversary date of the Effective Date, then, unless otherwise agreed by the Parties, the Agreement shall be renewed tacitly for a further period of the same duration and be subject to the terms applicable during the initial period. Neither Party may terminate the Agreement prior to its expiration date, unless the other Party materially breaches any of its essential obligations (including, for the Client, any breach by any Beneficiary or User), provided that the terminating Party proves the alleged breach of one or more essential obligations by sending a registered mail return receipt requested, and provided that the said breach has not been cured within thirty (30) days from receipt of the said letter by the Party concerned. In addition, Didomi may suspend access to the Services and/or to the Platform if the Client, a Beneficiary or a User breaches any of the obligations incumbent on the Client under the Agreement, and in particular in case of late payment exceeding thirty (30) days from the payment's due date. In such an event, access to the Services and/or to the Platform shall be restored as soon as the payment proof is provided by the Client. Upon expiration or termination of the Agreement, howsoever arising, access to the Services and to the Platform shall be disabled. Upon written substantiated request from the Client or after the termination of the Agreement, Didomi agrees to delete from its live environments, as soon as practicable, any such information and documents owned by the Client as shall have been supplied by it, except however for (1) any documents or information whose retention or archiving is permitted or mandated by law, in particular as regards any archiving mandated by the Regulation and by the statute of limitations in civil and commercial matters (2) backups which are stored securely in compliance with industry standards, provided their access remains strictly limited to disaster recovery procedures or periodic tests as documented in Didomi's information security policies. Any expiration or termination shall be without prejudice to any obligations that, because of their nature, are to survive expiration or termination, and in particular any clauses related to liability, confidentiality, governing law and jurisdiction. The matter of Personal Data processed by Didomi upon expiry or termination of the Agreement is governed by the paragraph "Deletion of Data" in Section III of the Appendix containing the Personal Data Protection Agreement.

Article 6 : Confidentiality

Each Party agrees to treat as strictly confidential and not to disclose or communicate to third parties, by any means whatsoever, any Confidential Information transmitted to it by the other Party or that it may receive in connection with the execution of the Agreement, unless otherwise stipulated in the Agreement or instructed by the other Party. No Confidential Information disclosed by a Party may be used by the other Party for any other purpose than the performance of the Agreement. Any other use shall be subject to the prior written consent of the other Party. In particular, each Party agrees: (a) not to use the Confidential Information, directly or indirectly, for industrial, commercial or research purposes otherwise than under a future agreement with the other Party in the relevant area and/or strictly for the purposes of the Agreement; (b) not to duplicate, reproduce or copy all or part of the Confidential Information, unless the relevant action has been authorized by the other Party; (c) not to publish or use any Confidential Information on its own behalf or on behalf of any competing enterprise; (d) not to disclose, sell, transfer, license, market, assign or otherwise dispose of any Confidential Information in favor of any third party; (e) to ensure that each person to whom it has supplied such Confidential Information treats it as confidential; (f) to promptly inform the other Party of any actual or suspected unfair use, misappropriation or unauthorized disclosure of any Confidential Information. The above provisions shall survive for the duration of the Agreement between the Parties and for a period of five (5) years from expiration or termination thereof. However, the above confidentiality obligation shall not apply to any information in respect of which either Party is able to demonstrate that: (i) it was in possession of such information prior to its disclosure by the other

Party, or (ii) such information was available to the general public prior to its disclosure by the other Party or the said information became available to the general public without any negligence attributable to the other Party, or (iii) it received such information from a third party authorized to disclose the same and it was under no obligation to treat the same as confidential, or (iv) the disclosure of the Confidential Information was necessary to enforce its rights or to respond to a query from a government authority, court, statutory auditor or chartered accountant.

Article 7 : Security

Didomi agrees to provide its best efforts to provide secure access, retrieval and use of the Services and the Platform. However, Didomi does not warrant that the Services and the Platform can be used without any error or interruption. Didomi's obligation to ensure the security of the Services and the Platform and the security and confidentiality of any stored information shall in any event be a best efforts obligation, and Didomi cannot warrant absolute security. In the event of any security failure observed by Didomi capable of seriously compromising the security of the Platform and the Services, Didomi may temporarily interrupt without any prior notice the Services and/or the Platform in order to cure such security failure as soon as possible. The Client confirms that it is fully informed that the Client should (i) verify the quality and completeness of the Client's backups ; and (ii) complete multiple backups in compliance with the state of the art. As regards the security of any personal data collected on the Client's Supports in respect of which Didomi is acting as a processor, the Parties refer to the Appendix hereto.

Article 8 : Compliance with third-party integrations

This clause applies in case of subscription to the Consent Management Platform and if the Client expressly decides to activate any integration option in the Platform, such as TCF, Google Consent Mode or any other integration supported by Didomi.

Organizations responsible for these integrations, such as IAB for TCF, conduct regular audits of sites, mobile applications, and other media using their integrations and may sanction Didomi as well as all its clients if non-compliant media is identified. To protect its clients, Didomi therefore requires compliance with the standards of each integration from each of its clients using such integrations.

If the Client activates any such integration, it guarantees that it complies with the version of the integration standards used.

If the rules for any integration change:

- The Client undertakes to comply with them, as set out in the integration policy owner's timetable.
- The Client agrees that Didomi will make the necessary modifications to remain compliant.
- If the Client has made changes to the Didomi standard, the Client must make all necessary changes to remain compliant with the integration standards.

If the Client uses non-standard configuration settings (changes to banner text, buttons, etc.), the Client must notify Didomi and wait for Didomi validation prior to deployment. In any case, the Client warrants that its modifications are compliant with the version of the integration standard used.

The Client also undertakes not to use CSS/JavaScript or any means to override any compliance features/elements of the integrations.

If Didomi becomes aware (by its own means or upon notification from the relevant organization) of the Client's non-compliance with the integration standards or the use of Javascript/CSS to this effect, Didomi may notify the Client, who must comply within five (5) days of the notification. If the Client fails to comply within this time period, Didomi may disable the integration in the Services provided to the Client.

Article 9 : User License

9.1 Scope of the license

Didomi hereby grants a personal, non-exclusive, non-assignable and non-transferable right to use and operate (i) the Platform as accessible through the Account and (ii) any part of the Services protected by an intellectual property right, only for the purpose its operation on the Supports, during the entire term of the Agreement and for the entire world. In this context, the Client agrees that only duly authorized persons including the Beneficiaries and Users shall have access to the Services and the Platform, and that Didomi may presume in good faith that all instructions or queries received from the Client, any User or any Beneficiary originate from a person authorized by the Client. Therefore, the Client is solely responsible for any use of the Account(s), the Platform and the Services, and the Client agrees to bear any and all consequences arising from the use of the Services or the Platform, whether by itself or by any Beneficiary, User or third party using the Account(s). The Client shall be responsible for ensuring that the Beneficiaries and Users comply with the terms of the license and the Agreement. The Client, the Beneficiaries and the Users are authorized to use the Services and the Platform only in relation to the data owned by them or to any personal data in respect of which they are acting as data processors. Unless expressly authorized in writing by Didomi, the Client shall not – and shall not authorize any Beneficiary, User or third party to – (i) enable any third party not expressly authorized by Didomi to access the Services or the Platform, sublicense, sell, translate, loan, lease, distribute or use the Services or the Platform for the purposes of operating any IT services company, providing any (direct or indirect) access to the Services or to the Platform or using the Services or the Platform under any time-share arrangement; (ii) create any derivative works or access the Services or the Platform in order to develop any competing product or service or to copy any material, function or graphics of the Services or the Platform; (iii) retro-engineer, decompile, disassemble, reverse translate, seek to remove or circumvent any of the devices of the Services or the Platform, or seek to rebuild or discover the related source code; (iv) remove any material allowing for the identification of any copyrights or trademarks or any other indication pertaining to protected rights. When using Services and the Platform, the Client, the Beneficiaries and the Users agree not to upload, download, publish, send or circulate in any manner whatsoever any materials or contents: (i) breaching, whether intentionally or not, any applicable law or regulation; (ii) breaching any rights of third parties, including any intellectual property rights or personality rights; or (iii) likely to damage, disable, overload or impair the Services or the Platform or any server or networks connected to the Services or to the Platform, or to breach any requirements, procedures, rules or regulations of the networks connected to the Services.

9.2 Account

An Account shall be created (i) by Didomi at the request of the Client or any Beneficiary or User or (ii) by the Client or any Beneficiary or User by using the form accessible on the Platform's homepage. The various steps to be taken to open an Account are detailed in the said form. Prior to approving such form, the Client may check the supplied information and correct any misstatements and shall receive, as soon as practicable by email sent to the address specified in the form, an acknowledgement of receipt informing it that its sending has been taken into account. After verification of the supplied information, Didomi shall send an electronic mail containing the login information allowing for access to the created Account. The Client agrees not to use its login information for any purposes other than in order to use the Services and the Platform under the license so granted, and agrees to take any step necessary in order to protect the confidential and secure use of its connection data, in particular by avoiding to disclose or make them available to any third party. The Client shall also be responsible for protecting the confidentiality and security of the Account(s), and where applicable any Accounts of the Beneficiaries and Users, e.g. by regularly changing the relevant passwords. If the Client or any Beneficiary or User has any grounds for considering that its connection data (and in particular its identifiers and passwords) have been lost, stolen, or compromised in any manner whatsoever, or in case of unauthorized use of any Account, the Client shall immediately inform Didomi by any means of the relevant event. In such case, the Client authorizes Didomi to take any necessary steps to ensure the security of the Account, e.g. by resetting the passwords or temporarily suspending access to the Services and to the Platform. Absent any such notice, any use of the Account, the Platform and the Services shall be deemed to originate from the Client. The Client shall hold any rights in and to any contents created or generated on its Account in relation to its compliance with the Regulation (excluding the format or structure of the same as resulting from the

Platform). Didomi shall record and retain any contents created or generated on the Account, unless different instructions have been previously agreed with or imposed by the Client, it being understood that the Client shall be solely responsible for any deletion or modification of such contents by the Client or by any Beneficiary or User on its Account. Didomi may monitor, collect and use data pertaining to the use of the Services to extract, compile, synthesize, and analyze data or information resulting from Client's use of the Services or by visitors of the Client's Supports ("Statistical Data"). Didomi may only use Statistical Data for research, development (including to improve the Services and develop new products) and marketing purposes and may only publicly disclose such Statistical Data in an aggregated format that in no way identifies the Client, any particular person, and/or Client's confidential information. With regard to personal data collected on the Client's or Beneficiaries' Supports, and for which Didomi is a processor, this data is processed in accordance with the Appendix.

Article 10 : Personal data

The Client declares that it is aware and has informed the Users that Didomi collects and processes personal data of the Users (e.g. name, first name, position) in the course of managing the Agreement.

This collection is essential for Didomi to manage its relations with the Client and for marketing purposes.

The data protection officer may be contacted at dpo@didomi.io.

The persons whose data is collected have the right to access, oppose or rectify their own data, which the Client undertakes to inform the Users of. These rights can be exercised by contacting the data protection officer.

10.1. CMP and PMP Services

Any personal data collected on the Supports of the Client or the Beneficiaries, in respect of which Didomi is acting as a processor, shall be treated in accordance with the Appendix hereto.

10.2. Didomi "Advanced Compliance Monitoring" Service

Within the framework of the Didomi "Advanced Compliance Monitoring" service, Didomi does not process personal data as the Client's processor.

Article 11 : Intellectual property

The user license is granted to the Client only in strict compliance with the terms of the Agreement and shall not operate any transfer of intellectual property rights in or to the Services or the Platform. The Platform, the parts of the Services susceptible of being protected and the related Documentation shall be protected by the applicable intellectual property rights, as acknowledged by the Client. The organization, structure, sequences, logic and source code of such materials are trade secrets. Such materials and any copies and parts thereof, as well as any improvements, modifications and derivative works, and any intellectual property rights therein, are and shall remain Didomi's exclusive property. Except for the rights expressly granted under the license, Didomi shall hold and retain any and all rights, titles and interest related to the Platform and to the Services, to any database contained in the Platform and to any material related to the Services and to the Documentation. Didomi reserves the right to correct any possible errors.

Article 12 : Warranties and liabilities

Didomi warrants that the Client can use the Platform throughout the execution of the Agreement. In the event that Didomi considers that the Platform becomes or is likely to become the target of an infringement suit, the Client allows Didomi to, at Didomi's discretion, (i) to obtain the right to continue to provide the Platform, or (ii) to replace or modify the Platform so that it ceases being infringing, in order to enable the Client to keep using the Platform, or (iii) to terminate the right to use the Platform. This Article defines Didomi's full liability and the Client's sole right of recourse in relation to the infringement of any intellectual property right, and Didomi shall not assume any other liability in relation to any alleged or actual infringement. Didomi warrants that it is legally and contractually authorized to execute the Agreement. Didomi shall provide its best efforts to provide a correction or an alternative solution in case of any material and reproducible non-compliance of the Platform with the essential specifications set out in the Agreement. This warranty is applicable only insofar as the Platform is used in compliance with the Agreement, and no change is made thereto unless with Didomi's prior consent. The Client shall cooperate with Didomi and supply any information available to it in written form, so as to enable Didomi to reproduce and seek to correct any non-compliance. In the event that Didomi is unable to correct any material non-compliance and/or Didomi considers that such a correction is not reasonably feasible, Didomi and/or the Client may terminate the Agreement at no cost and without any indemnity. To the fullest extent permitted by law, the obligations described in this Article shall be Didomi's only obligations and responsibilities and are the Client's sole and only remedy in case of non-compliance. Save for the express stipulations above, the Services and the Platform are supplied on an "as-is" basis and without any other warranty. Didomi excludes and expressly disclaims any implied warranty of merchantability and fitness for a specific use and any other warranty, whether express or implied, resulting from any provision of law, other legal rule or trade practice. Each Client may publish any information through the Platform or through any Beneficiary or User under its own responsibility and agrees to ensure that the information is published in compliance with applicable laws and regulations. Didomi is under no obligation to review or verify the accuracy or completeness of any document, howsoever received, if the same is received through any Client, Beneficiary or User.

All set-up of the Services is under the Client's sole responsibility, as they are provided in a standard version. It refers notably and without limitation to the Client's selection of integration to use, as well as all API implementation by the Client.

DIDOMI MAY NOT BE HELD LIABLE FOR (I) THE QUALITY, ADVISABILITY OR COMPLETENESS OF THE CONTENTS OR THE EXISTENCE OF ANY CONFLICT OR REPETITIONS IN THE INFORMATION COMMUNICATED THROUGH OR IN CONNECTION WITH THE SERVICES OR THE PLATFORM (INCLUDING ANY ELECTRONIC MAILS, INDICATORS, WARNINGS AND ANY OTHER FORMS OF NOTICES RELATED TO THE SERVICES OR TO THE PLATFORM), (II) THE INTERPRETATION OF SUCH INFORMATION BY ITS INTENDED RECIPIENTS, AND (III) ANY STEP TAKEN, OMITTED OR TOLERATED ON THE BASIS OF INSTRUCTIONS, QUERIES OR GUIDELINES RECEIVED FROM ANY CLIENT, BENEFICIARY OR USER OR ON THE BASIS OF ANY OTHER DOCUMENT DELIVERED, SENT OR SIGNED BY ANY CLIENT, BENEFICIARY OR USER.

DIDOMI MAY IN NO EVENT BE HELD LIABLE FOR ANY INDIRECT LOSSES SUSTAINED BY THE CLIENT, THE BENEFICIARIES, THE USERS OR ANY THIRD PARTIES BECAUSE OF OR IN CONNECTION WITH THE AGREEMENT OR THE USE OF SERVICES OR THE PLATFORM. "INDIRECT LOSSES" MEANS IN PARTICULAR, BUT IS NOT LIMITED TO, ANY LOSSES OF GAINS OR PROFITS, COMMERCIAL DAMAGE, LOSS OF DATA (EXCEPT IF HOSTED BY DIDOMI), LOSS RESULTING FROM THE INABILITY TO USE ANY SOFTWARE, THE CONSEQUENCES OF ANY COMPLAINTS, ACTIONS OR THIRD-PARTY CLAIMS INSTITUTED AGAINST THE CLIENT, EVEN WHERE DIDOMI HAS BEEN INFORMED OF THEIR OCCURRENCE, EXCEPT FOR THE WARRANTIES GIVEN BY DIDOMI. IN ANY EVENT, SHOULD DIDOMI BE HELD LIABLE, ON ANY GROUNDS WHATSOEVER REGARDLESS OF THE LEGAL THEORY ASSERTED OR TAKEN INTO CONSIDERATION, DIDOMI'S TOTAL LIABILITY, FOR ALL LOSSES IN THE AGGREGATE, SHALL BE EXPRESSLY LIMITED AND MAY NOT, FOR ANY CONTRACTUAL YEAR, EXCEED EIGHTY (80) % OF THE TOTAL AMOUNT PAID BY THE CLIENT TO DIDOMI DURING THE CURRENT YEARLY PERIOD, AS STATED IN THE PURCHASE ORDER.

DIDOMI MAY IN NO EVENT BE HELD LIABLE IN CASE OF (I) USE OF THE SERVICES OR THE PLATFORM BY THE CLIENT, THE USERS OR THE BENEFICIARIES IN ANY MANNER NOT AUTHORIZED BY THE AGREEMENT; (II) USE OF ALL OR PART OF THE SERVICES OR THE

PLATFORM AT A TIME WHEN DIDOMI, FOLLOWING ANY DIFFICULTY OR FOR ANY OTHER REASON WHATSOEVER, HAD RECOMMENDED TO SUSPEND SUCH USE; (III) THE OCCURRENCE OF ANY DAMAGE RESULTING FROM ANY FAULT OR NEGLIGENCE OF THE CLIENT, ANY BENEFICIARY OR ANY USER OR OCCURRENCE OF ANY DAMAGE THAT COULD HAVE BEEN AVOIDED BY SEEKING DIDOMI'S ADVICE; (IV) USE, IN RELATION TO THE SERVICES OR THE PLATFORM, OF PROGRAMS NOT SUPPLIED OR ENDORSED BY DIDOMI AND LIKELY TO AFFECT THE SERVICES, THE PLATFORM OR THE CLIENT'S DATA.

Article 13 : Export control

If the Client is a US entity, the Client acknowledges and agrees that the Platform and/or Service are susceptible to be subject to the U.S. Export Administration Laws and Regulations. Client agrees that no part of the Platform and/or Service or information obtained through use of the Platform and/or Service, is being or will be acquired for, shipped, transferred, or re-exported, directly or indirectly, to proscribed or embargoed countries or their nationals, nor be used for nuclear activities, chemical biological weapons, or missile projects unless authorized by the U.S. Government. Proscribed countries are set forth in the U.S. Export Administration Regulations and are subject to change without notice, and Client must comply with the list as it exists in fact. Client certifies that neither Client nor any Users are on the U.S. Department of Commerce's Denied Persons List or affiliated lists or on the U.S. Department of Treasury's Specially Designated Nationals List. Client agrees to comply strictly with all U.S. export laws and assumes sole responsibility for obtaining licenses to export or re-export as may be required. Any unauthorized use of the Platform and/or Service may violate copyright laws, trademark laws, the laws of privacy and publicity, and communications regulations and statutes. The Service may use encryption technology that is subject to licensing requirements under the U.S. Export Administration Regulations, 15 C.F.R. Parts 730-774.

Article 14 : Miscellaneous provisions

14.1 Contents of the Agreement

This Agreement, together with the Purchase Order and Appendix annexed hereto, represent the parties' entire understanding relating to the use of the Platform and Service and supersedes any prior or contemporaneous, conflicting, or additional, communications. No text or information set forth on any purchase order form, preprinted form or document shall add to or vary the terms and conditions of this Agreement. For clarification, the Parties explicitly agree that the terms and conditions of purchase of the Client, if they exist and/or if they are included in a Client purchase order, do not apply to this Agreement.

Should any provision of the Agreement be held unlawful or unenforceable, prohibited or invalid, whether in whole or in part under applicable laws, such provision shall be disregarded only to the extent of its invalidity, and this shall not invalidate the remaining part of the said provision or the other provisions of the Agreement. In addition, the Parties refuse to assume the risk related to any change in circumstances unforeseeable upon the execution of the Agreement that makes the performance of either Party's obligations excessively onerous. In such situation, the Party concerned may request the renegotiation of the Agreement. The Parties agree to act in good faith in connection with any such renegotiation, under penalty of being held liable. Failing an agreement within sixty (60) days from activation of this clause, the Agreement may be terminated as a matter of law by either Party at no cost and without any indemnity.

14.2 Waivers

Neither Party's failure to seek from the other Party the performance of any obligation under the Agreement shall affect such Party's right to demand such performance at any later date. No failure to enforce any obligation stipulated in the Agreement shall be construed as a waiver in case of continuous or repeated breach of such obligation or as an amendment of the provision concerned.

14.3 Transfer of the Agreement

Neither Party may transfer any of its rights or obligations under this Agreement unless with the other Party's prior written consent. However, each Party is authorized to transfer its rights and obligations under this Agreement to the surviving entity in connection with any merger, transfer or business combination in which it is involved or to the buyer of all or substantially all of its shares or business. In addition, Didomi may subcontract all or part of its rights and obligations under this Agreement.

14.4 Communication

The Client authorizes Didomi, on a non-exclusive basis, free of charge and for the term of this Agreement, to use and affix its own trademarks and logos, and where applicable the trademarks and logos of the Beneficiaries, for the purposes of the supply of the Services. In addition, the Client authorizes, after the Effective Date, any publication in the press by which Didomi announces the execution of the Agreement. The Client authorizes Didomi to use its logo for the sole purpose of listing Didomi's clients on all marketing or commercial media, such as Didomi's website or any brochures. Should legal proceedings be brought against Didomi on any grounds whatsoever because of the use of the Client's trademarks and logos or because of the use of any document or information supplied by the Client, the Client expressly agrees to be responsible forthwith for any and all amounts, howsoever characterized, of any awards entered against Didomi, whether provisionally or finally, and the Client more generally agrees to remedy at its sole expense and risk any and all losses related to the institution and consequences of the above actions, and to carry out any and all works so that Didomi shall not suffer any loss. Didomi agrees to inform the Client as soon as practicable of the existence of any such actions and to communicate to the Client any additional information that the Client may request in order to be able to defend its own interests.

Article 15 : Governing law - Jurisdiction

The Agreement shall be governed by and construed in accordance with French law.

The Parties agree to submit any dispute or controversy arising in connection with the validity, interpretation, performance and/or termination of the Agreement to the exclusive jurisdiction of the Paris Commercial Court.

Notwithstanding the above:

- If the Client is located in Germany or Austria, the applicable law is German law, and the Parties elect to the jurisdiction of the Berlin courts.
- If the Client is located in the United Kingdom, the applicable laws are the laws of England and Wales, and the Parties elect to the jurisdiction of the London, England courts
- If the Client is a US company, any action related to this Agreement will be governed by New York law and controlling U.S. federal law. Any disputes, actions, claims, or causes of action arising out of or in connection with this Agreement or the Service shall be subject to the exclusive jurisdiction of the state and federal courts located in New York City, New York.
- If the Client is a Canadian company, any action related to this Agreement will be governed by Québec law and Canadian laws. Any disputes, actions, claims, or causes of action arising out of or in connection with this Agreement or the Service shall be subject to the exclusive jurisdiction of the state and federal courts located in Montréal, Québec.

DIDOMI

Annex 1 - Personal Data Processing Agreement

This Annex applies only to the CMP, PMP and DSAR Services, excluding the ACM Service.

Preamble :

Didomi provides its Clients with a solution commonly referred to as a "C*onsent management platform"* enabling the collection of consent from Data Subjects by the processing of their Personal Data and the remote management of compliance in terms of privacy and Personal Data. This solution collects consents and stores proof of consent from Data Subjects. It can be configured to integrate the IAB's *transparency and consent framework*. Didomi also offers a solution for collecting and storing Data Subjects' preferences, particularly in terms of communications.

The functionalities offered by Didomi's Consent Management Platform and Preference Management Platform are presented in Appendix 1 of this agreement and the related security measures in Appendix 2.

I. Purpose

The purpose of this appendix is to define the conditions under which the Data Processor (Didomi) undertakes to carry out the following Personal Data Processing operations on behalf of the Data Controller (the Client as identified in the Order Form or Agreement). As part of their contractual relationship, the Parties undertake to comply with the Regulation.

II. Role and qualifications

Didomi acts as the Client's Data Processor within the framework of the present Agreement, for the following Processing purposes:

- Collection and storage of consents from Data Subjects using the Client's Support and distribution of consent signals to the various partners declared by the Client
- Collection and storage of user preferences for the Client's Support.

Didomi also acts as an independent Data Controller for Data Processing carried out for the purposes of managing the commercial relationship with the Client.

Didomi also acts as Data Controller for the subsequent purposes set out below which are compatible with the initial purposes for which the Client's Data was processed:

- Drawing up and managing the Client's invoices,
- Statistical analysis,
- Improving Didomi's products and services.

The processing operations for which Didomi acts as Data Controller are described in Appendix 3 of this Agreement.

III. Description of the processing operation to be outsourced

The Processor is authorised to process, on behalf of the Data Controller, the Personal Data necessary to provide, depending on the service ordered by the Data Controller:

- (Service no. 1) the service for collecting consents on one or more Support determined by the Data Controller and storing the consents collected, as well as transmitting these consents to the partners declared in the CMP; and/or,
- (Service no. 2) the service for managing and storing the preferences and of persons using the Data Controller's Support
- (Service no. 3) the statistical analysis service for consent data collected in connection with the use of service no. 1.
- (Service no. 4) the Data Subject rights management service.

The Processing is carried out by the Processor in accordance with the instructions of the Data Controller below:

Service no. 1:

- **Scope, Nature and Purpose of the Processing of Personal Data**
    - Purpose and duration of Processing operations: The Parties have agreed that the Data Processor will Process Personal Data on behalf of the Data Controller to enable it to manage the consents of the users of its Support.
    - Scope of Processing and retention periods for Personal Data: Processing operations are carried out for the duration of the Agreement. The Personal Data processed on behalf of the Client is kept for a period of (5) five years from the date of its collection by the Processor in accordance with the limitation period referred to in article 2224 of the French Civil Code.
    - Nature and purpose of the Processing operations: The purpose of the Processing is to collect and store the consents of the Data Subjects who use the Client's Support and to transmit consent signals to the partners declared by the Client on the Platform. To this end, the nature of the Processing operations carried out is as follows:
        - the use of the IP address of the Data Subjects to determine the country in which they are located for the purposes of configuring the display of the banner and/or popup,
        - the collection and storage of privacy management choices,
        - The deposit of essential cookies aimed at authenticating people on the site in order to retrieve their privacy management choices,
        - the supply of information and aggregated statistics to the Data Controller concerning the choices made by individuals with regard to privacy management.
- **Categories of Personal Data and Data Subjects.**
    - Data Subjects: The Data Controller's Personal Data concerns the following categories of people: people who use the Client's Support.

- Categories of Personal Data: The Data Processor processes the following categories of Personal Data:
  - IP address, (to determine the country and region of the user and the regulations to be applied), the IP address is not stored or kept by Didomi.
  - User_ID (computer cookie identifier)
  - Consent of Data Subjects (purposes, partners, etc.)
  - Organization_user_ID: User ID supplied by the Client
  - Domain name or identifier of the application used
  - Browser information (User-Agent)
  - Timestamp
  - Other information relating to consent (method of consent, language, country, etc.)

Service no. 2

- **Scope, Nature and Purpose of the Processing of Personal Data**
  - Purpose and duration of Processing operations: The Parties have agreed that the Processor will Process Personal Data on behalf of the Data Controller to enable it to manage the preferences of users of its Support, particularly in terms of communications.
  - Extent of Processing and retention periods for Personal Data: the duration of Processing operations is that of the duration of the Agreement. The Personal Data processed on behalf of the Client is kept for a period of (5) five years from the date of its collection by the Processor in accordance with the limitation period referred to in article 2224 of the French Civil Code.
  - Nature and purpose of the Processing operations: the purpose of the Processing is to collect and store the preferences of Data Subjects who use the Client's Support. To this end, the nature of the Processing operations carried out is as follows:
    - the use of people's IP addresses to determine their country of location for the purposes of configuring the display of the Platform,
    - Collecting and storing preferences,
    - The deposit of essential cookies or the use of other tools (session token, email, telephone number, etc.) to authenticate users.
- **Categories of Personal Data and Data Subjects.**
  - Persons concerned: The Data Controller's Personal Data concerns the following categories of people: people who use the Client's Support.
  - Categories of Personal Data: The Data Processor processes the following categories of Personal Data:
    - The IP address is not stored or kept by Didomi.
    - User_ID (computer cookie identifier)
    - Preferences of the persons concerned
    - Organization_user_id: Identifier provided by the Client (e.g. internal customer ID, email address, telephone number, etc.)
    - Domain name or identifier of the application used
    - Browser information (User-Agent)
    - Other information relating to preferences (mode, language, etc.).

Service no. 3

- **Scope, Nature and Purpose of the Processing of Personal Data**
  - Purpose and duration of the Processing operations : The Parties have agreed that the Processor will Process Personal Data on behalf of the Data Controller in order to enable it to generate statistical analyses of the consents collected under service no. 1.
  - Scope of Processing and retention periods for Personal Data: Processing operations are carried out for the duration of the Agreement. Personal Data processed on behalf of the Client is kept for a period of (5) five years from the date of collection, in accordance with the limitation period referred to in article 2224 of the French Civil Code.
  - Nature and purpose of Processing operations : The purpose of the Processing is to carry out statistical analyses of the consents collected. This service is intrinsically linked to service No. 1. To this end, the nature of the Processing operations carried out is as follows:
    - Aggregation of data for statistical analysis.
- **Categories of Personal Data and Data Subjects.**
  - Persons concerned: The Data Controller's Personal Data concerns the following categories of people: people who use the Client's Support.
  - Categories of Personal Data: The Data Processor processes the following categories of Personal Data:
    - The IP address is not stored or kept by Didomi.
    - User_ID (computer cookie identifier)
    - Preferences of the Data Subject
    - Organization_user_id: Identifier provided by the Client (e.g. internal customer ID, email address, telephone number, etc.)

- Domain name or identifier of the application used
- Browser information (User-Agent)
- Other consent information (mode, language, country, etc.).

Service no. 4

- **Scope, Nature and Purpose of the Processing of Personal Data**

  - Purpose and duration of the Processing operations: The Parties have agreed that the Processor will Process Personal Data on behalf of the Data Controller in order to enable it to receive requests to exercise rights from Data Subjects using its Support and to manage their implementation.

  - Scope of Processing and retention periods for Personal Data: Processing operations are carried out for the duration of the Agreement. The Personal Data processed on behalf of the Client is kept for a period of five (5) years from the closure of the request.

  d) Nature and purpose of the Processing operations: The purpose of the Processing is to manage requests to exercise the rights of Data Subjects who use the Client's Support. To this end, the nature of the Processing operations carried out is as follows:
  - Receipt of the e-mail addresses of the Data Subjects
  - Reconciliation of the Data Subject's email address with their User_ID
  - Retention of the e-mail address of the Data Subject as well as the type of request made and the date on which the request was made.

- **Categories of Personal Data and Data Subjects.**
  - Persons concerned: The Data Controller's Personal Data concerning the following categories of persons: persons using the Client's Support who wish to exercise one or more rights relating to their Personal Data.

  - Categories of Personal Data: The Data Processor processes the following categories of Personal Data:
    - Email address of the person concerned (Organization_User_ID)
    - User_ID of the person concerned
    - right exercised
    - regulation linked to the right exercised
    - the user's location when making this request
    - date of request
    - request status
    - Any Personal Data linked to the user's e-mail address.

III. Obligations of the Processor to the Controller

The Processor undertakes to :

- process Personal Data solely for the sole purpose(s) for which it is contracted
- process Personal Data in accordance with the Data Controller's documented instructions, as provided in the Agreement and in the Services console. If the Processor considers that an instruction constitutes a breach of the Regulation or of any other provision of Union law or of the law of the Member States relating to data protection, it shall inform the Data Controller . In addition, if the Processor is required to transfer data to a third country or to an international organisation, by virtue of Union law or the law of the Member State to which it is subject, it must inform the Data Controller of this legal obligation prior to Processing, unless the law concerned prohibits such information on important grounds of public interest
- guarantee the confidentiality of Personal Data processed under this Agreement
- ensure that the persons authorised to process Personal Data under this Agreement (i) undertake to respect confidentiality or are subject to an appropriate legal obligation of confidentiality and (ii) receive the necessary training in the protection of Personal Data
- take into account, with regard to its tools, products, applications or services, the principles of data protection by design and data protection by default.

Ulterior Processor

The Processor is authorised to call upon the following entities (hereinafter, the "Ulterior Processor") to carry out the following activities:

- **Amazon Web Services EMEA SARL, Avenue John F. Kennedy 38, Luxembourg 1855, LUXEMBOURG**

Activity	Location	Supervision of any transfers	Documentation
Hosting	EU	N/A AWS joins the DPF	https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

- **Snowflake Computing Netherlands B.V, Gustav Mahlerlaan 300-314. 1082 ME Amsterdam, NETHERLANDS.**

Activity	Location	Supervision of any transfers	Documentation
Data analytics	EU	N/A Snowflake joins	https://www.snowflake.com/legal/data-processing-

		the DPF	addendum/

The Processor guarantees that Ulterior Processors present sufficient guarantees as to the implementation of appropriate technical and organisational measures so that the Processing meets the requirements of the Regulations and guarantees the protection of the rights of Data Subjects.

It is the responsibility of the initial Processor to ensure that the Ulterior Processor presents the same sufficient guarantees regarding the implementation of appropriate technical and organisational measures so that the Processing meets the requirements of the Regulation. If the Ulterior Processor fails to fulfill its data protection obligations (in particular the requirements of Article 28 of the GDPR), the initial Processor shall remain fully liable to the Controller for the Ulterior Processor's performance of its obligations.

The Controller grants the Processor general authorisation to call upon Ulterior Processors to carry out specific Processing activities. In this case, the Processor shall inform the Data Controller in advance and in writing of any changes envisaged concerning the addition or replacement of other Ulterior Processors. This information must clearly indicate the processing activities subcontracted and the identity and location of the subcontracted activities. This information is provided electronically by email and to the address https://www.didomi.io/sub-processors, which will be updated at least annually. The Data Controller may object to such subprocessing in writing within seven (7) calendar days of such information, in which case (i) if relevant, Didomi may propose any financially and technically reasonable alternative within seven (7) calendar days of such objection failing which (ii) either party may immediately and ipso jure terminate the contract subject to thirty (30) days' notice after sending a formal request to that effect by registered post with acknowledgement of receipt.

Transfers

The Controller grants the Processor a general authorisation to use subsequent Processors involving a transfer of Personal Data outside the EU and/or EEA subject to conditions:

- there is an adequacy decision from the European Commission indicating that the third country of destination provides protection equivalent to that granted by the GDPR,
- or that one of the appropriate safeguards referred to in Article 46 of the GDPR is implemented.

In this case, the Processor shall inform the Data Controller in advance and in writing of any change envisaged concerning the implementation of a new transfer. This information shall be provided electronically by email and to the address: https://www.didomi.io/sub-processors, which shall be updated at least annually. The Data Controller may object to the new transfer in writing within seven (7) calendar days of such notice, in which case (i) if relevant, Didomi may propose any financially and technically reasonable alternative within seven (7) calendar days of such objection failing which (ii) either party may immediately and ipso jure terminate the agreement subject to thirty (30) days' notice after sending a formal request to do so by registered post with acknowledgement of receipt.

Didomi may enter into standard contractual clauses with Ulterior Processors if legally required (module 3 of the standard contractual clauses would apply unless changes are made to them by the European Commission).

In the event that the Processor is required to make a transfer to a third country or an international organisation by virtue of the law of the European Union or the law of the Member State to which the Sub-processor is subject, the Processor shall inform the Data Controller of this legal obligation prior to processing, unless the law concerned prohibits such information for important reasons of public interest.

Exercising individual rights

Insofar as possible, the Processor must use appropriate technical and organisational measures to help the Data Controller fulfill its obligation to respond to requests to exercise the rights of individuals, such as the right of access and the right to have Data deleted. Where Data Subjects make requests to the Processor to exercise their rights, the Processor must forward such requests within five (5) working days of receipt by post to the address given in the quotation or to any e-mail address provided for this purpose by the Data Controller. Data Subjects may exercise their rights of withdrawal of consent and opposition directly on the Platform (Service no. 1 and Service no. 2); it being specified that the methods of opposition to Processing based on legitimate interest may be configured by the Data Controller on the Platform. In this case, the Data Controller must choose between two options:

- To allow Data Subjects to object to all Processing based on legitimate interest by clicking on the global refusal button;
- Allow Data Subjects to object granularly to the various Processing based on legitimate interest by clicking on "refuse" for each of the processing purposes or partners presented in the Platform; in this case, simply clicking on the global refuse button will not allow Data Subjects to object to said Processing based on legitimate interest.

Notification of Personal Data breaches

The Processor shall notify the Data Controller of any breach of Personal Data presenting a risk for the Data Subjects, within a maximum of forty-eight (48) hours of becoming aware of it by post to the address indicated in the quotation or to any email address provided for this purpose by the Data Controller. The Processor shall in this case use its best endeavours to provide the Data Controller with the information necessary to enable it to notify the competent data protection authority where required by the Regulations, namely :

- A description of the nature of the Personal Data breach including, if possible, the categories and approximate number of persons affected by the breach and the categories and approximate number of Personal Data records affected;
- A description of the likely consequences of the Personal Data breach;
- the measures taken or proposed to be taken by the Data Processor to remedy the Personal Data breach.

If all the necessary information is not available at the time of the initial notification, a supplementary notification will be sent as soon as the additional information is available.

The Parties have agreed that it is the Data Controller's responsibility to carry out notifications in the event that notification of the competent supervisory authority and/or the Data Subjects is required.

Assisting the Processor in ensuring that the Data Controller complies with its obligations

The Processor may provide the Data Controller with additional services aimed at carrying out data protection impact analyses and/or prior consultation with the supervisory authority and/or notification of breaches.

Security measures

The Processor undertakes to implement the appropriate technical and organisational measures in order to guarantee a level of security appropriate to the state of knowledge, the costs of implementation and the nature, scope, context and purposes as well as the risks, in accordance with Article 32 of the GDPR.

The security measures implemented by the Processor are provided in Appendix 2 of this Personal Data Processing Agreement. They may be updated by the Processor at any time.

Deletion of Data

On expiry or termination of the Agreement, the Data Controller may request the Processor to delete all Personal Data or, request additional services enabling all Data to be returned to the Data Controller or the Processor designated by the Data Controller. To do this, the Processor will allow, where technically feasible, the direct downloading of content and Personal Data from the Controller via the Account; alternatively, Didomi undertakes to provide the Controller with these elements in a commonly usable format (by default a json format) within fifteen (15) working days following a written request from the Client to this effect - fees may apply if the request involves the intervention of a consultant, if the requests are too frequent, if the request is too costly, or exceeds a simple extraction of content. This request may also be sent over the course of the execution of the Agreement and the same conditions apply. In the event of termination of the Agreement, the Client must send this request in writing no later than fifteen (15) days after the end of the Agreement. When the content and Personal Data are returned encrypted, a decryption password will be sent separately. In the absence of a data deletion request from the Data Controller, the Processor will retain the Personal Data until the expiry of the five (5) year period from the date of collection of said Data.

Documentation and audit

The Processor shall make available to the Data Controller the documentation necessary to demonstrate compliance with all of its obligations under this Personal Data Protection Agreement.

To this purpose, the Processor will also allow and contribute to a maximum of one (1) audit per contractual year to be carried out by the Data Controller or another auditor appointed by the Data Controller. These audits will be exclusively documentary, without any on-site audit, in the Processor's computer systems, or within the premises or computer systems of Ulterior Processors.

The audit will be subject to thirty (30) days' written notice by the Data Controller. It may be carried out by the Data Controller, or any person appointed by it, subject to an obligation of confidentiality at least equivalent to that of the Agreement, and not being a competitor of the Processor.

The audit report is submitted to the Processor for its opinion.

In the event of a non-compliance, the Parties will discuss how to remedy the situation. It is agreed, however, that the Data Controller may not impose any modification of the Services on the Processor. If the Parties fail to find an amicable solution to rectify the non-compliance within a reasonable period of time, the Data Controller has the right to terminate the Agreement unilaterally, by simple written notification, without penalty and with pro-rated reimbursement of sums paid in advance for the period during which the Agreement is terminated.

Each Party shall bear its own audit costs.

Record of processing activities

The Data Processor declares that it will keep and keep up to date a record of the Processing activities carried out on behalf of the Data Controller containing the information set out in Article 30.2 of the GDPR.

Contact details for the Data Protection Officer

In accordance with the Regulations, the Processor has appointed a Data Protection Officer whose contact details are as follows: dpo@didomi.io.

In the absence of a Client Data Protection Officer contact in the Order Form, the Client's billing contact email address given therein will be used for any notification relating to this Data Protection Agreement.

IV. Obligations of the Controller towards the Processor

The Data Controller undertakes to:

- Document in writing any instructions, or use the Services to provide any instructions, concerning the processing of Personal Data by the Processor;
- To inform Data Subjects in accordance with articles 12 et seq. of the GDPR (1) of the use of a Consent management platform to collect and store their consents and for the purposes of carrying out statistical analyses, involving the deposit of an essential cookie exempt from consent on their terminal, and/or (2) of the use of a Preference management platform to collect and store their Preferences.
- Comply with all applicable legislation and ensure that instructions comply with it;
- Process Personal Data in accordance with the applicable Regulations, including providing all necessary information;
- Notify Didomi if it learns that the Personal Data has become inaccurate or out of date.

The Data Controller remains fully responsible for ensuring that his choices and settings comply with the applicable Regulations.

California Consumer Privacy Act ("CCPA")

The Processor only discloses the personal information to third-parties if required to provide the Services, as detailed in the "Ulterior Processing" section.

The Processor does not sell the personal data provided by its Clients to third parties. Personal data is also not sold by the Clients to the Processor. The Parties therefore agree that do not sell requests are not applicable to the processor.

The Processor will assist the Data Controller, as required by the Regulation, to provide the Data Subject with their right to access, the right to delete and the right to opt-out, as follows:

- Right to access: the processor will list the categories and specific pieces of personal information collected, categories of sources from which the personal information is collected, the business or commercial purpose for which the personal data is collected, the categories of personal information that disclosed for a business purpose, any categories of personal information sold, the categories of third-parties with whom the personal information has been shared, and the business or commercial purpose for selling the personal information, if applicable.
- Right to delete: all data will be deleted or anonymized except data required to perform the Services, to maintain and/or upgrade the Services, to ensure the security of the Services, to comply with applicable laws.
- Right to opt-out: if applicable, the Processor will allow the Data Subject to opt-out of the sale of its personal data to third-parties.

The Processor will not discriminate against the Data Subjects for exercising any of its rights.

The Data Controller may ask the Processor for assistance at dpo@didomi.io. If a Data Subject directly sends a request to exercise its rights to the Processor, the Processor will forward the request to the controller.

The Processor will provide assistance to ensure that the request is responded to in the timeline and format mandated in the Regulation.

DIDOMI

Appendix 1: Functionalities of the consent management platform and the preference management platform.

I- Consent management platform (Service no. 1)

Consent collection and storage functionality (standard functionality)	Description of the function: This function enables the consent of Data Subjects using the Data Controller's Support to be collected and stored. Personal data processed: - User_ID (computer cookie identifier) - Consent of Data Subjects (purposes, partners, etc.) - Organization_user_ID: User ID supplied by the Client - Domain name or identifier of the application used - Browser information (User-Agent) - Timestamp - Other information relating to consent (method of consent, language, etc.)
Functionality for broadcasting consent signals to partners declared by the Client	Description of the function: This function enables consent signals to be transmitted to partners declared by the Client on the Platform. Personal data processed: - consent of data subjects (purposes, special functions/features, authorised partners, etc.) - Legal bases activated in the CMP
***Version and proof* feature** (premium feature)	Description of the function: This feature enables Clients to gather evidence of how consent was obtained at any time, as well as the history of their information notice configurations. This allows the Client to : - Generate proof in the event of an audit: to demonstrate how notification has been configured on your website for a given period, - Generate evidence in the event of complaints: to show a user the partners and purposes available in the notice when they have given their consent, - Solving problems relating to information notices: to study the differences between one published version and another, - Track published changes to information notices: easily track changes made to a notice by checking the comments made at the time of publication. Personal data transmitted : - User_ID - Organization_user_ID - consent of Data Subjects (purposes, partners, etc.) - Timestamp - Domain name or identifier of the application used - Country - Region - Browser information (User Agent) - Information on the operating system used
***Cross-device* functionality** (premium feature)	Description of the function: This feature enables a unified experience acro applications.

	Personal data processed: - Organization_user_ID - Consent of Data Subjects (Purposes, partners, etc.) - Browser information (User-Agent) - Timestamp
Batch export (premium feature)	Description of the function: This functionality enables the Client to access all the Consents of all the Data Subjects using its Support collected via Didomi's consent Management Platform in one go. Personal data transmitted : - User_Id - Organization_user_ID - Consent of Data Subjects (purpose, partners, etc.) - Domain name or identifier of the application used - Timestamp - Country - Region - Metadata
Analytics exports **feature** (premium feature)	Description of the function: This functionality provides access to the analytical data and metrics collected by the Didomi platform for the consent Management Platform (or "CMP"), in a single file. Personal data transmitted : No personal data is transmitted, only aggregated data. **When using this function, the Client undertakes not to attempt, by any means whatsoever, to re-identify the persons using its Support.**

II- Preference management platform (Service no. 2)

Functionality for collecting and storing preferences (standard functionality)	Function description: This function enables the preferences of Data Subjects using the Data Controller's Support to be collected and stored. Personal data processed: - User_ID (computer cookie identifier) - Preferences of the persons concerned - Organization_user_id: Identifier provided by the Client (e.g. internal customer ID, email address, telephone number, etc.) - Domain name or identifier of the application used - Browser information (User-Agent) - Other information relating to preferences (mode, language, etc.).
Batch export (premium feature)	Function description: This functionality allows the Client to access all the preferences of the users of its Support collected via Didomi's preference management platform in one go.

DIDOMI

	Personal data transmitted : - User_ID (computer cookie identifier) - Preferences of the persons concerned - Organization_user_id: Identifier provided by the Client (e.g. internal customer ID, email address, telephone number, etc.) - Domain name or identifier of the application used - Country - Metadata

DIDOMI

Annex 2: Security measures implemented by the Processor

The Processor maintains adequate and appropriate technical and organizational security measures to protect the confidentiality, integrity and availability of personal data. In addition, The Processor regularly reviews, maintains and updates its security measures to comply with all applicable laws and regulations.

The Processor restricts access to personal data to those authorized persons who need such information to deliver the services to the Controller under the agreement(s) or as required by law.

At all times during which the Processor or an authorized person has access to or retains personal data, the Processor complies, and causes each authorized person to comply with all applicable laws and regulations. The Processor ensures that all authorized persons complete adequate and appropriate privacy and data security training.

The Processor maintains the following policies and procedures in support of its privacy and security program:

Encryption:
Each application and environment use a specific TLS encryption protocol with secrets regularly renewed and managed by a key management system; no engineer has access to. All personal data collected is encrypted during its transit and during storage.

Anonymization:
Raw data (proof of consents) and analytics data are compartmentalized. Anonymization mechanisms provide safeguards against possible user re-identification in our analytic environments.
Except if our Client asks to store an organization user ID, we do not store any ID that can produce a cross domain identification.

Partitioning Data:
Logical data storage limits access and ensures confidentiality between customer organizations.

Logical access control:
User profiles are defined and attributed with appropriate means of authentication and respect the security rules applicable to passwords.

Monitoring network activity and traceability (logging):
The monitoring of events and logs allows threat detections, follow-ups and inquiries if needed.

Archiving:
The storage of data is subject to archive management to allow backup restoration.

Minimizing the amount of personal data:
IP address is processed but not stored by Didomi. Except if Client asks to, no unique ID that can produce a cross domain identification will be stored. Analytics data are anonymized or aggregated as soon and as often as possible. Regular access rights to raw data are limited to customer employees, the principle of least privilege is systematically applied and monitored for the Didomi teams.

Operating security:
Policies are in place to limit the risks related to the exploitation of information system infrastructures (updates, bug fixes and vulnerabilities).

Clamping down on malicious software:
Access to networks, and servers is protected against malicious software.

Website security:
Technical security measures applied to sites and data flows reduce the possibility of unauthorized use of personal data (including TLS encryption of flows, https restrictions, security audits and penetration tests).

Backups:
Backups ensure the availability and/or integrity of personal data, while protecting their confidentiality.

Maintenance:
Technical equipment is maintained to limit its failure, access for remote maintenance will be secured and authorized on a case-by-case basis.

Network security:
Adequate protection systems are positioned on the infrastructure, servers and network handling the data (including firewalls, intrusion detection probes, denial of service).

Monitoring network activity:
Monitoring systems are positioned on network to detect intrusions and suspicious activity.

Physical access control:
Physical access to the premises is secured and limited to authorized personnel.

Hardware security:
Measures to prevent personal data and customer data from being compromised or exposed to human or non-human risks are set up with cloud service providers.

Organization:
An organization leads and controls the security and the protection of personal data within the organization (including appointment of a DPO, Information Security Management System monitoring committee).

Managing privacy risks:
Incidents and business developments are analyzed to determine security and/or data protection risks in order to adapt security measures (privacy or security by design).

Personnel management:
Awareness-raising and training measures are taken when people take up their post. Security trainings are yearly followed by the whole company. Measures are taken when people accessing data leave.

Acquisition, development, and maintenance of systems:
Development and production are carried out only by authorized personnel in a secure process. The data used during the test phases are anonymized and cannot be consulted by unauthorized third parties.

DIDOMI

Business continuity management and recovery plan:
A business continuity plan is in place to ensure the availability of information processing facilities and systems.

Compliance:
An information systems security policy is in place, regularly updated and communicated to authorized personnel to ensure data security. Didomi is ISO 27001 certified and uses Only Certified Cloud Providers as ulterior processors.

DIDOMI

Appendix 3: Processing carried out by Didomi as Data Controller

I- Processing carried out for the purpose of managing the commercial relationship with the Client.

Didomi processes the Client's Personal Data, including that relating to the Client's employees (e.g. name, mobile phone number, email address), for the purposes of managing the commercial relationship (invoicing, order processing, etc.), complying with legal obligations and for security and business continuity purposes. This Processing is carried out for the execution of the Agreement and/or on the basis of Didomi's legitimate interests. This Personal Data is necessary to enable Didomi to fulfill its obligations under the Agreement. If the Client does not provide Didomi with the Personal Data, Didomi will not be able to fulfill its obligations under the Agreement. This Personal Data may be disclosed to Didomi's internal departments. In addition, Personal Data may be transferred outside the EEA, in particular to the United States on the basis of the Standard Contractual Clauses signed with Didomi's Ulterior Processors or the adherence of these Ulterior Processors to the *Data Privacy Framework*. This Personal Data will be kept for the duration of the Agreement and may be archived for documentary and/or evidential purposes.
In accordance with the applicable Regulations, Data Subjects have the right to access, rectify, erase, limit, oppose, request the portability of their Personal Data and the right to define directives concerning their Personal Data in the event of their death, as well as the right to lodge a complaint with the competent supervisory authority. The Data Subjects may exercise these rights by writing to: dpo@didomi.io.

Insofar as Didomi does not have a direct relationship with the Data Subject whose Personal Data is collected, the Client undertakes to provide its staff concerned by the Processing with all information relating to the Processing of their Personal Data for the purposes described above.

II- Processing carried out for the purposes of drawing up and managing the Client's invoices for the provision of Service no. 1

Purpose of processing	Drawing up and managing the Client's invoices
Type of treatment	Deduplication and counting
People concerned	Persons using the Client's Support
Personal data processed	Pages viewed, User_ID and/or Organization_User_ID
Legal basis	Legitimate interest

III- Processing for statistical analysis and improvement of Didomi products and services

Purpose of processing	Carrying out statistical analyses and improving products and services
Type of treatment	Aggregation of data for study and research purposes
People concerned	Persons using the Client's Support
Personal data processed	User_ID and/or Organization_User_ID encrypted,Type of device/tool used (computer, mobile),Type of browser used, Type of operating system used, Browser information (User-Agent), Country,Region, Date of consent, Consent (yes/no), Metadata
Legal basis	Legitimate interest

IV- Authorisation to re-use Personal Data entrusted by the Controller to the Processor

For the Processing referred to in paragraphs II to IV of this appendix, Didomi guarantees that the purposes are strictly limited to what is set out in the tables above. In this context, the Client grants Didomi permission to re-use the Personal Data entrusted to it for the subsequent purposes set out in paragraphs II to IV, which are strictly compatible with the initial processing purposes covered by the instructions given by the Data Controller.

DIDOMI

Annex 2 - Onboarding

The process varies depending on the monthly fee applicable to the Client (this table is provided for information purposes and Didomi may update it at its discretion):

MRR brackets in EUR

Client follow-up / Monthly fee (depending on currency)	**250-500 € 400-700 USD 400-800 CAD**	**500-1500 € 700 - 2000 USD 800-2000 CAD**	**>=1500 € >=2000 CAD/USD**	**>=10000 € >=10000 CAD/USD**
Kick-off Call	Didomi Academy Access	45 min	45 min	45 min
Onboarding follow-up calls	One 30min follow-up call	30min follow-up calls every 10 days *(during the time of the onboarding)*	Weekly 30min follow-up calls *(during the time of the onboarding)*	Weekly 30min follow-up calls *(during the time of the onboarding)*
Onboarding Duration	4 weeks	6 weeks	10-14 weeks	12-14 weeks
Follow-up	Account Manager	Account Manager	Account Manager	Account Manager
Support	Support team remains available at support@didomi.io or via the Console chat			