Fanplayr

Last Revised 3rd February 2023

FANPLAYR MEDIA SERVICES AGREEMENT

This Fanplayr Media Services Agreement (this "Agreement") is entered into as of the date of commencement of the Fanplayr Services at Your Website ("Effective Date") between Your Corporation ("You" or "Your") and Fanplayr Inc, 725 Alma Street, Palo Alto, CA 94301, USA ("Fanplayr").

1. **Definitions**
   a. "Fanplayr Portal" means the administration portal provided by Fanplayr for Your Account at http://portal.fanplayr.com/.
   b. "Fanplayr Service" means the Fanplayr web-based interactive onsite analytics, segmentation and targeting service for ecommerce and websites which allows display of personalized content and offers to Users based on their web browsing and online shopping behavior, demographics and other information and any other feature as described on http://www.fanplayr.com.
   c. "Fanplayr Tags" means the Javascript snippets as described on http://www.fanplayr.com/docs/ that when implemented on Your Website enable Fanplayr to track and target Your Users through the Fanplayr Service.
   d. "FP Offers" means Offers setup for use in the Fanplayr Service on Your Website.
   e. "FP Promo Code" means a promo code specifically allocated on the Fanplayr Portal for use in FP Offers.
   f. "Monthly Service Fees" means the monthly fees attributed to monthly campaign, application hosting, reporting, account management and analytics as set forth in Your Subscriber Agreement.
   g. "Offers" means offers in the form of promotional codes used on Your Website.
   h. "Offer Wallet" means the software that allows Users to accumulate store, retrieve and use FP Offers and FP Promo Codes.
   i. "Parties" means Fanplayr and You.
   j. "Service Fees" means the fees (if any) payable under Your Subscriber Agreement for consulting services from Fanplayr.
   k. "Set-Up Fees" means the fees (if any) attributed to initial set-up and integration of the Fanplayr Service as set forth in Your Subscriber Agreement.
   l. "Shopping Cart" means the online shopping cart software on Your Website that allows Users to purchase items.
   m. "Subscriber Agreement" means the subscriber agreement between You and Fanplayr (or a subsidiary or distributor of Fanplayr), and if no such agreement is signed the form of subscriber agreement set out in Schedule A.
   n. "Term" shall have the meaning set forth in Section 7.
   o. "Transaction Fees" means the fees (if any) set forth in Your Subscriber Agreement attributed to the of the value of each conversion or order including lead capture, and may include per message charges for SMS (exclusive of shipping and taxes), attributed to Fanplayr.
   p. "User" means a natural person who receives, views, or interacts with the features of Your Website.
   q. "User Data" means the User PI Data and User non-PI Data.
   r. "User PI Data" information that can be used on its own or with other information to identify, contact, or locate a single person, collected with respect to the Users of Your Website in connection with the Fanplayr Service.
   s. "User non-PI Data" means non-personally identifiable information collected with respect to Users of Your Website in connection with the Fanplayr Service.
   t. "Your Media" means Your copyrightable or trademarked images or text used on Your Website or added by You into the Fanplayr Service.
   u. "Your Website" means the website, e-commerce site, mobile site, or mobile application owned by You or under Your control which uses the Fanplayr Service.

2. **Fanplayr Services**
   a. Access to the Fanplayr Service.
   Following implementation of the Fanplayr Tags on Your Website:
      i. Fanplayr shall use commercially reasonable efforts to provide the Fanplayr Service in accordance with the instructions and directions provided via the Fanplayr Portal, and Fanplayr grants You permission to use the Fanplayr Service on a non-exclusive basis for Your Website;
      ii. you agree to provide access to Fanplayr to Your Website, and Your Shopping Cart for Fanplayr to provide the Fanplayr Services;
      iii. Fanplayr will provide the Fanplayr Service to You in accordance with Your Subscriber Agreement.

   b. Account and Passwords.
   The Fanplayr Service includes a mechanism that allows You to create an online account in order to manage the Fanplayr Service. You are solely responsible:
      i. for maintaining the confidentiality of account passwords,
      ii. for restricting access to Your account on the Fanplayr Service, and
      iii. for all activities that occur under Your account or passwords. If You have reason to believe that Your account is no longer secure (e.g., in the event of unauthorized disclosure or use of account credentials), You shall immediately notify Fanplayr by sending an email to support@fanplayr.com. You shall be liable for the losses incurred due to any unauthorized use of Your account on the Fanplayr Service.

3. **License by You**. You grant to Fanplayr the non-exclusive right to reproduce, distribute and use Your Media, in order to provide the Fanplayr Service. In addition, you grant Fanplayr the non-exclusive and royalty free right during the Term of this Agreement to use your name and trademarks, service marks or logos for the purpose of listing You as a customer of the Fanplayr Service, including on the Fanplayr website and marketing materials.

4. **Support.** Fanplayr shall use reasonable efforts to provide the support services with respect to the Fanplayr Service, in accordance with Your Subscriber Agreement with Fanplayr.

5. Data

a. Data Collection.

You authorize Fanplayr to process data (whether or not referable to an identifiable person) on your behalf for the purpose of this Agreement and you can choose where the data have to be processed. In the event that the provision of the Fanplayr Service requires the processing of "personal data" and triggers the application of the European General Data Protection Regulation EU 2016/679 ("GDPR"), Schedule B – Data Processing Agreement or Schedule C – Standard Contractual Clauses will apply, depending on where you chose to process the data (within the European Union or outside the European Union in a country with an adequate data protection legislation as for Schedule B or outside the European Union in a country without an adequate data protection legislation as for Schedule C). Where the application of the GDPR is not triggered, data protection legislation of your jurisdiction will apply,

You authorize Fanplayr:

i. to collect, consolidate, manipulate and analyze data (whether or not referable to an identifiable person) about Your Website and visitors that interact electronically with Your Website;

ii. to implement Fanplayr Tags, tracking pixels, cookies, or other tracking elements within Your Website;

iii. to collect data (whether or not referable to an identifiable person) from Facebook, other social media sites or other data services relating to Your Website;

iv. in accordance to Your documented instructions, to collect User Data, including e-mail addresses, SMS numbers, IP addresses, cookies data, web requests, browser type, browser language, referring / exit pages and URLs, platform type, number of clicks, domain names, landing pages, pages viewed and the order of those pages, features used, items placed in or removed from Users' Shopping Carts, Offers added to or used from Users' Offer Wallet, data relating to orders, the amount of time spent interacting with Your Offers and Your Websites, and all other data relating to user activity on Your Website, interaction data relating to emails and SMS messages, site speed data, data relating to social sharing of Offers on Facebook, Twitter or any other site, demographic data collected via Facebook, Twitter or any other site, the dates and times of requests, and other similar or related data; and

v. to use such data (whether or not referable to an identifiable person) for the purposes of the Fanplayr Service in accordance with Your documented instructions.

b. Reporting. Subject to the terms and conditions of this Agreement and in accordance with its Schedule B or Schedule C, Fanplayr shall use reasonable efforts to provide the reports with respect to Your use and use by Your Users of the Fanplayr Service, in accordance with Your Subscriber Agreement with Fanplayr.

c. Fanplayr Data.

i. You acknowledge and agree that all User Data (excluding any User Data provided directly by You to Fanplayr ("Your Data")) collected, produced, calculated or derived by Fanplayr in connection with its performance of this Agreement ("Fanplayr Data") will, as between You and Fanplayr, be the property of Fanplayr. In any case, this is subject to the anonymization of all User PI Data or making them irreversibly not referable – on its own or in connection with other data – to any identifiable person and You expressly authorize this.

ii. You may request from Fanplayr, an electronic file of the Fanplayr Data at Fanplayr's then current prices. Within 14 days of receiving payment, Fanplayr will provide You with such electronic file and grant You a perpetual, non-exclusive license to use such data solely for Your internal business purposes.

iii. You agree not to use Fanplayr Data for any other purpose or in any other manner that violates applicable law.

d. Fanplayr's Use of User Data. Fanplayr shall not sell or otherwise use or distribute User Data collected at Your Website to, or share that User Data with, anyone other than You, except: (i) in connection with its performance of the Fanplayr Service and to improve the Fanplayr Service; and (ii) in anonymized, blinded formats that do not identify, reference or imply an association with You, for the purposes of creating benchmarking, statistical, research and marketing analyses, surveys, reports and studies. User Data may be used to access extended data from third party services for delivering add-on Fanplayr services to You and Users of Your Website.

Privacy Policies. You will post on Your website Your privacy policy and adhere to Your privacy policy, which will be consistent with applicable laws, including the GDPR.
Failure by You to continue to post a privacy policy, or non- adherence to such privacy policy, is ground for immediate termination of this Agreement by Fanplayr.

e. Data Retention. You and Fanplayr agree that Fanplayr shall not be obligated to retain Fanplayr Data, unless otherwise required to do so by law, after the termination or expiration of this Agreement.

6. Ownership

Nothing in this Agreement shall be deemed an assignment of a Party's pre-existing intellectual property rights.

a. Fanplayr owns, and shall own, all right, title, and interest, including all intellectual property rights, in and to the Fanplayr Service and associated technology, software, and documentation, including any improvements, modifications, and enhancements made or provided by or on behalf of Fanplayr, or utilized by Fanplayr in performing the Fanplayr Services, the Fanplayr Data and all intellectual property rights with respect thereto (excluding only Your Media) (along with Fanplayr's Confidential Information, collectively the "Fanplayr IP"). Fanplayr reserves all right, title and interest in and to the Fanplayr IP not expressly granted to You herein.

b. You own, and shall own, all right, title, and interest, including all intellectual property rights, in and to Your Media, Your Websites, technology, software, and hardware owned by the You, including any improvements, modifications, and enhancements made or provided by or on behalf of You and all of its intellectual property rights with respect thereto (excluding the Fanplayr IP) (along with Your Confidential Information, collectively "Your IP"). You reserve all right, title and interest in and to Your IP not expressly granted to Fanplayr herein.

c. In the event that You provide feedback to Fanplayr concerning the functionality and performance of the Fanplayr Service (other than any feedback which You designate in writing at the time it is provided as being Your IP) You grant to Fanplayr and its successors and assigns an unlimited, perpetual, irrevocable, worldwide, nonexclusive, royalty free, fully paid, transferable, sub-licensable license to use, and incorporate that feedback into the Fanplayr Service, and to otherwise improve that service.

7. Fees and Payment

a. Fees. You agree to pay Fanplayr the fees specified in Your Subscriber Agreement with Fanplayr, including any Set-Up Fees, Transaction Fees, Service Fees, and Monthly Fees (collectively, the "Fees").

b. Payment.

i. Payment Information. Registration for the Fanplayr Service or Your Subscriber Agreement may require You to submit to Fanplayr online payment information service account ("Payment Account") or credit card information. You agree that by submitting such Payment Account or credit card information, Fanplayr is authorized to charge such Payment Account or credit card the Fees due and You agree to pay the same.

ii. Timing of Payment. Any Set-Up Fees will be billed and charged upon completion of that work. Transaction Fees and Monthly Fees will be billed and charged at the end of each calendar month in arrears, payable within 15 days of invoice (or as otherwise specified in the Subscriber Agreement). You will make payment of invoices for customization and other services in advance prior to commencement. Past due amounts will accrue interest at a rate of one and one half percent (1.5%) per month.

c. Calculation of Conversion and Transaction Fees and Use of Promo Codes.

i. To calculate the monthly Transaction Fees, Fanplayr may track purchases that use FP Promo Codes that are displayed to the on-site shopper by a Fanplayr banner or widget. Fanplayr recommends the use of a consistent format for these FP Promo Codes and will provide such format to You prior to the launch of the first campaign.

ii. Fanplayr will not refund any Fees charged to You because of Your use of a general promotional code that is identical to a FP Promo Code.

iii. Although the Fanplayr service contains features that provide for security for FP Promo Codes, these features are optional, and Fanplayr will not be responsible for the unintended distribution of FP Promo Codes.

iv. Additionally, further definitions of what a conversion attributable to Fanplayr is can be specifically defined as part of Your Subscription Agreement, in accordance with the features of the Fanplayr service You are subscribing to.

v. SMS message fees, email fees and web push notification fees shall be charged by Fanplayr in accordance with your Subscription Agreement.

8. Confidentiality.

a. Definitions. "Confidential Information" includes any and all information or data of a Party ("Discloser") that is disclosed to the other Party ("Recipient"), either directly or indirectly, whether in writing, verbally, or by visual means, and which is designated (either in writing or verbally) as confidential, proprietary, or the like. However, such designation shall not be necessary to deem information as Confidential Information if the nature of the information makes it generally considered confidential including relating to: (1) Fanplayr Data, (2) trade secrets or know-how, (3) finance or accounting, (4) technology, research, or development, (4) internal processes or procedures, (5) algorithms, digital data, or designs, (6) business, operations, or planning, (7) sales or marketing strategies, and (8) the terms of the Subscriber Agreement related to payment, pricing or consideration, and the discussions, negotiations, or related proposals.

b. Exceptions. "Confidential Information" will not include information which: (1) was previously known to Recipient, (2) was or becomes generally available to the public through no fault of Recipient, (3) was rightfully in Recipient's possession free of any obligation of confidentiality at, or prior to, the time it was communicated to Recipient by Discloser, (4) was developed by employees or agents of Recipient independently of, and without reference to, Confidential Information, or (5) was communicated by Discloser to an unaffiliated third party free of any obligation of confidentiality.

c. Obligations. Recipient will protect Confidential Information in the same manner that it protects its own information of a similar nature, but in no event with less than reasonable care. Recipient shall not disclose Confidential Information to anyone except an employee, agent, affiliate, or third party who has a need to know same, and who is bound by confidentiality and non-use obligations at least as protective of Confidential Information as are those in this section. Recipient will not use Discloser's Confidential Information other than as provided for in this Agreement. Notwithstanding the foregoing, the Recipient may disclose Confidential Information of the Discloser in response to a valid order by a court or other governmental body, as otherwise required by law or the rules of any applicable securities exchange, or as necessary to establish the rights of either Party under this Agreement; provided, however, that both Discloser and Recipient will stipulate to any orders necessary to protect such information from public disclosure.

9. Term andTermination.

a. This Agreement will remain in effect from the Effective Date and during the term of the Subscriber Agreement or (if applicable) for such additional period during which You use the Fanplayr Service.

b. Fanplayr reserves the right in its sole discretion and at any time to upon notice in writing to You to modify or discontinue providing the Fanplayr Service, or any part thereof.

c. Either party may terminate this Agreement for any breach by the other party of any of its obligations hereunder which breach is not cured within thirty (30) days written notice by the non-defaulting party.

d. The provisions of Sections 3, 4, 5 (for amounts owing accrued during the Term), 6, 7, 8, 9, 10, 11, 12 and 13 shall survive termination.

10. Fanplayr Service Restrictions and Limitations.

a. You agree not to: (1) interfere with or disrupt the integrity or performance of the Fanplayr Service, (2) attempt to gain unauthorized access to the Fanplayr Service or its related systems or networks, (3) use the Fanplayr Service or access to the Fanplayr Service for the purpose of reverse engineering or copying all or part of the Fanplayr Service, or producing or contributing to a service or product which is or is likely to be in any way competitive to the Fanplayr Service, (4) intentionally or unintentionally violate any applicable local, state, national, or international law in connection with Your use of the Fanplayr Service, (5) resell the Fanplayr Service (or information derived therefrom) without the prior written consent of Fanplayr, or (6) send messages, emails offers or promotions on behalf of third parties where You do not have legal authority to bind such third party.

b. You agree that: (1) You have and will maintain throughout the Term of the Agreement adequate rights in and to Your Media (including without limitation under the intellectual property rights in and to any third party content contained therein) in order to use Your Media in connection with the Fanplayr Service, (2) Your Website, Your Offers and content will not portray or promote illicit drugs; and do not contain pornography, adult or mature content or any content that otherwise promotes violence, illegal activity or infringes on the rights of others, and (3) you will comply with Fanplayr's acceptable use policy for the Fanplayr Service (if any) as may be promulgated and amended by Fanplayr from time to time and posted on the Fanplayr website.

c. You and Fanplayr will at all times comply with all international, federal, state, and local laws, ordinances, regulations, and codes which are applicable to each Party's performance of their respective obligations under this Agreement. By providing Your Data, and permitting Fanplayr access to Your Media in order to provide the Fanplayr Service, You represent and warrant that Fanplayr's use of Your

Data and Your Media as provided herein complies with Your privacy policy, and will not violate any agreements with third parties, applicable law (including CAN-SPAM) or applicable privacy policies.

d. The Fanplayr Service includes a mechanism that allows You to create and offer coupons and other incentives to Users as part of Your Offers. You are solely responsible for creating the terms of, and honoring, Your Offers, and ensuring that Your Offers are compliant with the law. Your Offers should represent a reasonable discount for a product or service purchase or a small incentive to increase customer traffic and conversion, but not represent an opportunity for a material giveaway or reward to any individual.

e. Fanplayr will determine the timing and frequency of personalized content and Offers to selected groups of visitors as determined by a set of parameters selected in the Fanplayr Portal.

f. Fanplayr reserves the right not to display a small percentage of personalized content or Your Offers or Your content to Your Users for the express purpose of monitoring and optimizing performance, through AB testing.

11. Warranties and Disclaimer.

a. By You. You represent and warrant that (i) all information provided by You at the time of registration is complete and accurate in all respects and that You shall promptly update this information so that it is complete and accurate in all respects throughout the Term;
(ii) You have the necessary rights to use and to permit the use of Your Data and Your Media; and (iii) You are in compliance with, and shall not violate any applicable law, including without limitation privacy and data protection laws and regulations, or your internal privacy policies, in connection with the collection, use or processing of User Data. In the event of a breach or reasonably anticipated breach of the foregoing warranties, in addition to any other remedies available at law or in equity, Fanplayr will have the right to immediately, in its sole discretion, suspend the Fanplayr Service if deemed reasonably necessary by Fanplayr to prevent any liability accruing to it.

b. By Fanplayr. Fanplayr represents that it will provide the Services in a professional manner consistent with applicable industry standards.

c. The Fanplayr Service is controlled and operated by Fanplayr from its offices within the State of California USA and its other offices as listed on http://www.fanplayr.com/contact/. Fanplayr makes no representation that materials on the Fanplayr Service are appropriate or available for use in other locations. Those who choose to access or use the Fanplayr Service from other locations, do so on their own initiative and are responsible for compliance with local laws, if and to the extent local laws are applicable.
Access to the Fanplayr Service from jurisdictions where the contents or practices of the Fanplayr Service are illegal, unauthorized or penalized is strictly prohibited.

The Fanplayr Service may include certain sample language regarding coupons that may be included in Your Offers, and certain other sample language regarding the privacy of Users and legal disclaimers for Your Offers. You are free to modify or alter such sample language. Fanplayr makes no representation or warranty that such sample language, are compliant with all applicable legal requirements, will be sufficient to limit Your liability under applicable law or otherwise will meet Your needs. Your use of such sample language is at Your own risk; PLEASE CONFER WITH YOUR OWN LEGAL COUNSEL REGARDING SUCH MATTERS.

d. EXCEPT AS SET FORTH IN THIS SECTION 9, THE FANPLAYR SERVICE, THE FANPLAYR DATA, FANPLAYR

IP AND OTHER MATERIALS AND SERVICES PROVIDED BY FANPLAYR HEREUNDER, INCLUDING THE RESULTS ACHIEVED BY YOUR USE OF THE FANPLAYR SERVICE ARE, AND LEGAL TERMS THAT ARE INCLUDED AS DEFAULT LANGUAGE IN YOUR OFFERS, TO THE FULLEST EXTENT PERMITTED UNDER APPLICABLE LAW, PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OUT OF A COURSE OF DEALING OR USAGE OF TRADE, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, MERCHANTABLE QUALITY, FITNESS FOR ANY PARTICULAR PURPOSE OR USE, NONINFRINGEMENT, QUALITY, ACCURACY, PRODUCTIVENESS OR CAPACITY AND SATISFACTORY RESULTS. FANPLAYR AND ITS SUPPLIERS AND LICENSORS HEREBY DISCLAIM ALL SUCH WARRANTIES. FANPLAYR DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE FANPLAYR SERVICE WILL BE CORRECT, UNINTERRUPTED OR ERROR-FREE, THAT DEFECTS WILL BE CORRECTED, OR THAT THE FANPLAYR SERVICE IS FREE OF HARMFUL COMPONENTS. FANPLAYR MAKES NO GUARANTEE REGARDING THE NUMBER, QUALITY, OR CONTENT OF YOUR OFFERS OR THE TIMING OF DELIVERY OF YOUR OFFERS. YOU UNDERSTAND AND ACKNOWLEDGE THAT THERE IS NO GUARANTEE THAT ANY MINIMUM LEVEL OF REVENUE, OR ANY REVENUE, WILL BE GENERATED AS A RESULT OF THIS AGREEMENT AND YOUR USE OF THE FANPLAYR SERVICE.

12. Limitation of Liability.

THE TOTAL LIABILITY OF FANPLAYR ARISING OUT OF OR RELATED TO THIS AGREEMENT SHALL NOT EXCEED THE FEES PAID BY YOU TO FANPLAYR IN CONNECTION WITH YOUR USE OF THE FANPLAYR SERVICE DURING THE ONE (1) YEAR PERIOD IMMEDIATELY PRECEDING THE DATE THE CAUSE OF ACTION AROSE AND IN NO EVENT SHALL FANPLAYR HAVE LIABILITY FOR ANY LOSS OR CONSEQUENTIAL, INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL, OR EXEMPLARY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATIONS, DAMAGES FOR LOSS OF PROFITS OR REVENUES, BUSINESS INTERRUPTION, LOSS OF INFORMATION, AND THE LIKE), WHETHER UNDER TORT, CONTRACT OR OTHER THEORIES OF RECOVERY, EVEN IF FANPLAYR KNEW OR SHOULD HAVE KNOWN OF THE POSSIBILITY OF SUCH DAMAGES. THESE LIMITATIONS SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY. THE PARTIES AGREE THAT THE FOREGOING LIMITATIONS REPRESENT A REASONABLE ALLOCATION OF RISK UNDER THIS AGREEMENT.

13. Indemnification.

a. By You. You will defend, indemnify, and hold harmless Fanplayr from damages, liabilities, costs, and expenses (including reasonable attorneys' fees) (collectively, "Losses") resulting from any claim, judgment, or proceeding (collectively, "Claims") brought by a Third Party and resulting from any claim or allegation: (a) that Your Website, Your Offer(s) and/or Your use of the Fanplayr Services (1) violate any applicable law, regulation, judicial or administrative action, or the right of a third party, or (2) are fraudulent, misleading, defamatory or obscene, or (3) are otherwise in breach of this Agreement; (b) related to Your breach of Sections 8 and/or 10, or 11(a) ; and/or
(c) that Your Website, Your Media and/or Your Data infringes or misappropriates the intellectual property rights of any third party.

b. By Fanplayr. Fanplayr will defend or at its option settle any Claim brought against You to the extent it alleges that the Fanplayr Service infringes any third party's intellectual property rights.

c. Process. The indemnified Party will promptly notify the indemnifying Party of all Claims of which it becomes aware (provided that a failure or delay in providing such notice will not relieve the indemnifying Party of its obligations hereunder except to the extent such Party is prejudiced by such failure or delay), and will: (i) provide reasonable cooperation to the indemnifying Party at the indemnifying Party's expense in connection with the defense or settlement of all Claims and (ii) be entitled to participate at its own expense in the defense of all Claims. The indemnified Party agrees that the indemnifying Party may have control over the defense and settlement of all third party Claims; provided, however, the indemnifying Party will not acquiesce to any judgment or enter into any settlement, either of which imposes any obligation or liability on the indemnified Party without its prior written consent.

14. Force Majeure.

Excluding payment obligations, neither Party will be liable for delay or default in the performance of its respective obligations under this Agreement if such delay or default is caused by conditions beyond its reasonable control, including, but not limited to, fire, flood, accident, earthquakes, telecommunications line failures, electrical outages, network failures, pandemics, acts of God, or labor disputes ("Force Majeure Event"). If a Force Majeure Event has continued for five (5) business days, Fanplayr has the right to cancel the Agreement effective upon notice.

15. Miscellaneous.

a. Neither Party may resell, assign, or transfer any of its rights or obligations hereunder, and any attempt to resell, assign, or transfer such rights or obligations under this Agreement without the other Party's prior written approval will be null and void. Notwithstanding the foregoing, Fanplayr may assign or transfer this Agreement in connection with a merger, sale of assets, reorganization and or reincorporation of Fanplayr.

b. Subject to the foregoing, this Agreement will be binding upon and inure to the benefit of the Parties hereto and their respective permitted transferees, successors, heirs and assigns.

c. This Agreement (including information linked thereto and incorporated by reference) will constitute the entire agreement of the Parties with respect to the subject matter thereof and supersedes all previous communications, representations, understandings, and agreements, either oral or written, between the Parties with respect to the subject matter.

d. The relationship between the Parties will be that of independent contractors, and this Agreement will not in any way create or be deemed to create any agency, partnership, or joint venture between the Parties.

e. This Agreement and Your Subscriber Agreement will be governed by the laws of the State of California, without reference to its conflict of law principles. The Parties agree that any claims, legal proceedings, or litigation arising in connection with the Agreement hereunder will be brought solely in Santa Clara County, California, and the Parties consent to the exclusive jurisdiction of such courts.

f. No modification of this Agreement or Your Subscriber Agreement will be binding unless in writing and signed by both Parties. No waiver or modification of this Agreement or Your Subscriber Agreement shall be valid unless in writing signed by each Party.

g. The waiver by either Party of any default or breach of this Agreement or Your Subscriber Agreement will not constitute a waiver of any other or subsequent default or breach.

h. If any provision herein is held to be unenforceable, the remaining provisions will remain in full force and effect.

i. All rights and remedies hereunder are cumulative.

j. Section or paragraph headings used in this Agreement are for reference purposes only, and should not be used in the interpretation hereof.

k. The singular includes the plural and vice-versa. A reference to one gender includes any gender. A reference to a grammatical part of speech includes all other parts of speech.

l. Any notice required to be delivered hereunder will be deemed delivered three days after deposit, postage paid, in U.S. mail, return receipt requested, one business day if sent by overnight courier service, and immediately if sent electronically with receipt confirmed. All notices to You shall be sent to the addresses provided at the time of registration (as may be updated by You from time to time) and all notices to Fanplayr will be sent to the address in the first paragraph of this Agreement (as may be updated by Fanplayr from time to time).

Should you have any questions concerning this Agreement, or if you desire to contact Fanplayr for any reason, please contact support@fanplayr.com

SCHEDULE A

Standard Form Subscriber Agreement

This applies if no signed Subscriber Agreement is entered into between You and Fanplayr (or its subsidiaries or distributors)

SUBSCRIPTION AGREEMENT

A. Recitals

This Subscription Agreement ("Agreement") is made between Fanplayr Inc. ("Fanplayr"), and the "Client" listed below, for implementation and execution of the Fanplayr Service ("the Service") on the Client's website(s) listed below ("the Site"), subject to the Media Services Agreement and Privacy Policy available at https://fanplayr.com/legal.

"FANPLAYR"
Fanplayr Inc.
725 Alma St
Palo Alto, CA, 94301
USA

"CLIENT" (Company Name):

Client's Site:

Bill To Address:

VAT No.:

Billing Contact:

Billing Contact email:

eInvoicing (if applicable):

Purchase Order No. (if applicable):

B. Services

Fanplayr agrees to provide the following services:

1. Undertake data collection on the Site;
2. Provide the Service to the Client for use on the Site, which includes use of the features described in section D of this Agreement and access to the Fanplayr Portal for their management;
3. Support ongoing operations of the Service on a continuous basis (7 days a week, 24 hours a day) using system resources;
4. Provide a reasonable response via phone or email from designated support staff members.

Support from Fanplayr staff members is included in the services for up to 10 hours per 1 million monthly visitors' sessions per month.

C. Integration

The Client will integrate Fanplayr into its Site using a custom-built integration developed by its own Development Team. Fanplayr will provide support in all the steps of the integration process.

D. Features

Fanplayr agrees to provide the following features as part of the Service:

- Behavioral Analytics Dashboard (Insights);
- Real Time Segmentation;
- On-site Targeting with Personalized Offers and Messages;
- Streams (Integration with 3rd party applications such as Email Service Providers, SMS Providers, etc.);
- Web Push Notifications;
- Product Recommendations;
- Product Rankings;
- Personalized SMS;
- Site Speed Analytics.

E. Term Of Engagement

The initial term of this Agreement shall be valid as of_____________(the "Effective Date") and for a term of 12 months (the "Initial Term").

The billable term of this Agreement will commence on the date that the Fanplayr tags are installed on the Site and data collection is confirmed.

Upon the expiration of the Initial Term and any Renewed Term, this Agreement will automatically renew for a further term of the same duration as the Initial Term ("Renewed Term"), unless any of the Parties gives notice in writing of their will to cancel the Agreement, one month prior to the date of expiration of the Term. In the event of cancellation by the Client, the Client agrees to pay Fanplayr a termination fee equal to all Fees (as such term in defines in the next section F) that would have been payable for each month remaining of the Term. In this Agreement "Term" means Initial Term and any Renewed Terms.

F. Pricing

The Client agrees to pay Fanplayr a one-time set-up and integration fee of $ 0 plus the applicable value added tax, payable on the first invoice to the Client (“Integration Fee”).

Fanplayr will provide integration support at the following rates:

1. 1 day to 30 days after the Effective Date – $ 0 additional charge plus the applicable value added tax;
2. 31 days to 60 days after the Effective Date – $ 5,000 additional charge plus the applicable value added tax;
3. 61 days or more after the Effective Date – $ 5,000 additional charge plus the applicable value added tax.

The Client agrees to pay Fanplayr the following fixed monthly fees for the usage of each of the following features (“Fixed Monthly Feature Fee”):

- For Behavioral Analytics Dashboard (Insights) a fixed monthly fee of $ 3,500 per 1 million monthly visitors’ sessions (minimum $750) plus the applicable value added tax;
- For Real Time Segmentation a fixed monthly fee of $ 3,500 per 1 million monthly visitors’ sessions (minimum $750) plus the applicable value added tax;
- For On-site Targeting with Personalized Offers and Messages a fixed monthly fee of $ 3,500 per 1 million monthly visitors’ sessions (minimum $750) plus the applicable value added tax;
- For Streams (for email retargeting) $ 2,000 per 1 million monthly visitors’ sessions (minimum $750) plus the applicable value added tax;
- For Web Push Notifications a fixed monthly fee of $ 1,500 per 1 million monthly visitors’ sessions (minimum $750) plus the applicable value added tax;
- For Product Recommendations a fixed monthly fee of $ 5,000 per 1 million monthly visitors’ sessions per product catalog (minimum $2,500) plus the applicable value added tax;
- For Product Rankings a fixed monthly fee of $ 1,500 per 1 million monthly visitors’ sessions (minimum $750) plus the applicable value added tax;
- For Personalized SMS a fixed monthly fee of $ 750 and CPM (cost per thousand SMS sent) of $150 plus the applicable value added tax;
- For Site Speed Analytics a fixed monthly fee of $ 1,000 per 1 million monthly visitors’ sessions (minimum $500) plus the applicable value added tax.

The Client agrees to pay Fanplayr an hourly fee of $ 250 plus the applicable value added tax for each hour of support from Fanplayr staff members in excess of what defined in section B of this Agreement.

G. Invoicing

Fanplayr or one of its regional subsidiaries will invoice the Client on the 1 calendar day of each month for fees due from the preceding month.

The payment term for these invoices shall be net 15 days. All the amounts due will be paid to the entity issuing invoices.

H. Signature

In witness whereof, the Parties have caused this Agreement to be executed in two counterparts, as of the date ____________

Company: Fanplayr Inc.	Company:
Signed By:	Signed By:
Print Name:	Print Name:
Title:	Title:

SCHEDULE B

DATA PROCESSING AGREEMENT

This DPA is part of the Fanplayr Media Service Agreement (the "Main Agreement") between Fanplayr (the “Data Processor”) and You (the “Data Controller”)

WHEREAS

(A) The Parties entered into the Main Agreement whereby the Data Processor undertook to provide Fanplayr Services to the Data Controller.

(B) The purpose of this Data Processing Agreement is to regulate the relationship between the Data Controller and Data Processor in relation to the processing of personal data underlying the obligations under the Main Agreement;

(C) In addition to the provisions agreed upon by the Parties in the Main Agreement, which remain applicable, the Parties herein agree as provided in this Data Processing Agreement;

(D) In the event of any conflict between the provisions of this DPA and any other contract between the Parties, including, but not limited to, the Main Agreement, the provisions of this DPA shall prevail with respect to the Parties' obligations and responsibilities related to the protection of Personal Data. In the event of any conflict or inconsistency between the provisions of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

1. DEFINITIONS

a. Terms such as "*to process/processing*", "*data subject*", "*Data Processor*", “*Data Controller*”, "*personal data*", "*data breach*", "*data impact assessment*", etc. will have the meaning given to them in the current Data Protection Legislation;

b. "Parties" means the Data Controller and the Data Processor (also individually indicated as the "Party");

c. “Data Protection Legislation” means, in relation to any Personal Data that is processed in connection with the Main Agreement, the GDPR and all domestic laws that transpose or integrate it and any other applicable laws on data protection or privacy;

d. “EEA” means the European Economic Area;

e. **"**Personal Data**"** means any data indicated in Appendix 1 *(Description of the processing),* and any other personal data processed by the Data Processor on behalf of the Data Controller pursuant to or in connection with the Main Agreement;

f. "Services" means the services described in the Main Agreement;

g. "Standard Contractual Clauses" means the applicable module of the standard contractual clauses for transferring Personal Data to third countries outside the EEA, as approved by the European Commission in the framework of Decision (EU) 2021/914 of 4 June 2021, as amended or replaced;

h. **“**Sub-processor**"** means any processor (including any third parties and any affiliates of the Data Processor) that has been appointed by the Data Processor to process Personal Data on behalf of the Data Controller;

i. **"**Supervisory Authority**"** means (a) an independent public authority which has been established by a Member State under Article 51 of the GDPR; and (b) any regulatory authority responsible for enforcing Data Protection Legislation;

j. "Data Processing Agreement" or "DPA" means this data processing agreement which is drafted pursuant to Article 28, paragraph 3 of the GDPR;

k. "Instructions" means the written instructions given by the Data Controller to the Data Processor.

l. Any definition given in the Main Agreement has the exact same meaning referred therein.

2. PROCESSING OF PERSONAL DATA

a. The Data Processor will implement technical and organisational measures to ensure that Personal Data is processed in compliance with the requirements of the GDPR and guarantees the protection of data subjects’ rights.

b. The Data Processor will only process Personal Data concerning the categories of data subjects under the Main Agreement and for the specific purposes indicated in Appendix 1 attached to this DPA (*Description of the processing*) in compliance with the written instructions given by the Data Controller (contained in the Main Agreement or elsewhere, including in the Instructions), unless EU laws or the laws of a Member State to which the Data Processor is subjected require that data be processed. In this case, to the extent permitted by law the Data Processor shall give the Data Controller notice of the legal requirements for processing such data before processing such Personal Data. In any case, the Data Processor shall inform the Data Controller immediately if it believes that any instruction given under this Section would violate the standards of the Data Protection Legislation or any other provision of the EU or a Member State in relation to data protection.

c. The Parties agree that this DPA supersedes any previous relating to the subject matter of this DPA.

3. DATA PROCESSOR’S STAFF

a. Without prejudice to any existing agreement between the Parties, the Data Processor shall keep all Personal Data strictly confidential. Pursuant to Article 29 of the GDPR, the Data Processor undertakes to supervise the activities of the persons authorized to processing operations and shall take all reasonable measures to ensure that any employee, agent, supplier and/or Sub-processor that might have access to the Personal Data is reliable, and guarantees in each case, as part of that person's obligations towards the Data Processor, that access is strictly limited to those persons that need to have access to their Personal Data, to the extent strictly necessary for the purposes set out in Section 2.b above.

b. The Data Processor shall ensure that all the persons or parties involved in the processing of Personal Data:

   i. are duly appointed as persons authorised to processing operations;

ii. are duly trained on the applicable Data Protection Legislation;

iii. are bound by confidentiality agreements and have received written instructions on how and to what extent Personal Data are processed; and

iv. are subjected to user authentication and login procedures when they access to the Personal Data.

4. SECURITY

a. Without prejudice to any other security standards agreed upon by the Parties, the Data Processor shall implement and update appropriate technical and organisational measures to ensure a level of security for Personal Data appropriate to the risk inherent thereto and shall implement all the measures provided for under Article 32 of the GDPR. In assessing the appropriate level of security, the Data Processor shall take the risks that are presented by processing into account, from destruction, in particular loss, alteration, unauthorised disclosure of, or accidental or unlawful access to personal data transmitted, stored or otherwise processed. The said technical and organisational measures will, in any case, include reasonable measures which:

i. guarantee that Personal Data can only be accessed by the parties authorised for the purposes set out in Appendix 1 (*Description of the processing*) to this DPA;

ii. protect Personal Data from accidental or unlawful destruction, loss or accidental alteration, unauthorised or unlawful storage, processing, access or disclosure;

iii. identify flaws of the Personal Data Processing in systems used to provide services to the Data Controller.

5. SUB-PROCESSING

a. The Data Controller hereby authorises the Data Processor to appoint the Sub-processors listed at the link https://fanplayr.com/legal/.

b. Subject to Section 5.1, the Data Processor shall provide reasonable notice to the Data Controller before engaging a new Sub-processor by means of email to the address provided in the Subscriber Agreement indicating to the Data Controller that it has updated the list of Sub-processors set forth at the link https://fanplayr.com/legal/.The Data Controller may object to such changes within thirty (30) calendar days of receipt of the notice, if there is a justified reason. In the event that the Data Controller objects to the appointment of a new Sub-processor, the Data Processor shall be entitled to make a change to the Services that avoids the processing of Personal Data by the new Sub-processor in favour of the Data Controller. If the Data Processor is unable to make such change available within a reasonable period, it will notify the Data Controller. In such case, the Data Controller may terminate the Main Agreement upon written notice sent by registered e-mail or registered letter with acknowledgment of receipt.

c. The Data Processor shall, in relation to each Sub-processor:

i. provide the Data Controller with information about the data processing operations that shall be carried out by each Sub-processor;

ii. conduct adequate due diligence procedures with respect to each Sub-processor for the purpose of ensuring that the latter is able to provide the level of protection for Personal Data required by this DPA, including, without limitation, providing sufficient guarantees that adequate technical and organisational measures will be implemented so that data processing operations comply with any requirements under the Data Protection Legislation and this DPA;

iii. include in the agreement executed by the Data Processor and each Sub-processor terms and conditions that substantially restate the same as those specified in this DPA;

iv. to the extent the agreement between the Data Processor and each Sub-Processor provides for the transfer of Personal Data outside the EEA, include the Standard Contractual Clauses or any other tool pursuant to Data Protection Legislation in any agreement with each Sub-processor in order to provide adequate protection to the processing of Personal Data; and

v. be fully liable towards the Data Controller for any breach committed by each Sub-processor in relation to its obligations concerning the processing of Personal Data.

6. DATA SUBJECT’S RIGHTS

a. Should it receive a request from a data subject pursuant to any Data Protection Legislation (including the data subject’s request to exercise the rights provided for under Chapter III of the GDPR), the Data Processor shall promptly notify the Data Controller by means of email to the address provided in the Subscriber Agreement. That notice shall in any event be given within two (2) business day and provide complete details of the request.

b. The Data Processor shall cooperate, as requested by the Data Controller, to allow the Data Controller to meet any request made by a data subject exercising his or her rights under any Data Protection Legislation, and comply with any inquiry, request for information, notification or investigation conducted under any Data Protection Legislation in connection with Personal Data or this DPA. This will include:

i. providing the relevant information required by the Data Controller within a reasonable timeframe, including full details and copies of any complaint, communication or request and any Personal Data in its possession concerning the data subject in question;

ii. where applicable, providing the support reasonably required by the Data Controller to allow the Data Controller to fulfil any request within the timeframe indicated by the applicable Data Protection Legislation; and

iii. implementing any additional technical and organisational measures which may be reasonably required by the Data Controller to enable the latter to respond effectively to any complaints, communications or requests.

7. INCIDENT MANAGEMENT

a. The Data Processor shall immediately notify the Data Controller, substantially in the form of Appendix 2 and, in any event, within forty-eight (48) hours after it becomes aware of or has reason to suspect that there has been a data breach, providing the Data Controller with sufficient information to enable the latter to comply with any requirement to report a data breach under the applicable Data Protection Legislation. The notice shall, at the very least:

i. describe the nature of the data breach, the categories and approximate number of data subjects involved, and the categories and the approximate number of Personal Data records in question;

ii. indicate the name and contact details of the data protection officer of the Data Processor, if any, or other contact persons from which more information can be obtained;

iii. describe the probable consequences of the data breach, and

iv. describe the measures that have been taken or that will be taken to address the data breach.

b. The Data Processor shall fully cooperate with the Data Controller and take all reasonable measures that have been indicated by the Data Controller as being necessary for assisting in investigating, mitigating and correcting each data breach, and allowing the Data Controller to *(i)* conduct a thorough data breach investigation; *(ii)* provide an appropriate response and take appropriate additional measures in relation to the data breach so as to meet any requirement under the applicable Data Protection Legislation.

c. The Parties shall coordinate with each other and cooperate in good faith in drafting any public statements in relation thereto, as well as any notices that might be requested by the persons involved. Each Party shall not give any notice to any third party without the prior written consent of the other Party, except where such notice must be given in accordance with laws of the EU or a Member State to which that Party is subjected, In that case, to the extent permitted by the law the relevant Party shall inform the other Party of such legal requirement and provide a copy of the proposed notice.

8. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATIONS

a. The Data Processor shall provide reasonable levels of assistance to the Data Controller in relation to any data protection impact assessments required under Article 35 of the GDPR and in relation to the Data Controller's or any of its affiliates' prior consultations with any Supervisory Authority that might be requested pursuant to Article 36 of the GDPR, in any case in connection with the Personal Data processed by the Data Processor on behalf of the Data Controller and taking into account the nature of such data processing and the information that the Data Processor has at its disposal.

9. TERMINATION – ERASURE OR RESTITUTION OF PERSONAL DATA

a. This DPA will terminate upon termination for reason whatsoever of the Main Agreement.

b. Subject to any applicable law allowing further retention of the Personal Data and the Main Agreement, on the date on which the Main Agreement is terminated for any reason whatsoever, the Data Processor shall immediately cease processing the Personal Data and securely delete all copies of the Personal Data processed by it within 90 (ninety) days.

10. RIGHT TO AUDIT

a. The Data Processor agrees to make available to the Data Controller, upon its request, all information necessary to demonstrate compliance with this DPA and to allow any checks to be conducted in relation thereto, including inspections by the Data Controller or any other person appointed by the Data Controller to inspect facilities or offices at which the Personal Data is processed. The Data Processor shall fully cooperate with the Data Controller in connection with any such verifications and, upon the Data Controller's request, provide the latter with proof (including, where requested, all information relevant for this purpose, subject to the execution of a confidentiality agreement and, in any case, access to Data Processor's trade secrets and confidential information kept restricted) of its compliance with its obligations under this DPA. The above applies to processing operations carried out by Sub-processors. It is understood that inspections may take place only where compliance cannot be demonstrated through remote exchange of information and documents and with a prior reasonable notice to the Data Processor. Inspections may not last longer than two working days and may be conducted only once per calendar year. The costs of the inspections shall be borne by the Data Controller.

11. INTERNATIONAL TRANSFERS OF DATA CONTROLLER'S PERSONAL DATA

a. The Data Processor shall not process, or allow any Sub-Processor to process, (permanently or temporarily) Personal Data in a country outside the EEA without an adequate level of protection, except in relation to the Sub-processors in those countries listed in the list available at the link https://fanplayr.com/legal/ and in relation to the new Sub-processors engaged pursuant to section 5.b above (transfers in relation to such Sub-processors shall be deemed as authorised by the Data Controller as of now).

b. The Data Processor shall promptly execute (or ensure that any relevant Sub-processor promptly executes) Standard Contractual Clauses in relation to any processing of Personal data in a country outside the EEA that does not provide an adequate level of protection.

12. LIABILITY

a. To the extent set forth in the Main Agreement, the Data Processor agrees to hold the Data Controller harmless from adverse consequences arising from the Data Processor's breach of the Data Protection Legislation and / or the Data Processor's breach of the provisions of this DPA.

13. MISCELLANEOUS

a. In the event that a Party becomes aware of any actual or potential judicial or administrative proceedings, including proceedings before any supervisory authority which concern the processing of Personal Data referred to in this DPA, it shall promptly inform the other Party in writing by e-mail and cooperate at its own expense with the other Party. To this purpose, the Data Controller shall notify the Data Processor in writing, within 7 (seven) days of signing this DPA, of the e-mail address to which such information shall be sent. In the absence of such notice, the Data Processor shall be free to use any other channel provided for in the Main Agreement. The Data Processor's email, to which the Data Controller must send the communications referred to in this Section a, is privacy@fanplayr.com.

b. If any provision of this DPA is or becomes invalid or unenforceable, the remainder hereof will continue to be fully valid and enforceable. Any invalid or unenforceable provision may be either (i) amended as necessary to guarantee its validity and applicability, while preserving, to the greatest extent possible, the intentions of the Parties, or, if this is not possible, *(ii)* interpreted as if the invalid or unenforceable provision was never included.

c. This DPA shall be governed by the law of the country where the Data Controller is established.

14. APPENDIXES

a. The following appendixes are attached to this DPA:

i. Appendix 1 – Description of the processing

ii. Appendix 2 - Form for notifying incidents that might result in data breaches

IN WITNESS THEREOF, this DPA has been executed and becomes an integral and binding part of the Main Agreement, entering into force with effect from the date of signature.

[●]	**[●]**
Signature ___________________________	Signature _________________________________
Data Controller	Data Processor

WHERE ITALIAN LAW APPLIES, PURSUANT TO SECTIONS 1341 AND 1342 OF THE ITALIAN CIVIL CODE THE DATA PROCESSOR

REPRESENTS THAT IT HAS UNDERSTOOD AND EXPRESSLY ACCEPTS THE FOLLOWING ARTICLES OF THIS AGREEMENT: 5 (SUB-PROCESSING), 11 (INTERNATIONAL TRANSFERS OF PERSONAL DATA), 12 (LIABILITY) AND c (MISCELLANEOUS – JURISDICTION).

[●]
Signature _______________________________
Data Controller

ANNEX 1: DESCRIPTION OF THE PROCESSING

This Annex 1 includes details about the processing of Personal Data as provided for under Article 28 (3) of the GDPR.

	Characteristics	Description
1	Subject of the processing	*User Data*
2	Duration of the processing	*On a continuous basis for the period of the Agreement*
3	Purposes of the processing	*To provide the Fanplayr Service.*
4	Kinds of personal data processed	*User Data, including e-mail addresses, SMS numbers, IP addresses, geolocation, cookies data, web requests, browser type, browser language, referring / exit pages and URLs, platform type, number of clicks, domain names, landing pages, pages viewed and the order of those pages, features used, products of interest, items placed in or removed from Users' Shopping Carts, Offers added to or used from Users' Offer Wallet, data relating to orders, the amount of time spent interacting with data exporter's Offers and data exporter's Websites, and all other data relating to user activity on the data controller's Website, interaction data relating to emails, SMS and Push Notifications messages, site speed data, the dates and times of requests, and other similar or related data.*
5	Categories of data subjects involved	*Website's users*
6	Operational locations of the Data Processor involved in the processing operations and locations where the data are stored	*Location of Processing (data centre location):* *Location of Service Desk:*
7	IT systems supporting data processing	- *Fanplayr Service* - *Amazon Web Services - https://aws.amazon.com/privacy/ (provision of cloud services)* - *Google Cloud Platform – https://cloud.google.com/privacy/ (provision of cloud services)*

APPENDIX 2: FORM FOR REPORTING OF INCIDENTS THAT MIGHT RESULT IN A DATA BREACH

1. Data Controller’s name, Data Processor’s name (including the name of any Sub-processor involved) which have been involved in an incident that could lead to a data breach
2. Date and time of the incident
3. Nature of the incident
4. Categories and approximate number of data subjects whose personal data has been involved in the incident
5. Categories and the approximate number of personal data records involved in the incident
6. Name and contact details of the Data Protection Officer (DPO) (if appointed)
7. Probable consequences of the incident
8. Measures that can be used to remedy the incident and mitigate its negative effects

SCHEDULE C

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

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

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter “sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

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

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

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

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

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

Clause 13

Supervision

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

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

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

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

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

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

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

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

Clause 15

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

15.1 Notification

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

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

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

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or 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 the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Italy.

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 Italy.

(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

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Client Company Name:

Client Company Address:

Contact person’s name, position and contact details:

Activities relevant to the data transferred under these Clauses: Owner of the website using the Fanplayr Service

Signature and date:

Role: Controller

Data importer:

Name: **Fanplayr Inc.**

Address: 725 Alma St, Palo Alto, CA, 94301, USA

Contact person’s name, position and contact details: Gabriele Favarò, VP Global Operations, privacy@fanplayr.com

Activities relevant to the data transferred under these Clauses: providing the Fanplayr Service

Signature and date:

Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Users of the data exporter's Websites, Stores, Loyalty Programs, and other services provided by the data exporter to its users.

Categories of personal data transferred

User Data, including e-mail addresses, SMS numbers, IP addresses, geolocation, cookies data, web requests, browser type, browser language, referring / exit pages and URLs, platform type, number of clicks, domain names, landing pages, pages viewed and the order of those pages, features used, products of interest, items placed in or removed from Users’ Shopping Carts, Offers added to or used from Users’ Offer Wallet, data relating to orders, the amount of time spent interacting with data exporter's Offers and data exporter's Websites, and all other data relating to user activity on the data exporter's Website, interaction data relating to emails, SMS and Push Notifications messages, site speed data, the dates and times of requests, and other similar or related data.

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

On a continuous basis

Nature of the processing

Automated with electronic means

Purpose(s) of the data transfer and further processing

To provide the Fanplayr Service.

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

for the duration of the Agreement

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

All data referred to in the Categories of personal data transferred is collected, recorded, organised, stored, retrieved, and generally made available using various services provided by sub-processors on a continuous basis. The duration of the processing is the duration of the time the end user is active on the Exporter’s website. The duration of the storage is defined by the duration of the Agreement. Purpose is to provide the Fanplayr Service.

C. COMPETENT SUPERVISORY AUTHORITY

Italian Data Protection Authority

Garante per la protezione dei dati personali,

Piazza Venezia 11, IT-00187, Roma

Email: protocollo@gpdp.it

PEC: protocollo@pec.gpdp.it

Centralino +39 06.696771

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

Fanplayr employs both technical and organizational measures to ensure that the data gathered is secure at all times.Such measures include:

Physical Security

Fanplayr leverages Amazon's state-of-the-art data centers designed to host mission-critical computer systems with fully redundant subsystems and compartmentalized security zones. Amazon's data centers adhere to the strictest physical security measures:

- *Requires multiple layers of authentication before access is granted to the server area*
- *Critical areas require two-factor biometric authentication*
- *Camera surveillance systems at critical internal and external entry points*
- *Security personnel monitor 24/7*
- *Unauthorized access attempts are logged and monitored by data center security*

All physical access to the data centers is highly restricted and stringently regulated. Fanplayr data operations uses security best practices such as "least access" hardened servers and regularly scheduled maintenance/upgrade/patch windows. For a complete list of Amazon's security measures, please read the AWS Security White Paper at http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf

Data Segregation

Fanplayr is a multi-tenant Software-as-a-Service (SaaS) application. Fanplayr isolates each customer tenant's application data. Fanplayr accomplishes this through a robust infrastructure layer called the Fanplayr Data Access Services. Every tenant is associated with exactly one Account Key. This in addition to an internal Account Id is then used to access the Fanplayr application. The Key itself is a secure non-sequential one-way hash providing an additional level of protection. All instances of application data (such as behavioral data, conversion data, etc.) are tenant based. Every time a new object is created, the object is also irrevocably linked to the tenant. The Fanplayr system maintains these links automatically, restricting access to every object based on the Account Key. When a user requests data, the system automatically applies a tenancy filter to ensure it retrieves only information corresponding to the user's tenant.

Encryption of Data in Transit (Network Security)

All business critical data such as conversion data is transmitted to Fanplayr via the Internet protected by Secure Socket Layer version 3. While this depends on the customer's site, when used it secures network traffic from passive eavesdropping, active tampering, or forgery of messages. Fanplayr also leverages AWS's proactive security procedures such as perimeter defense and network intrusion prevention systems. Vulnerability assessments and penetration testing of the Fanplayr network infrastructure are also evaluated and conducted on a regular basis.

Encryption of Data at Rest

All data stored on disk is encrypted with Advanced Encryption Standard (AES) with managed encryption keys. Any data queried and decrypted, automatically uses TLS encryption as it is transferred over the wire to other systems or any User Interfaces.

Data Backups

Fanplayr's master production database is replicated in real-time to a slave database maintained in a different geographic AWS region. A full backup is taken from this slave database every day and stored at the offsite data center facility. Fanplayr's database backup policy requires database backups and transaction logs to be implemented so that a database may be recovered with the loss of as few committed transactions as is commercially practicable. Transaction logs are retained until there are eight backups of the data after the last entry in the transaction log. Backups of the database and transaction logs are encrypted for any database which contains customer data.

Cloud Data and Disaster Recovery

Fanplayr operating procedures include a Disaster Recovery (DR) plan for the Fanplayr Production Service with a Recovery Time Objective (RTO) of 2 hours. The Recovery Time Objective is measured from the time the Fanplayr Production Service becomes unavailable until it is available again. The DR plan comes into effect only under extreme circumstances. Under normal circumstances, Fanplayr maintains identical production environments in multiple geographical regions, ensuring that any disaster in one location will not render the service unavailable. Regional environments are monitored every five minutes to check availability and users are automatically routed to alternate regions if needed. To ensure Fanplayr adheres to these procedures, Fanplayr maintains a DR environment with a complete replication of the production environment. In the event of an unscheduled outage where the outage is estimated to be greater than a predefined duration, Fanplayr executes its DR plan. The MySQL database is replicated to the DR data center, new service instances are started in the DR data center, and customers are redirected to the DR data center. The DR Plan is tested at least every six months.

Unified Security Model

Unlike legacy ERP systems, Fanplayr operates on a unified security model. This includes user access, system integration, reporting, device, and IT access. Everyone must log in and be authorized through the Fanplayr security model. By contrast, in legacy ERP systems there is typically an applications layer of security which IT and DBA personnel can bypass to access the data directly at the database level. This is not possible with Fanplayr. Fanplayr is an object-oriented in-memory system with a persistent data store. This ensures all access and changes are tracked and audited. This unique robust security model, combined with Fanplayr's automatic ability to effective date and audit all data updates, lowers the time and costs associated with governance and compliance and reduces overall security risk.

Authorization

The Fanplayr application enforces group policy-based security for authorization. The application prevents customer end users from directly accessing the production database. Fanplayr's security groups combined with Fanplayr predefined security policies grant or restrict user access to functionality, business processes, reports, and data. Security groups are based on users, roles, organizations, or business sites and can be combined into new security groups that logically include and exclude other groups. System-to-system access is defined by integration system security groups.

System-to-System Access

In Fanplayr, system-to-system access is via web services. Only inbound data (data gathered from customer sites) is allowed from external systems. Access to stored data is not possible using external systems, thereby providing a high level of security. Regardless of method, the data results are controlled by Integration System Security.

Application Security

In particular, Fanplayr incorporates security into its platform development processes at all stages. From initial architecture considerations to post-release, all aspects of platform development consider security.

- *Design phase – Guiding security principles help ensure Fanplayr technologists make the best security decisions possible. Threat assessments on high-risk features help to identify potential security issues as early in the development lifecycle as possible.*

- *Coding phase – Fanplayr addresses standard vulnerability types through the use of secure coding patterns and anti-patterns, and uses static code analysis to identify security flaws.*

- *Prior to release – Fanplayr validates that the functionality being developed and maintained meets its internal security requirements. Post-release, Fanplayr analyzes and monitors the product for potential security issues.*

Fanplayr implements industry-accepted best practices to harden all underlying host computers that support the various software layers of the Fanplayr cloud platform. For instance, all hosts use Linux distributions with non-default software configurations and minimal processes, user accounts, and network protocols. Host services never execute under root, and they log their activity in a remote, central location for safekeeping.

The underlying database layer of Fanplayr also plays a significant role in platform security. For example, the database protects customer passwords by storing them after applying an one-way cryptographic hash function, and supports the encryption of field data in custom fields.

Fanplayr enforces strict control of powerful database administrator access. Fanplayr's innovative metadata-driven, multitenant database architecture delivers operational and cost efficiencies for cloud-based applications without compromising the security of each organization's data.

- *When a user establishes a connection, Fanplayr assigns the session a client hash value.*

- *Along with the formation and execution of each application request, Fanplayr confirms that the user context (an tenant ID, accountKey, or accountId) accompanies each request and automatically includes it in the WHERE clause of all SQL statements to ensure the request targets the correct organization's data. On the flip side, Fanplayr validates that every row in the return set of a database query matches the session's accountID as well.*

- *Before the rendering of a Web page that corresponds to an application request, Fanplayr confirms that the calculated client hash value matches the client hash value that was set during the login phase.*

User Access Provisioning

The standards for access privileges are achieved through the use of the Role-based Access Control (RBAC) model. RBAC is an access control mechanism that permits system administrators to allow or disallow other user's access to systems under their control. Users can be easily reassigned from one role to another. Roles can be granted new permissions as new applications and systems are incorporated, and permissions can be revoked from roles as needed. This type of access greatly simplifies management of privileges and permissions.

The following RBAC implementation standards apply:

- *A user can only access data, services and capabilities based on an assigned role.*

- *Roles are defined based on job functions.*

- *Permissions are defined based on role authority and responsibilities within a job function.*

- *Operations on any data, service or capability are invoked based on the role permissions.*

- The data, service or capability is only concerned with the user's role and not the user.

- Roles are designed and implemented based on the principle of least privileged.

- A role contains only the minimum scope of permissions required.

- A user account is assigned to a role that allows it to perform only what's required for that role.

- No single role is given more permission than the same role for another user

Privilege Management

a. All access privileges adhere to the following principles:

i. Need to know – the legitimate requirement of a person to know, access, or possess sensitive information that is critical to the performance of the authorized job function.

ii. Least Privilege – every user and program must operate using the least set of privileges necessary to complete the authorized job function.

iii. Separation of duties – the practice of dividing the steps in a system function among different individuals, so as to keep a single individual from subverting the process.

b. The need to know is enforced though the account authorization process and establishment. The least privileges and separation of duties are achieved by:

i. Limiting the role of system administrator to the fewest number of individuals necessary to achieve adequate service;

ii. Implementing fine grain access privileges for the performance of privilege tasks;

iii. Separating system administrator accounts from regular user accounts;

iv. Separating system administrator functions from audit and logging functions.

c. In addition to various regular end-user roles, programmers, developers and testers will have separate roles with different privileges than system administrator roles.

Review of User Access

Fanplayr's information asset and IT asset owners review user access rights on a regular basis to ensure that role changes, such as promotion, demotion, transfer, and termination are correctly reflected in all information systems under their management.

Removal or adjustment of access rights

The access rights of all Users to information and information processing facilities shall be removed upon termination of their employment, contract or association with Fanplayr, or adjusted upon change.

Data Classification

1. Information Services (IS) Responsibility—All employees who come into contact with sensitive Fanplayr internal and customer information are expected to familiarize themselves with this data classification policy and to consistently use these same ideas in their daily Fanplayr business activities. Sensitive information is either Confidential or Restricted information, and both are defined later in this document. Although this policy provides overall guidance, to achieve consistent information protection, employees are trained and expected to apply and extend these concepts to fit the needs of day-to-day operations.

2. Addresses Major Risks - The data classification system, as defined in this document, is based on the concept of need to know. This term means that information is not disclosed to any person who does not have a legitimate and demonstrable business need to receive the information. This concept, when combined with the policies defined in this document, will protect Fanplayr information from unauthorized disclosure, use, modification, and deletion.

3. Applicable Information - This data classification policy is applicable to all electronic information for which IS is the custodian.

4. Owners and Production Information—All electronic information managed by IS has a designated Owner. Production information is information routinely used to accomplish business objectives. Owners should be at the VP level or above. Owners are responsible for assigning appropriate sensitivity classifications as defined below. Owners do not legally own the information entrusted to their care. They are instead designated members of the Fanplayr management team who act as stewards, and who supervise the ways in which certain types of information are used and protected.

5. Information Classification

a. RESTRICTED—This classification applies to the most sensitive business and customer data that is intended for use strictly within Fanplayr. Its unauthorized disclosure could seriously and adversely impact Fanplayr, its customers, its business partners, and its suppliers.

b. CONFIDENTIAL—This classification applies to less-sensitive business information that is intended for use within Fanplayr. Its unauthorized disclosure could adversely impact Fanplayr or its customers, suppliers, business partners, or employees.

c. PUBLIC—This classification applies to information that has been approved by Fanplayr management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be disseminated without potential harm.

6. Owners and Access Decisions—Data Owners make decisions about who will be permitted to gain access to information, and the uses to which this information will be put. IS takes steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of electronic information.

7. Object Reuse and Disposal - Storage media containing sensitive (i.e. restricted or confidential) information is completely empty before reassigning that medium to a different user or disposing of it when no longer used. Simply deleting the data from the media is not sufficient. A method is used (DOD 5220.22-M, DoD 5200.22-M (ECE), and DoD 5200.28-STD) that completely erases all data. When disposing of media containing data that cannot be completely erased it is destroyed in a manner approved by the Director of IS Security.

8. Special Considerations for Restricted Information - If Restricted information is stored on a personal computer, portable computer, or any other single-user system, the system must conform to data access control safeguards approved by IS and Corporate senior management. When these users are not currently accessing or otherwise actively using the restricted information on such a machine, they must not leave the machine without logging off, invoking a password protected screen saver, or otherwise restricting access to the restricted information.

9. Storage on non-production systems—Fanplayr employees and vendors must not create, copy or duplicate any of the Restricted Information on to any system that is not designated as a production system. Any such action is considered a breach of the confidentiality agreement between the employee and Fanplayr. Exceptions will not be made, and no employee is authorized to provide an exception. In the event of a need, any request has to be made to the Fanplayr Board of Directors, for explicit approval.

10. Key Management

a. Protection of Keys—Public and private keys are protected against unauthorized modification and substitution.

b. Procedures—Procedures are in place to ensure proper generation, handling, and disposal of keys as well as the destruction of outdated keying material.

c. Safeguarding of Keys—Procedures are in place to safeguard all cryptographic material, including certificates. IS Security is given copies of keys for safekeeping

Fanplayr

ANNEX III – LIST OF SUB-PROCESSORS

An updated list of sub-processors is available at the webpage https://fanplayr.com/legal

Fully Owned Subsidiaries:

Fanplayr UK Ltd. (UK) (service desk activities for clients in the UK)

Fanplayr Latin America S. de R.L. de C.V. (Mexico) (service desk activities for clients in the Latin American region)

Fanplayr Europe s.r.l. (Italy) (service desk activities for clients in the Continental Europe)

JAMU Inc.(Japan) (service desk activities for clients in Japan)

Fanplayr ANZ Pty Ltd. (Australia) (service desk activities for clients in the Australia and New Zealand)

FANPLAYR LATIN AMERICA SAS (Argentina) (service desk activities for clients in Argentina)

Fanplayr Brasil Tecnologia LTDA (Brazil) (service desk activities for clients in Brazil)

Fanplayr Spain SA (Spain) (service desk activities for clients in Spain)

Software suppliers:

Amazon Web Services - https://aws.amazon.com/privacy/ (provision of cloud services)

Google Cloud Platform – https://cloud.google.com/privacy/ (provision of cloud services)

Others:

Whose Next Inc. (Japan) (service desk activities for clients in Japan)