Petal Ads Services Agreement

Last Modified: January 10, 2023

The Petal Ads Services Agreement (hereinafter referred to as the "Agreement") is legally binding agreement signed between you (also referred to as "**Customer**") and Huawei. This Agreement is a supplementary agreement to the **HUAWEI Developers Service Agreement** and the **HUAWEI Partner Paid Service Agreement** and together control your relationship with Huawei when you use Petal Ads Services. By registering for the Advertising Services under this Agreement, or using any Advertising Services under this Agreement, you are agreeing to be bound by the terms of this Agreement, the HUAWEI Developers Service Agreement and the HUAWEI Partner Paid Service Agreement from the date of such registration or use ("**Effective Date**").

In the event of any inconsistency between the terms of this Agreement and the HUAWEI Developers Service Agreement and/or the HUAWEI Partner Paid Service Agreement, the terms of this Agreement shall prevail only to the extent of such inconsistency relating to Advertising Services.

If you are agreeing to be bound by this Agreement on behalf of your employer or any other entity, you represent and warrant that you have full legal authority to bind your employer or said entity to this Agreement. If you do not have the requisite authority, you may not accept the Agreement on behalf of your employer or any other entity.

1. Definitions

"Ads" means advertising materials that Customer provides through the AdsPlatform and authorizes Huawei to place on any Property provided by Huawei or its Affiliates on behalf of Huawei or, as applicable, a third party (hereinafter, a "Partner"), including but not limited to text, pictures, animations, videos, audio files, webpages, and URLs.

"Ads Policies" means policies on advertising content and other policies related to the Services available at https://developer.huawei.com/consumer/en/doc/distribution/promotion/overview-0000001188925990. The Ads Policies may be updated from time to time.

"**Business Area**" is the territory where Customer's Advertising is distributed through the Platform when Customer uses Huawei Services.

"**EU Standard Contractual Clauses**" means the standard contractual clauses issued by the European Commission by implementing decision 2021/914 of June 4, 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

"**Huawei**" means the applicable Huawei entity(ies) listed in the clause of "Distribution Area and Signing Huawei Entity" (Clause 6) of the Huawei Partner Paid Service Agreement.

"**Petal AdsPlatform**", the "**AdsPlatform**", or the "**Platform**" means the mobile internet platform(s) and the associated websites and portals (e.g., https://ads.huawei.com) that are developed and/or operated by Huawei and/or its Affiliates to provide Petal Ads Services.

"Petal Ads Services" or the "**Services**" means the advertising programs and services provided by Huawei to Customer through the AdsPlatform under this Agreement.

"**Products**" means the services and products defined in Clause 2.2 herein.

"**Property**" or "**Properties**" means any mobile application software (with the content therein) or other digital content on which Ads can be launched and displayed, which are provided by Huawei or its Affiliates on behalf of Huawei or, as applicable, a third Party ("**Partner**").

"**UK Addendum"** means the addendum to the EU Standard Contractual Clauses issued by the UK Information Commissioner under Section 119A(1) of the UK Data Protection Act 2018 (version B1.0, in force March 21, 2022, as amended, available at: https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf).

2. Services and Policies

2.1 The use of the Services is subject to Customer's creation and Huawei's approval of an HUAWEI ID. Huawei has the right to refuse or limit Customer's access to the Services.

2.2 Customer is solely responsible for all: (i) Ads, (ii) Ads trafficking or targeting decisions ("**Targets**"), (iii) destinations to which Ads direct viewers (e.g., landing pages, mobile applications) along with the related URLs, waypoints, and redirects (" **Destinations**"), and (iv) services and products advertised on Destinations (collectively, "

Products"). By using Services, Customer authorizes Huawei to use automated tool to format Ads and serve Ads on Properties upon Customer's insertion orders ("**IO**") on Service user interface. Huawei may also make available to Customer certain optional Service features to assist Customer with the selection of Targets, Ads, or Destinations. Customer may opt-in to or opt-out of usage of these features. However, if Customer uses these features, Customer shall be solely responsible for the Targets, Ads, and Destinations. Huawei and its Affiliate or Partners may reject or remove a specific Target, Ad, or Destination at any time for any or no reason. Huawei also has the right to refuse an IO. Huawei may modify or cancel Services at any time. Customer acknowledges that Huawei or its Affiliates may participate in Service auctions in support of its own services and products.

2.3 Customer is solely responsible for its use of the Services (e.g., access to and use of Service accounts and safeguarding usernames and passwords) ("**Use**"). The Use is subject to this Agreement and Ads Policies (collectively, "**Ads Terms**"). Customer also authorizes Huawei to modify Ads as described in the Ads Terms.

2.4 Customer will not, and will not authorize any third Party to, (i) generate automated, fraudulent or otherwise invalid impressions, inquiries, clicks or conversions, (ii) conceal conversions for Services where they are required to be disclosed, (iii) use any automated means or form of scraping or data extraction to access, query or otherwise collect Huawei advertising–related information from any Property except as expressly permitted by Huawei, or (iv) attempt to interfere with the functioning of the Services. Customer will direct communications regarding Ads on Partner Properties under these Terms only to Huawei.

2.5 Huawei reserves the right to review the Products and Ads which are submitted by Customer to Petal AdsPlatform for distribution pursuant to the terms of this Agreement either before or after the Petal Ads Services is rendered hereunder, and at its sole discretion to decide whether to provide Customer with the Petal Ads Services for such Products or Ads.

2.6 Notwithstanding the foregoing, Huawei's reviewing of Customer's Products and Ads shall not relieve Customer from its responsibilities and liabilities arising from or in connection with the Products or Ads hereof. In the event of any non-conforming Ads or Products in the Property, Huawei shall be entitled to immediately carry out a solution, including but not limited, to removing the Ads and Products in question from the Property.

3. Ad Serving

Customer shall plan Ad serving at Service user interface in the form of insertion orders ("IOs") and authorize Huawei to serve Ads according to IOs.

You grant Huawei and its Affiliates a free, permanent, and irrevocable right to duplicate, distribute, integrate, promote, display, sell, or otherwise use Ads and Products for the purpose of this Agreement.

You grant Huawei and its Affiliates to use your logo, business name, and trademarks for the purpose of cooperation under this Agreement. If you believe that Huawei has misused any of the aforementioned items, you have the right to raise an objection, and Huawei shall take corrective actions after you and Huawei reach an agreement through negotiation.

Customer can choose to use the segments provided by a third-party data management platform (DMP) in an IO for targeted advertising, and pay Huawei according to CPM. Further details are available at: **https://developer.huawei.com/consumer/en/doc/distribution/promotion/audience-targeting-0000001249248257**.

4. Ad Cancellation

4.1 Unless a Policy or an IO provides otherwise, either Party may cancel any Ad at any time before the earlier of Ad auction or placement, but if Customer cancels an Ad after a commitment date provided by Huawei (e.g., a reservation-based campaign or an IO based on CPT), then Customer is responsible for any cancellation fees communicated by Huawei to Customer, and the Ad may still be published. Canceled Ads will generally cease serving within eight (8) business hours or as described in a Policy or IO, and Customer remains obligated to pay all charges resulting from served Ads.

4.2 Customer must effect cancellation of Ads (i) online through Customer's Account, if the functionality is available, (ii) if this functionality is not available, with notice to Huawei via email to Customer's account representative (collectively, the "Ad Cancellation Process"). Customer will not be relieved of any payment obligations for Ads not submitted or submitted by Customer after the due date provided by Huawei. Huawei will not be bound by a Customer-provided IO.

5. Payments

5.1 Charges in connection with the Services are based on the billing criteria under the applicable Services, including but not limited to CPM (cost per impressions), CPC (cost per click), CPD (cost per download), CPT (cost per time), and other billing criteria made available by Huawei for Customer to select in a specific IO. All charges shall be VAT-inclusive, except when, according to local law, you are a tax agent who is obligated to withhold the VAT, under which circumstance the charges shall be VAT-exclusive.

5.2 The Services are provided in a prepaid mode, and/or the credit card payment mode (which is specifically applicable for some determined countries/regions excluding the Chinese mainland), as available on the Customer interface of the AdsPlatform. Customer shall enroll for Paid Services to have the Paid Service account ("**Account**") enabled for its HUAWEI ID. Customer must ensure that the name of the account that it uses for making payments is the same as its company name, or else Huawei has the right to suspend the provision of the Services to Customer.

(a) Prepaid mode: Customer shall top up the Account in advance in accordance with the top-up rules to use the Services for the charges of the IOs that Customer placed. Huawei has the right to adjust the minimum top-up amount and subscription renewal amount from time to time. If Customer does an offline top-up of more than US$1,000 or EUR1, 000 at a time, Huawei will bear the handling fee of the intermediary bank ("**Waiver Policy**"). If there are any refunds, Huawei will only refund the actual amount received. Huawei reserves the right to adjust the above-mentioned Waiver Policy from time to time.

(b) Credit card payment mode: Customer adds a valid credit card number as a payment method of the Account for automatic payment.

5.3 Reconciliation: No reconciliation statement will be sent to you. You may check your account balance and account details on the Platform.

5.4 The charges will be settled in real time upon each display based on the billing criteria under the applicable Service at the price agreed by you and Huawei and the terms of your IO. The charges will be directly deducted from the balance of your Account. Payments will be calculated solely based on Huawei's accounting.

5.5 Huawei is not obligated to deliver any Ads in excess of the balance of your Account or any quota you set for an IO (if any).

5.6 If Huawei does not deliver Ads to the selected Targets or Destinations, then Customer's sole remedy is to make a claim for advertising credits within sixty (60) days after the invoice date ("Claim Period"), after which Huawei will issue the credits following claim validation which must be used within sixty (60) days of issuance ("Use-By Date"). Customer understands that third parties may generate impressions or clicks on Customer's Ads for prohibited or improper purposes and if that happens, Customer's sole remedy is to make a claim for advertising credits within the Claim Period, after which Huawei will issue the credits following claim validation, which must be used by the Use By Date. To the fullest extent permitted by law, (a) Customer waives all claims

pertaining to any service charges unless it is a claim within the Claim Period and (b) the issuance of advertising credits (if any) is at Huawei's reasonable discretion and if issued, must be used by the Used By Date.

5.7 Huawei reserves the right to distribute rewards to Customer from time to time. Specifically:

(a) Huawei may specify the reward policy by email or through announcements on the AdsPlatform or by other proper means selected in its sole discretion and good faith, including but not limited to the reward amounts, reward recipients, and reward methods.

(b) Under no circumstances shall such rewards be redeemed for cash. Huawei does not issue any invoice for such rewards. Rewards are not reflected in the advertiser consumption invoices on the AdsPlatform, and shall be automatically invalidated when the validity period thereof expires.

(c) Customer must ensure the authenticity of operating data. In the event of any violation, including but not limited to data fraud, Huawei reserves the right to hold Customer liable and reclaim the distributed rewards.

(d) If a reward recipient is an advertiser, the involved Partner shall transfer the reward amount announced by Huawei to said advertiser's Petal Ads account. Said Partner shall verify the advertiser's Petal Ads account before making such transfer, and provide proof of the transfer to Huawei after making it.

(e) If a Partner does not transfer a reward to an advertiser in accordance with the preceding requirements, Huawei reserves the right to reclaim the transferred reward amount from the Partner and take other appropriate measures at its own discretion.

6. Representations and Warranties

6.1 Customer hereby represents, warrants and covenants:

(a) Customer holds, and hereby grants Huawei, its Affiliates and Partners, the rights in Ads, Destinations, and Targets for Huawei, its Affiliates and Partners to operate the Services;

(b) All information and authorizations provided by Customer are true, legal complete, correct, and up to date and Customer shall be solely responsible for any and all legal liabilities thereto.

(c) Customer warrants it has full power and authority to enter into this Agreement and entering into or performing under this Agreement will not violate any agreement you have with a third Party or any third-Party rights, or any applicable laws and regulations.

(d) Ads and Products do not contain any viruses, worms, Trojan horses, time bombs, malicious code, malicious advertisements, or any software that damages, interferes with, intercepts, or confiscates any system data or personal information, or any fee deduction mechanisms that can be implemented without the permission of end users. If Huawei is punished by the competent authority of the country where Products are sold or is subject to end user claims because you violate one or more of the preceding terms, Customer will indemnify and hold harmless Huawei against and from any and all of said punishment, end user claims, and any other economic losses caused by your violation of this clause. In addition, Huawei has the right to terminate this Agreement.

(e) If the Ads or Products that you provide violate third-Party rights, including, but not limited to, infringement of third-Party intellectual property rights, causing personal injury or damage, causing property loss, and violation of open source agreements, you shall deal with pertinent matters at your own cost and ensure that Huawei and its customers are not affected. If a third Party files claims against Huawei, you shall be liable for compensating Huawei any and all expenses and losses incurred therefrom, including but not limited to penalties, user compensation, and litigation/attorney's fees. Huawei has the right to terminate this Agreement immediately in the event of any such occurrence described herein.

(f) You are responsible for the legitimacy of your products and display content, ensuring the quality of such items. You are responsible for maintaining such items, ensuring the user experience. You are responsible for ensuring the authenticity and accuracy of the display content, and ensuring that they comply with any and all applicable advertising laws, consumer protection laws, as well as any other applicable laws and regulations. In the event of any complaint, government punishment, or other issue arising from the above, you shall be responsible for it and agree to compensate Huawei for the losses and expenses incurred therefrom. Huawei reserves the right to take any and all reasonable measures to protect the rights and interests of end users.

(g) You warrant that your products do not contain any illegal content or other content Huawei deems to be inappropriate at its reasonable discretion.

(h) If your Products or Ads are at type of an application, you warrant that those Products and Ads have been distributed on HUAWEI AppGallery.

6.2 In the event that you, your Ads or the products are investigated by the competent authority or complained, or you violate applicable laws and/or regulations or the terms of

this Agreement, Huawei has the right to decide to take one or more of the following measures at its sole discretion, including:

(a) Rejecting, suspending, or terminating the display of the content that is suspected of being illegal or non-compliant;

(b) Demanding you to modify the content until it meets relevant requirements;

(c) Suspending or prohibiting the display of the content relating to products and/or services that are suspected of being illegal or non-compliant;

(d) Suspending or restricting your use of the Service (for example, freezing your account and suspending the review of your content);

(e) Removing or shielding all your display content;

(f) Deducting an amount from your account to compensate user losses and any other reasonable expenses;

(g) Deducting all the balance of your account as liquidated damages, which is non-refundable (if your account balance is insufficient for the compensation, you shall make up for it);

(h) Freezing your account and terminating the cooperation; demanding you to assume any and all expenses and losses incurred upon Huawei, including but not limited to penalties, user compensation, and litigation/attorney's fees.

6.3 If you receive any complaint from Users or third parties about your display content and you fail to properly resolve such complaint within three (3) working days after your receiving it, Huawei has the right to take one or more of the following measures to protect the rights and interests of the users or others:

(a) Huawei decides to advance the expenses to settle disputes and compensate for losses. Huawei has the right to directly deduct such expenses from your account or claim compensation from you separately;

(b) Huawei deducts the balance of your account as liquidated damages, or use such balance to settle disputes and compensate for losses;

(c) Huawei cooperates with the user or competent authority to investigate the complaint (including but not limited to providing your materials);

(d) Huawei takes other measures in accordance with this Agreement.

7. Personal Data and Privacy Protection

7.1 Customer may, in some events as data controller, authorize Huawei to process Customer's personal data for the following purposes:

(a) Sending Ads to target groups defined by Customer. After receiving the personal data shared by Customer, Huawei will select one or more audience groups that meet Customer's request based on Customer's shared personal data and other instructions.

(b) Creating reports based on personal data collected from Customer's Ads landing pages or comparable sites or transferring such data directly to Customer via the AdsPlatform.

(c) Allowing Customer to access and manage personal data collected by Customer using AdsPlatform's landing page tools and forms.

7.1.1 When creating target groups for Ads using the AdsPlatform, Customer shall collect and use personal data about its users with users' prior consent in accordance with Petal Ads' user consent policies (https://developer.huawei.com/consumer/en/doc/development/HMSCore-Guides/publisher-service-consent-settings-0000001075342977) and personalized advertising policies (**https://developer.huawei.com/consumer/en/doc/distribution/promotion/personalized-ad-0000001192925291**).

7.1.2 If Customer collects or transfers data to the AdsPlatform by using any cookies or trackers, Customer is solely responsible for the lawfulness of such use of cookies and trackers, and Customer shall ensure that the user has given valid consent for Customer's use of such technologies in accordance with applicable laws.

7.1.3 The Data Processing Agreement (Attachment 1) is applicable to the processing described in Clause 7.1 herein.

7.2 As the data controller, Customer may, in some circumstances, collect personal data related to served Ads, including but not limited to the Open Advertising ID (OAID, the device ID generated by Huawei), the Google Advertising ID (GAID, the device ID generated by Google), User Agent (UA, a browser user agent), advertiser account ID, app ID, advertising task ID, creative ID, user behavior (such as Ads display, clicks, and downloads), and information about users' device and network, to perform attribution analysis, conversion tracking, remarketing, fraud protection, and effect evaluation in accordance with the following terms:

(a) Customer's use of personal data collected from the AdsPlatform shall respect the privacy of users and comply with applicable data protection laws and regulations.

(b) Customer undertakes to collect and process the data only for the purposes and requirements specified in this Agreement. Without Huawei's prior consent, Customer shall not use or share any such data for any other purposes. For the avoidance of doubt, Customer agrees that the personal data it collects from the AdsPlatform shall not be used to create or augment any user profiles, device profiles, or other profiles.

(c) Customer shall obtain consent from users for processing their data collected from the AdsPlatform for personalized advertising, including remarketing, in accordance with Petal Ads' user consent policies (https://developer.huawei.com/consumer/en/doc/development/HMSCore-Guides/publisher-service-consent-settings-0000001075342977). Customer shall create target groups with data from the AdsPlatform in compliance with Petal Ads' personalized advertising policies (https://developer.huawei.com/consumer/en/doc/distribution/promotion/personalized-ad-0000001192925291).

(d) The application of this Agreement shall not prevent either Party from performing its statutory obligations in accordance with applicable laws.

(e) The Parties acknowledge and agree that they are independent data controllers or the equivalent based on applicable data protection laws.

(f) If Customer designates a third-party company to conduct processing on Customer's behalf, for example, to track conversions, the third-party company is acting as Customer's data processor and Customer shall ensure that the third party complies with the applicable laws, regulations, and requirements and processes the personal data in accordance with this Agreement. Customer is liable for any non-compliance of such third party.

(g) Customer shall have a publicly stated privacy policy in compliance with applicable laws and regulations that accurately describes what personal data about end users is collected by Customer, how Customer collects, uses, discloses, and protects the information, and how end users may access their personal data. The privacy policy shall be displayed prominently in Customer's apps and other services.

(h) Customer shall be solely responsible for resolving the privacy and security protection issues that occur between Customer and the users in respect to Customer's products and services.

(i) It is further acknowledged that, in terms of any personal data, under no circumstances shall either party be a joint controller or have a comparable status, implying joint control and responsibility between parties.

(j) Customer must implement appropriate organizational and technical measures to protect the personal data against loss, misuse, and unauthorized or unlawful access, disclosure, alteration, and destruction.

(k) When Aspiegel SE is providing the Service to Customer, Customer receives personal data as a controller outside the European Union/European Economic Area from any country or region, and said country or region is not recognized by the European Commission as providing an adequate level of protection for personal data, the EU Standard Contractual Clauses (Controller-to-Controller) (Attachment 2) shall be an integral part of this Agreement. Attachment 2 shall prevail in the event of any discrepancies or conflicts between Attachment 2 and this Agreement. Parties agree that:

• the relevant module of the EU Standard Contractual Clauses is "MODULE ONE: Transfer controller to controller";

• in clause 11, the Parties do not choose the optional complaint mechanism;

• in clause 17, the Parties choose Option 1 and the governing law shall be Irish law;

• in clause 18, the Parties choose the courts of Ireland;

• the competent supervisory authority referred to in clause 13 shall be the supervisory authority of Ireland; and

• the scope and nature of the transfer is further set out in the Section B of Annex I later in this document.

To the extent that the data protection laws of the UK apply to the transfer of personal data under this Agreement, the Parties shall execute the UK Addendum, which is incorporated into this Agreement and applies to transfers of personal data outside the UK (except for cases where such data is transferred to a country within the EU/EEA or to another country recognized by the UK as providing an adequate level of data protection). Part 1 of the UK Addendum shall be completed as follows: (i) In Table 1, the "Exporter" is Huawei and Company is the "Importer", and their details are set forth in this Agreement; (ii) in Table 2, the first option shall be selected and the "Approved EU SCCs" are the EU Standard Contractual Clauses referred to in Section 7.2 (k) above; (iii) in Table 3, the information is as provided in Annex I (A and B) and Annex II to the "Approved EU SCCs" (as set out in Attachment 2 of this Agreement); and (iv) in Table 4, the "Exporter" can terminate the UK Addendum.

(l) When Huawei Services (Hong Kong) Co., Limited is providing the Service to Customer and Customer receives personal data as a controller outside Singapore from

any country (except Russia), the Data Transfer Agreement (Attachment 3) shall be an integral part of this Agreement.

(m) When Huawei Services (Hong Kong) Co., Limited is providing the Service to Customer and Customer is processing the personal data that is collected and stored in databases within the territory of Russia, both the Data Processing Agreement (Attachment 1) and the Data Transfer and Processing Agreement (Attachment 4) shall be an integral part of this Agreement.

7.3. If Customer has been legally authorized by another company (hereinafter referred to as "Client") to conduct the processing activities subject to Sections 7.1 and/or 7.2 on their behalf:

(a) Parties acknowledge that for the purposes of the aforementioned Sections, and any attachments referenced therein, Client is the data controller (defined as "Customer" in 7.1 and 7.2);

(b) Company authorizes Huawei, as separate data processor, to conduct the processing activities subject to Section 7.1 on behalf of Client in accordance with the Data Processing Agreement (Attachment 1) which shall be effective between the Client and Huawei upon signing of this Agreement; and

(c) Customer shall inform Client about the processing of Client's personal data taking place under this Agreement by Huawei and contractually require Client to comply with the terms set forth in Sections 7.1 and 7.2.

8. Disclaimer

8.1 No conditions, warranties or other terms apply to any Service or to any other goods or services supplied by Huawei or its Affiliates under this Agreement unless expressly set out in this Agreement To the fullest extent permitted by law, no implied conditions, warranties or other terms apply (including any implied terms as to satisfactory quality, fitness for purpose or conformance with description). None of Huawei, its Affiliates or Huawei's Partners makes any guarantee in connection with the Services or Service results. To the fullest extent permitted by law, Huawei makes no promise to inform Customer of defects or errors.

8.2 THIRD PARTY SERVICES (E.G., DMP, ANALYTICS AND INVALID TRAFFIC DETECTION SERVICES) MAY BE PROVIDED FROM OR ACCESSED THROUGH PETAL ADS PLATFORM, WHICH MAY BE SUBLICENSED THROUGH HUAWEI OR LICENSED DIRECTLY FROM THIRD PARTY SERVICE PROVIDERS.

HUAWEI EXPLICITLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESS OR IMPLIED, AS TO SAID THIRD PARTY SERVICES, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES, DUTIES, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, REASONABLE CARE, WORKMANLIKE EFFORT, RESULTS, LACK OF NEGLIGENCE, OR ACCURACY OR COMPLETENESS OF RESPONSES.

9. Breach and Termination

9.1 If either Party (the "Defaulting Party") violates the obligations specified in this Agreement or relevant management regulations, the Defaulting Party shall immediately stop its breach of this Agreement and compensate for any and all direct economic losses of the other Party (the "Non-Defaulting Party") within ten (10) working days upon receiving a written notice of the Non-Defaulting Party demanding for curing said breach.

9.2 If the Defaulting Party fails to cease the breach or perform its obligations, in addition to the liquidated damages received, the Non-Defaulting Party also has the right to terminate this Agreement by issuance a notice of termination in writing to the Defaulting Party.

9.3 This Agreement shall be terminated on the same day when either Party terminates the HUAWEI Developers Service Agreement or the HUAWEI Partner Paid Service Agreement.

9.4 If Huawei decides not to provide the Services any more, or decides to change the Services, or does not intend to enter into an agreement with you on providing the Services to you, Huawei has the right to terminate this Agreement at any time after sending a notice to you at least thirty (30) days in advance.

9.5 Notwithstanding anything to the contrary contained herein, in no circumstance shall Huawei be held liable for damages under the Ads Terms or arising out of or related to performance of the Ads Terms for any given event or series of connected events in the aggregate of more than the amount payable to Huawei by Customer under this Agreement in the thirty (30) days before the date of the activity first giving rise to the claims.

10. Changes to This Agreement

10.1 Notwithstanding any other provisions of the Agreements, Huawei may make non-material changes to this Agreement at any time without notice, but Huawei will provide advance notice of any material changes to this Agreement. The Agreement will be posted on the AdsPlatform. The changes to this Agreement will not apply retroactively

and will become effective 7 days after posting. However, changes made for legal reasons shall be effective immediately upon notice. Either Party may terminate this Agreement at any time with notice to the other Party, but (i) campaigns not cancelled under Section 4 and new campaigns may be run and reserved and (ii) continued Service Use is, in each case, subject to Huawei's terms and conditions then in effect for the Services (available on AdsPlatform). Huawei may suspend Customer's ability to participate in the Services at any time. In all cases, the running of any Customer campaigns after termination is in Huawei's sole discretion.

11. Distribution Area and Signing Huawei Entity

11.1 Please refer to the Clause of "Distribution Area and Signing Huawei Entity" (Clause 8) of the HUAWEI Partner Paid Service Agreement.

12. Governing Laws and Dispute Resolution

12.1 Please refer to the Clause of "Governing Law and Dispute Resolution" (Clause 9) of the HUAWEI Partner Paid Service Agreement.

12.2 Customer agrees that regardless of which company enters into this Agreement, if Customer's Business Area is a country/region with legal requirements beyond those set forth in this Agreement, Customer undertakes to carry out their activities in accordance with such requirements. If Huawei is held liable for Customer's culpable violation of the legislation of the country/region in which its Business Area is located, Customer undertakes to hold harmless and indemnify Huawei against any and all the losses.

13. Miscellaneous

13.1 You and Huawei shall comply with any and all applicable laws during the performance of this Agreement.

13.2 The contact persons of yours and Huawei's shall take charge of the liaison and coordination between you and Huawei during the fulfillment of this Agreement. All notices relating to this Agreement shall be in written form.

13.3 These Terms do not create any agency, partnership or joint venture among the Parties.

13.4 Any and all appendixes hereto constitute an integral part of this Agreement. This Agreement is the Parties' entire agreement relating to their subject matter and supersedes any prior or contemporaneous agreements on those subjects.

13.5 Huawei may, at its sole discretion, subcontract any rights or obligations under this Agreement, in whole or in part, to any third party, or assign this Agreement (with any and all supplementary agreements of this Agreement) to any Huawei Affiliate upon prior written notice. You shall not transfer your rights and obligations under this Agreement without Huawei's prior written consent.

13.6 If any part of this Agreement is deemed as invalid by a court or other competent authorities, any other provisions shall not be affected and shall continue to be enforceable and binding upon the Parties to the fullest extent permitted by applicable law.

13.7 If one or more clauses or part of them in this Agreement are held invalid for any reason, such invalid content does not compromise the effectiveness of any other clauses hereof, and such invalid content shall be deemed to be non-existent from the beginning to the end.

13.8 Neither Party will be treated as having waived any rights by not exercising (or delaying the exercise of) any rights under the Agreement.

Attachment 1

Data Processing Agreement

1.1 This Data Processing Agreement (DPA) reflects the Parties' agreement with respect to the terms governing the Processing and security of Customer Data under the Agreement. This DPA shall apply to the Parties if and insofar as Huawei Processes Personal Data on behalf of Customer as a Processor when providing Service to Customer under the Agreement. In the event of a conflict, this DPA shall take precedence over the Agreement. In the event of a conflict between the DPA and the Standard Contractual Clauses (in Annex 2) or the Data Transfer Agreement (in Annex 3), the latter shall take precedence over this DPA.

2. Definitions

2.1 Capitalized terms used but not defined in this DPA have the meanings set out in the Agreement. In this DPA, unless stated otherwise:

Applicable Laws and Regulations means any privacy or data protection laws, regulations and rules that apply to the Processing of Customer Personal Data at each given time, such as the GDPR and any laws and rules which supersede the former, as applicable.

Customer Data means Personal Data provided by Customer.

Customer End Users means the users of Customer's services (for example, the users of a Customer app).

Customer Personal Data means the Personal Data contained within the Customer Data.

EEA means the European Economic Area.

GDPR means 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, and repealing Directive 95/46/EC.

Huawei's Third Party Auditor means a Huawei-appointed, qualified and independent third Party auditor, whose then-current identity Huawei will disclose to Customer.

ISO 27001 Certification means an ISO/IEC 27001:2013 certification or a comparable certification for the Audited Services.

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed by or otherwise Processed by Huawei. "Personal Data Breach" will not include unsuccessful Security Incident described in Clause 5.7.

Security Measures has the meaning given in Clause 4.1.1.

Security Documentation means all certificates made available by Huawei under Clause 4.4.1.

Standard Contractual Clauses mean the contractual clauses issued by the European Commission by implementing decision 2021/914 of June 4, 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

Sub-processors means third parties authorized under this DPA to have logical access to and Process Customer Data in order to provide parts of the Services.

Third Country means a country that is neither part of the EEA nor has been declared adequate by a decision of the European Commission according to the mechanism lined out in Article 45 GDPR.

2.2 The terms "Personal Data", "Data Subject", "Processing", "Controller", "Processor" and "Supervisory Authority" as used in this DPA have the meanings given in the Applicable Laws and Regulations. Should any of the terms in 2.1 have a different meaning under Applicable Laws and Regulations, then the meaning given to the term in the Applicable Laws and Regulations shall prevail.

3. Roles, Scope of Processing, and General Obligations

3.1 The Parties acknowledge and agree that:

3.1.1 For the Processing of Personal Data under this DPA, Customer shall be regarded as the Controller and Huawei shall be regarded as the Processor as defined under Applicable Laws and Regulations.

3.1.2 Each Party undertakes to comply with its obligations under the Applicable Laws and Regulations. Each Party is solely responsible for compliance with the obligations of the Applicable Laws and Regulations which apply to it. As between the Parties, Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired the Personal Data.

3.1.3 In order to perform the Service to Customer, Huawei shall Process Customer Personal Data.

3.1.4 Processor shall Process Personal Data only in accordance with this DPA, and/or to the extent necessary to provide the Service to Customer under the Agreement.

3.1.5 The Agreement and this DPA shall be seen as instructions from Customer to Huawei for the Processing of Personal Data. Additional instructions outside the scope of the Agreement or this DPA (if any) require prior written Agreement between Customer and Huawei, including Agreement on any additional fees payable by Customer to Huawei for carrying out such instructions. Customer is entitled to terminate this DPA and the Agreement if Huawei refuses to follow instructions reasonably required by Customer that are outside the scope of, or changed from, those given in this DPA or the Agreement.

3.1.6 Huawei will comply with the instructions described in Clause 3.1.5 unless applicable law to which Huawei is subject requires other Processing of Customer Personal Data by Huawei, in which case Huawei will inform Customer (unless that law prohibits Huawei from doing so on important grounds of public interest).

3.1.7 In order to perform the Service to Customer, Huawei shall Process the Personal Data to comply with Applicable Laws and Regulations, and other laws that Huawei may be subject to.

3.2 Without prejudice to Clause 3.1.1, if Customer is a Processor, Customer warrants to Huawei, which will be acting as Sub-processor, that Customer's instructions and actions with respect to that Customer Personal Data, including its appointment of Huawei as another Processor, have been authorized by the relevant Controller.

3.3 If Customer requests Huawei to comply with any privacy or data protection laws and regulations that would otherwise not apply to Huawei's Processing of Customer Personal Data, Huawei reserves the right to, at its sole discretion, (i) either reject the Customer requirement, if compliance is commercially unreasonable; or (ii) comply with the new requirements, if commercially reasonable, upon payment of a fee determined by Huawei.

4. Data Security

4.1 Huawei's Security Measures, Controls and Assistance

4.1.1 Huawei's Security Measures

Huawei implements the appropriate physical, technical, and organizational security measures to protect Customer data throughout its lifecycle according to common industry standards to prevent data breach, damage, or loss and ensure security, confidentiality, integrity and availability of Customer data. The measures are including but not limited to communication and storage encryption, data center access control, access minimization, and recording access to Personal Data systems as detailed on Annex 1. In order to respond to the new identified security threats and vulnerabilities the security measures will be updated in time to time in such manner that overall security of the services is ensured.

4.1.2 Security Compliance by Huawei Staff and Sub-processors

Huawei will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Sub-processors to the extent applicable to their scope of

performance, including ensuring that all persons authorized to Process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.1.3 Additional Security Controls

As an additional security control, Huawei validates the efficiency of the security measures of Service via periodical security tests by internal or independent third party as well as continues to upkeep the relevant security certificates.

4.1.4 Huawei's Security Assistance

Customer agrees that Huawei will (taking into account the nature of the Processing of Customer Personal Data and the information available to Huawei, and any restrictions on disclosing the information, such as confidentiality) assist Customer in ensuring compliance with any of Customer's obligations in respect of security of Personal Data and Personal Data Breaches, including Customer's obligations pursuant to Applicable Laws and Regulation, including, if applicable, Articles 32 to 34 (inclusive) of the GDPR, by:

(a) Implementing and maintaining the Security Measures in accordance with Clause 4.1.1 (Huawei's Security Measures);

(b) Complying with the terms of Clause 5 (Personal Date Breach); and

(c) Providing Customer with the Security Documentation in accordance with Clause 4.4.1 (Reviews of Security Documentation) and the information contained in the applicable Agreement including this Data Processing Amendment.

4.2 Customer's Security Responsibilities and Assessment

4.2.1 Customer's Security Responsibilities

Customer agrees that, without prejudice to Huawei's obligations under Clause 4.1 (Huawei's Security Measures, Controls and Assistance.) and Clause 5 (Personal Data Breach):

(a) Customer is solely responsible for its use of the Service, including:

I. Making appropriate use of the Service to ensure a level of security appropriate to the risk in respect of the Customer Data;

II. Securing the account authentication credentials, systems and devices Customer uses to access the Service;

III. Backing up its Customer Data as appropriate; and

(b) Huawei has no obligation to protect copies of Customer Data that Customer elects to store or transfer outside of Huawei's and its Sub-processors' systems (for example, offline or on-premises storage).

4.2.2 Customer's Security Assessment

4.2.2.1 Customer is solely responsible for reviewing the Security Documentation and evaluating for itself whether the Services, the Security Measures, the Additional Security Controls and Huawei's commitments under this Clause 4 (Data Security) will meet Customer's needs, including with respect to any security obligations of Customer under Applicable Laws and Regulations.

4.2.2.2 Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing of Customer Personal Data as well as the risks to individuals) the Security Measures implemented and maintained by Huawei as set out in Clause 4.1.1 (Huawei's Security Measures) provide a level of security appropriate to the risk in respect of the Customer Data.

4.3 Security Certifications and Reports

Huawei will do the following to ensure the continued effectiveness of the Security Measures:

4.3.1 Huawei will use independent external auditors to verify the adequacy of its security measures.

4.3.2 The audit will be performed (i) according to ISO 27001 standards or such other substantially equivalent standards; (ii) at reasonable intervals; and (iii) by independent third party auditors at Huawei's selection and expense.

4.3.3 The audit will generate (a) relevant certificates (Security Documentation); and (b) an audit report, which will be Huawei's confidential information.

4.4 Reviews and Audits of Compliance

4.4.1 Reviews of Security Documentation

In addition to the information contained in this DPA, upon Customer's request, and provided that the parties have an applicable NDA in place, Huawei will make available Security Documentation and other documentation Huawei deems necessary to demonstrate compliance by Huawei with its obligations under this DPA.

4.4.2 Customer's Audit Rights

If Customer's review of Huawei's Security Documentation in accordance with Clause 4.4.1 is not enough for Customer to reasonably verify Huawei's compliance with its obligations under this DPA:

(a) Huawei will allow Customer or an independent auditor appointed by Customer to conduct an audit (including an inspection) to verify Huawei's compliance with its obligations under this DPA in accordance with Clause 4.4.3 (Additional Business Terms for Reviews and Audits). Huawei will contribute to such audits as described in Clause 4.3 (Security Certifications and Reports) and this Clause 4.4 (Reviews and Audits of Compliance).

(b) If Customer has entered into Standard Contract Clauses as described in Clause 8.2 (Data Locations and Transfers), Huawei will, without prejudice to any audit rights of a Supervisory Authority under such Standard Contract Clauses, allow Customer or an independent auditor appointed by Customer to conduct audits as described in the Standard Contract Clauses in accordance with Clause 4.4.3 (Additional Business Terms for Reviews and Audits).

4.4.3 Additional Business Terms for Reviews and Audits

4.4.3.1 Customer must send written requests for reviews or audits under Clauses 4.4.1 and 4.4.2 to **contact us**.

4.4.3.2 Following receipt by Huawei of a request under Clause 4.4.3.1, Huawei and Customer will discuss and agree in advance on the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit under Clause 4.4.2.

4.4.3.3 The audit will include only material necessary to verify Huawei's compliance with this DPA and it will not include any material which Huawei is obligated to keep confidential based on a contractual requirement.

4.4.3.4 Huawei may charge a fee (based on the reasonable costs occurred on Huawei) for any audit under Clause 4.4.2. Huawei will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. Customer

will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

4.4.3.5 Huawei may object in writing to an auditor appointed by Customer to conduct any audit under Clause 4.4.2 if the auditor is, in Huawei's reasonable opinion, not suitably qualified or in dependent, a competitor of Huawei, or otherwise manifestly unsuitable. Any such objection by Huawei will require Customer to appoint another auditor or conduct the audit itself.

5. Personal Data Breach

5.1 Where required by Applicable Laws and Regulations, Huawei shall notify Customer without undue delay after becoming aware of a Personal Data Breach. Taking into account the information reasonably available to it, Huawei shall use its best commercial efforts to address the following in the notification:

(a) Description of the nature of the Personal Data Breach including, where possible, the categories and approximate number of Data Subjects concerned;

(b) Name and contact details of Huawei's data protection officer or other point of contact where more information can be obtained;

(c) Description of the likely consequences of the Personal Data Breach;

(d) Description of the measures taken to address the Personal Data Breach, including where appropriate measures to mitigate its possible adverse effects.

5.2 Where it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5.3 Huawei will promptly take the necessary and appropriate actions to investigate, mitigate and remediate any effects of a Personal Data Breach, and provide assistance to Customer to ensure that Customer can comply with specific obligations under Data Protection Legislation it may be subject to in relation to the Personal Data Breach.

5.4 Notification of any Data Incident will be delivered to the Notification Email Address or, at Huawei's discretion, by direct communication (for example, by phone call or an in-person meeting). Customer is solely responsible for ensuring that the Notification Email Address is current and valid.

5.5 Huawei will not assess the contents of Customer Data in order to identify information subject to any specific legal requirements. Without prejudice to Huawei's obligations under this Clause 6 (Assistance to the Controller), Customer is solely

responsible for complying with incident notification laws applicable to Customer and fulfilling any third party notification obligations related to any Data Incident(s).

5.6 Huawei's notification of or response to a Data Incident under this Clause 6 (Assistance to the Controller) will not be construed as an acknowledgement by Huawei of any fault or liability with respect to the Data Incident.

5.7 Customer agrees that an unsuccessful Security Incident will not be subject to this Clause 5 (Personal Data Breach). An unsuccessful Security Incident is one that results in no unauthorized access to Customer Data or to any of Huawei's equipment or facilities storing Customer Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.

6. Assistance to the Controller

6.1 To the extent required by Applicable Laws and Regulations and taking into account the nature of the Processing and the information reasonably available, Huawei shall provide Customer with reasonable assistance with regards to:

6.1.1 ensuring compliance with Controller's obligations pursuant to Applicable Laws and Regulations;

6.1.2 making available to Controller all reasonable information necessary to demonstrate compliance with Applicable Laws and Regulations;

6.1.3 where applicable, performing the necessary data protection impact assessments and prior consultation procedures as mentioned in articles 35 and 36 GDPR, respectively;

6.1.4 providing the information contained in the Agreement including this DPA.

6.2 Where assistance requested by Customer and provided by Huawei in accordance with Clause 6.1 is not part of the Service and Huawei's regular activities related thereto, Huawei may charge Customer for the reasonable costs occurring on Huawei for such assistance.

6.3 Where required by Applicable Laws and Regulations, Huawei shall maintain a record of all categories of Processing activities carried out on behalf of Customer. Accordingly Customer will, where requested, provide such information to Huawei.

6.3.1 The records of processing shall contain the information required in article 30.2 of the GDPR, as applicable.

6.3.2 Huawei shall make such information available to the Supervisory Authorities, on request.

6.3.3 Huawei shall maintain the records of processing in electronic form.

7. Data Subject Rights

7.1 Huawei shall reasonably cooperate with Customer and assist Customer with respect to any action taken relating to fulfilling its obligations towards Data Subjects requests. As far as reasonably possible and taking into account the nature of the Processing, the information available to Huawei, industry practices and costs, Huawei will implement appropriate technical and organizational measures to provide Controller with such cooperation and assistance. Huawei may charge Customer for the reasonable costs occurring on Huawei for any assistance which Huawei considers to go beyond the aforementioned cooperation and assistance measures.

8. Data Location and Transfers

8.1 Huawei shall store Customer Data solely in data centers communicated to Customer by Huawei. The Customer Personal Data is located in data centers determined by the area of distribution selected by Customer. When the area of distribution is:

• Australia, New Zealand, Europe or North America: user data will be stored in data centers located in the EU/EEA.

• Russia: user data will be stored in data centers located in the Russia.

• Africa, Latin America, Oceania (excluding Australia and New Zealand), Central Asia, South Asia, Southeast Asia, Western Asia, or Northern Asia, your data will be stored in data centers located in Singapore and/or Hong Kong (China), and can be accessed for maintenance from China or India.

• Chinese mainland, user data will be stored in data centers located in People's Republic of China.

8.2 Due to the Huawei entity providing the Service establishment location, and the Customer establishment location or the Customer Data Subjects' location, the Processing by Huawei may be subject to the Data Transfer Agreement in Annex 3. In addition, in case that Customer is established in a Third Country, the Parties acknowledge that:

• the Parties shall be deemed to have executed the Standard Contractual Clauses Module FOUR: Transfer processor to controller (Annex 2) by executing this Agreement.

- Huawei is the "data exporter" and Customer is the "data importer" in respect of the Clause 1 and Annex 1 of the Standard Contractual Clauses;

- in clause 7, the Parties choose to include the "docking clause";

- in clause 11, the Parties do not choose the optional complaint mechanism;

- in clause 17, the Parties choose Option 1 and the governing law shall be the law of Ireland;

- in clause 18, the country of the applicable court in respect of any disputes arising from Standard Contractual Clauses shall be as the Irish Courts with jurisdiction in Dublin;

- the information required for Section B of Annex I is documented in connection with the Annex later in document and here; and

- the competent supervisory authority is the Irish Data Protection Commission.

For avoidance of doubt, the Data Transfer Agreement applies only if the GDPR does not apply to the Processing. Without prejudice to Clause 9.2, Huawei may transfer data if it is required by applicable law to which Huawei is subject, provided that Huawei informs Customer of that legal requirement before Processing, unless the law prohibits such information on important grounds of public interest.

8.3. If the transfer of data in accordance to Clause 8.2 or 9.2 requires under Applicable Laws and Regulations an approval from an authority, Customer shall obtain the necessary approval prior to such transfer. Customer and Huawei agree to deposit and/or file (as applicable) a copy of this Agreement with any relevant authority if it so requests or if such filing and/or deposit is required under the Applicable Laws and Regulations.

9. Sub-processors

9.1 Customer provides Huawei hereby with a general authorization to engage Sub-Processors. Where required by Applicable Laws and Regulations, Huawei will impose data protection obligations on the Sub-Processors which are substantially the same as those set out in this DPA, in particular in relation to the implementation of appropriate technical and organizational measures. A list of the Sub-Processors currently engaged by Huawei to carry out Processing activities are made available at **https://developer.huawei.com/consumer/en/devservice/doc/10126**, and Customer is deemed to have accepted all Sub-Processors included in the list on the effective date of this Agreement.

Huawei shall make available, the information regarding any changes concerning the engagement or replacement of a Sub-Processor, to Customer by appropriate means Huawei provides to Customer.

9.2 If a Sub-processor, engaged in accordance with Clause 9.1 above, is established or otherwise Processes Customer Data outside the country where Customer and/or Huawei are located and a data transfer agreement is required under Applicable Laws and Regulations, Customer hereby authorizes Huawei, in the name of and on behalf of Customer, to enter into a data processing agreement with such Sub-Processor that incorporates the Data Transfer Agreement as provided by Annex 3. If Applicable Laws and Regulations requires entering into Standard Contractual Clauses, MODULE THREE: "Transfer processor to processor" of the Standard Contractual Clauses with the Sub-processors established in Third Countries is incorporated. Huawei's Sub-processors will act as "data importers" and Huawei will act as "data exporter" according to Clause 1 and Annex 1 of the Standard Contractual Clauses. Customer shall take into account Clause 8.3.

9.3 Customer shall have the right to object to a new Sub-Processor with reasonable grounds by written notice to Huawei within 14 days after becoming aware of the new Sub-Processor. If Huawei chooses to engage the new Sub-Processor despite Customer's objection in accordance with this Clause 9.3, Customer shall have the right to, terminate the Agreement.

9.4 For the avoidance of doubt, in the event Huawei uses Sub-Processors, Huawei shall, pursuant to Applicable Laws and Regulations, remain fully liable to Customer for the fulfilment of its obligations under this DPA.

10. Liability

10.1 Each Party is liable for damages incurred by the other Party which are caused directly by a Party's breach of the commitments made in this DPA, subject to the limitations and exclusions of liability agreed in the Agreement.

10.2 Provided that Customer is not in breach of this DPA, Huawei shall indemnify and keep Customer harmless from any claim or proceedings (including reasonable legal fees) brought against Customer by a third party as a result of a breach by Huawei of its data protection commitments in this DPA. Huawei shall be entitled to take control of the defense and investigation of such claim, or any proceedings, and shall employ counsel of its choice to handle and defend the same, at Huawei's sole cost and expense.

10.3 Notwithstanding any other provisions in this DPA, neither Party shall be liable to the other Party for:

(a) loss of profits;

(b) loss of business;

(c) loss of revenue;

(d) damage to goodwill or any similar losses;

(e) anticipated savings;

(f) loss of use; and

(g) any punitive, other indirect or, consequential loss or damage.

11. Changes to this DPA

11.1 From time to time, Huawei may change any URL referenced in this DPA and the content at any such URL.

11.2 Huawei may change this DPA if the change:

(a) is expressly permitted by this DPA, including as described in Clause 11.1;

(b) reflects a change in the name or form of a legal entity;

(c) is required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency; or

(d) does not: (i) result in a degradation of the overall security of the Services; (ii) expand the scope of, or remove any restrictions on, Huawei's Processing of Customer Personal Data, as described in Clause 3.1 (Huawei's Compliance with Instructions); and (iii) otherwise have a material adverse impact on Customer's rights under this DPA, as reasonably determined by Huawei.

11.3 If Huawei intends to change this DPA under Clause 11.2(c) or (d), Huawei will inform Customer at least 30 days (or such shorter period as may be required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency) before the change will take effect. If Customer objects to any such change, Customer may terminate the Agreements by deleting their HUAWEI ID within ninety (90) days of being informed by Huawei of the change.

12. Term and Termination

12.1 This DPA shall take effect from the Effective Date and, continues until the termination or expiration of the Agreement. Notwithstanding the termination or the expiration of the Agreement, the DPA will remain in effect until, and automatically expire upon, deletion of all Customer Data by Huawei as described in clause 12.2 below.

12.2 Huawei shall, upon termination or expiration of this DPA, delete all Customer Data (including existing copies) from Huawei's systems in accordance with Applicable Laws and Regulations and without undue delay.

12.3 Customer acknowledges and agrees that Customer will be responsible for exporting to its own systems, before the Term expires, or the termination of the DPA, any Customer Data it wishes to retain afterwards.

ANNEX 1: Security Measures

As from the Effective Date, Huawei will implement and maintain the Security Measures set out in this ANNEX 1. Huawei may update or modify such Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Service.

1. Data Center and Network Security

Huawei uses third party data centers that are geographically distributed within selected region, in which the cloud provider is required to have sufficient security measures in place.

2. Data

(a) Data Storage and Isolation.

Huawei stores data on multi-tenant environment on third party servers. The data and file system architecture are replicated between multiple geographically dispersed data centers. Huawei isolates Customer's data logically.

(b) Decommissioned Disks and Disk Erase Policy. Disks containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned ("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes that are handled by the Data Center operator.

3. Access Control

3.1 Data Access by Customer

Customer's administrators must authenticate themselves via a central authentication system with two-factors authentication in order to administer the Service.

3.2 Internal Data Access Policy.

Huawei employs a centralized access management system that is integrated to LDAP system to control personnel access to production servers, and only provides role-based access to a limited number of authorized personnel. Huawei requires the use of unique user IDs, strong passwords, two-factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; and a need to know basis.

4. Personnel Security

4.1 Huawei personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Huawei conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

4.2 Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Huawei's confidentiality and privacy policies. Personnel are provided with security training and their knowledge of security and privacy policies are evaluated periodically. Furthermore the latest security news from the world are delivered to personnel periodically to improve their awareness. Personnel handling Customer Data are required to complete additional requirements appropriate to their role

(e.g., Huawei Cyber Security Certification). Huawei's personnel will not process Customer Data without authorization.

ANNEX 2

STANDARD CONTRACTUAL CLAUSES
MODULE FOUR

Processor to Controller

This Annex 2 shall incorporate the EU Standard Contractual Clauses (Module four, transfer: processor to controller), as further specified above in section 8.2, and as set out at: **https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en**

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data Exporter(s): Huawei as defined in the Agreement that will be processing Customer Data on its behalf as per the DPA, or the Sub-Processor engaged by Huawei, as applicable.

Address: 3rd floor, Mespil Court, Mespil Road, Ballsbridge, Dublin 4, D04 E516, Ireland, with company number 561134, at the Companies Registration Office, Ireland

Contact person's name, position and contact details: Joerg Thomas, Director, DPO Office, dpo@huawei.com Activities relevant to the data transferred under these Clauses: Detailed in Annex I B

Signature and date: _____

Role (controller/processor): processor

Data Importer(s): Customer, who is the Controller of Customer Data, who is either established in the EEA, and/or offers goods/services to Data subjects established in the EEA, or monitors their behavior which taking place in the EEA.

Name: your name or, as the case may be, the name of the company you represent

Address: your place of business or, as the case may be, the place of business of the company you represent.

Contact person's name, position and contact details: our contact details and information as you have provided them in context of the Agreement and your Developer account

Activities relevant to the data transferred under these Clauses: Detailed in Annex I B

Signature and date: _____

Role: controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Customer End Users

Categories of personal data transferred

Conversion tracking data about ads behavior.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A

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

Customer decides when to use Petal Ads tracking features.

Nature of the processing

Maintain Customer data, create reports, etc. about ads conversion.

Purpose(s) of the data transfer and further processing

As defined in Section 7.1 of the Agreement.

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

Customer can manage and erase data via Petal Ads.

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

Data Center and operations and maintenance related sub-processors:

https://developer.huawei.com/consumer/en/doc/distribution/app/aspgsubprocessor

C. COMPETENT SUPERVISORY AUTHORITY

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

Irish Data Protection Commission

ANNEX II

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

The measures are provided in the DPA's Clause 4 Data Security and Annex 1 Security Measures.

ANNEX 3: Data Transfer Agreement (Processors)

Only when GDPR does not apply

Name of the data exporting organization:

Customer as defined in Agreement

(the data exporter)

And

Name of the data importing organization:

Huawei

(the data importer)

Each a "party"; together "the parties".

Clause 1: Definitions

For the purposes of this Data Transfer Agreement ("DTA"):

(a) Applicable Laws and Regulations means any privacy or data protection laws, regulations and rules that apply to the processing of Customer Personal Data at each given time;

(b) Customer Data means Personal Data provided by Customer or Customer End Users via the Service;

(c) Customer End Users means the users of Customer's services (for example, the users of a Customer app);

(d) Customer Personal Data means the Personal Data contained within the Customer Data;

(e) "Personal Data", "Special Categories of Data", "Process/Processing", "Controller", "Processor", "Data Subject", "Sub-processing", "Sub-processor" and "Supervisory Authority" shall have the same meaning as in the EU General Data Protection Regulation ("GDPR"), unless the term is differently defined by applicable data protection law; and

Any terms not defined in this DTA shall have the meaning given to these terms (i) in the Data Processing Agreement ("DPA") to which this DTA is attached or (ii) in the Applicable Laws and Regulations.

Clause 2: Details of the Transfer

The details of the transfer (as well as the Personal Data covered) are specified in Appendix 1.

Clause 3: Obligations of the Data Exporter

The data exporter agrees and warrants:

(a) that the Processing, including the transfer itself, of the Personal Data has been and will continue to be carried out in accordance with the relevant provisions of the Applicable Laws and Regulations (and, where applicable, it has notified the relevant authorities of the country in which the data exporter is established) including, if required by the Applicable Laws and Regulations, gaining consent from the Data Subject before transfer of the Personal Data and informing the Data Subject of the following:

(i) the name of the data importer;

(ii) the contact details of the data importer;

(iii) the types of Personal Data to be transferred;

(iv) the purpose for which the Personal Data is being transferred; and

(v) any other information required by the Applicable Laws and Regulations;

(b) that after assessment of the requirements of the Applicable Laws and Regulations, the technical and organizational security measures specified in the DPA's Clause 4 (Data Security) and Annex 1 (Security Measures) are appropriate to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing, and that these measures ensure a level of security appropriate to the risks presented by the Processing

and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(c) that, if the transfer involves Special Categories of Data, the Data Subject has, prior to the transfer, been informed of or consent to the transfer of his or her data outside the country in which the data exporter is established in accordance with Applicable Laws and Regulations;

(d) the data exporter agrees to obtain the prior approval of and deposit a copy of this DTA with the Supervisory Authority if it so requests or if such deposit is required under the applicable data protection law; and

(e) where required by Applicable Laws and Regulations, that Customer Data be maintained for a certain period of time.

Clause 4: Obligations of the Data Importer

The data importer agrees and warrants:

(a) to Process the Personal Data only on behalf of the data exporter in accordance with the instructions of the data exporter, this DTA (in particular Appendix 1) and, where required, in accordance with applicable laws, governmental or regulatory bodies, or an order by a court, in which case it shall notify the data exporter as soon as practicable before complying with such law or order; if it cannot provide compliance with the data exporter's instructions or this DTA, for whatever reasons, it agrees to inform the data exporter without undue delay of its inability to comply, in which case the data exporter is entitled to suspend the transfer of Personal Data and the parties shall work together in good faith to agree any steps which have to be taken to allow the data importer to continue to provide such compliance;

(b) where required by the Applicable Laws and Regulations of the country of the data exporter (and in accordance with Clause 11), to protect the Personal Data it receives at a standard that is comparable to that under the Applicable Laws and Regulations of the country of the data exporter; at the request of the data importer, the data exporter shall inform the data importer about the obligations under such Applicable Laws and Regulations that go above and beyond the obligations arising from this DTA or any other data processing agreement entered into by the data exporter and the data importer;

(c) to comply with the requirements under Applicable Laws and Regulations of its country of incorporation, such as those on data transfers;

(d) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the

DTA and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by this DTA, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and the parties shall work together in good faith to agree any steps which have to be taken to allow the data importer to continue to provide such compliance;

(e) that it has implemented the technical and organizational security measures specified in the DPA's Clause 4 (Data Security) and Annex 1 (Security Measures) before Processing the Personal Data transferred to prevent unauthorized or accidental access, collection, use, disclosure, copying, modification, disposal or destruction of Personal Data, or other similar risks;

(f) that it will without undue delay notify the data exporter about:

(i) any legally binding request for disclosure of the Personal Data, including by a law enforcement authority, unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any actual or suspected loss, theft, damage, accidental or unauthorized access or Processing;

(iii) any request received directly from a Data Subject, without responding to that request, unless it has been otherwise authorized or required to do so; and

(iv) any complaint received related to the Processing of the Personal Data, and comply with any instructions of data exporter in connection therewith.

(g) to deal promptly and properly with all inquiries from the data exporter relating to its Processing of the Personal Data subject to the transfer, to provide reasonable cooperation in responding to enquiries from the relevant Supervisory Authority or other relevant authority within the country of the data exporter, and to abide by the legally binding advice of the relevant Supervisory Authority with regard to the Processing of the data transferred;

(h) at the request of the data exporter or a relevant authority within the country of the data exporter, to submit its data Processing facilities used to Process Personal Data pursuant to the DTA, for audit;

(i) that, in the event of Sub-processing, it will previously inform the data exporter and obtain the data exporter's agreement; and

(j) that the Processing services by the Sub-processor will be carried out in accordance with Section 7.

Clause 5: Liability

1. The data importer may not rely on a Sub-processor's breach of its obligations in order to avoid the data importer's own liabilities.

2. The parties agree that if one party is held liable for a violation of this DTA committed by the other party (and for the avoidance of doubt, in the case of the data importer, violation of this DTA committed by any Sub-processor), the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred. Indemnification is contingent upon:

(a) the data exporter promptly notifying the data importer of a claim; and

(b) the data importer being given the possibility to cooperate with the data exporter in the defense and settlement of the claim.

Clause 6: Governing Law

This DTA shall be governed by the law of the country in which the data importer is established.

Clause 7: Sub-processing

The data exporter provides the data importer a general authorization to engage Sub-Processors. Where the data importer subcontracts its obligations under this DTA, with the consent of the data exporter, it shall do so only by way of a written agreement with the Sub-processor which imposes the same obligations on the Sub-processor as are imposed on the data importer under this DTA. Where the Sub-processor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the Sub-processor's obligations under such agreement.

A list of the Sub-Processors currently engaged by the data importer to carry out Processing activities shall be made available to the data exporter and the data exporter is deemed to have accepted all Sub-Processors included in the list on the Effective Date. For any other Sub-Processor, the data exporter shall have the right to object to a new Sub-Processor with reasonable grounds by written notice to the data importer within 14 days after becoming aware of the new Sub-Processor. If the data importer chooses to engage the new Sub-Processor despite the data exporter's objection, the data exporter

shall have the right to, terminate this DTA and the agreement which incorporates this DTA.

For the avoidance of doubt, in the event the data importer uses Sub-Processors, the data importer shall, pursuant to Applicable Laws and Regulations, remain fully liable to the data exporter for the fulfilment of its obligations under this DTA.

Clause 8: Data Transfers

The data exporter provides the data importer a general authorization to transfer the Personal Data outside of the data importer's country of incorporation provided such transfer complies, specifically, with the Clause 4(a) and all other clauses of this DTA and with the Applicable Laws and Regulations. The data processing agreement or any other agreement entered into by the data exporter and the data importer shall specify the countries and territories to which the Personal Data may be transferred under the contract.

Clause 9: Obligation after the Termination of Personal Data Processing Services

The parties agree that on the termination of the provision of data Processing services, the data importer and the Sub-processor shall, at the choice of the data exporter, return all the Personal Data transferred and the copies thereof to the data exporter or shall destroy all the Personal Data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the Personal Data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the Personal Data transferred and will not actively Process the Personal Data transferred anymore.

Clause 10: Supplemental Provisions

In the event that the applicable law of the country where the data exporter is located requires additional or more stringent requirements than those established by this DTA, then such applicable law will apply.

APPENDIX 1 - DESCRIPTION OF TRANSFER

Data exporter

The data exporter is: Customer, who is the Controller of Customer Data.

Data importer

The data importer is: Huawei, as defined in the Agreement, that will be Processing Customer Data on Customer's behalf as per the DPA, or the Sub-Processor engaged by Huawei, as applicable.

Data Subjects

The Personal Data transferred concern the following categories of Data Subjects (please specify): Customer End Users

Categories of data

The Personal Data transferred concern the following categories of data: Customer End Users' Personal Data

Special Categories of Data (if appropriate)

The Personal Data transferred concern the following Special Categories of Data (please specify): N/A

Processing operations

The Personal Data transferred will be subject to the following basic Processing activities (please specify):

Process the Customer Data to Provide the Service.

APPENDIX 2 - DESCRIPTION OF THE TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES IMPLEMENTED BY THE DATA IMPORTER

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 3(b) and 4(c): the measures are provided in the DPA's Clause 4 (Data Security) and Annex 1 (Security Measures)

Attachment 2

STANDARD CONTRACTUAL CLAUSES

Controller to Controller

This Attachment 2 shall incorporate the EU Standard Contractual Clauses (Module one, transfer: controller to controller), as further specified above in section 7.2(k), and as set out at: **https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en**

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: Aspiegel SE

Address: 3rd floor, Mespil Court, Mespil Road, Ballsbridge, Dublin 4, D04 E516, Ireland, with company number 561134, at the Companies Registration Office, Ireland

Contact person's name, position and contact details: Joerg Thomas, Director, DPO Office, dpo@huawei.com

Activities relevant to the data transferred under these Clauses: Detailed in Annex I B

Signature and date: _____

Role (controller/processor): controller

Data importer(s): Customer

Name: your name or, as the case may be, the name of the company you represent

Address: your place of business or, as the case may be, the place of business of the company you represent.

Contact person's name, position and contact details: our contact details and information as you have provided them in context of the Agreement and your Developer account

Activities relevant to the data transferred under these Clauses: Detailed in Annex I B

Signature and date: _____

Role (controller/processor): controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Users interacting with Customer's ads served with Petal AdsPlatform.

Categories of personal data transferred

User's ad behavior data such as Advertising ID, advertiser account ID, application ID, advertising task ID, creative ID, and user behavior (such as advertisement display, clicks, and downloads).

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A

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

Whenever User interacts with Customer's ads.

Nature of the processing

Passing on ads behavior data to Customer.

Purpose(s) of the data transfer and further processing

Perform attribution analysis and effect evaluation of the launched advertisement based on the data that the Platform reports.

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

Determined by each data controller separately

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

Data maybe shared with 3rd party tracking platforms (Customer's data processor) as authorized by Customer. Sharing is done under same conditions as if User data was shared directly with Customer.

C. COMPETENT SUPERVISORY AUTHORITY

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

Irish Data Protection Commission

ANNEX II

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

•Implement Information Security and Privacy Protection policies and procedures for critical assets and business processes in accordance with relevant laws, regulations and aligned to industry standards like ISO27001 or NIST Cyber Security Framework.

•Regularly assess security controls and risks in your information system(s) to determine if the controls are effective in their application, particularly following major changes, security incidents or data breaches.

•Ability to ensure the ongoing confidentiality, integrity, availability and resilience of Personal Data and systems and services that process the Personal Data.

•Manage supplier relationships including security requirements, SLAs, outsourcing agreements for contracts being used as part of the service provision including data processing agreements in place with the sub-processors you use to deliver the services or products in accordance with the GDPR.

•Perform appropriate background checks on personnel (employees, contractors and third party users) before hiring, when needed and legally permitted.

•All relevant personnel should be adequately and regularly trained on security and privacy protection.

•Manage access to protect personal data and systems or services that process and store personal data from unauthorized access following separation of duties and least privilege

principles. Access controls should include identity management, authentication of users incorporating a strong password policy, authorization, accountability, network segregation, regular access reviews (i.e. rights and privileges) and access revocation where access is no longer necessary.

•Implement a strong password policy by enforcing the use of sufficiently complex combinations of characters and numbers, length, enforcing periodic password renewal, restrictions on password reuse, ensure passwords are encrypted and incorporate multi-factor where possible.

•Establish, protect, and maintain the integrity of your network, platforms and services by taking steps to detect and prevent successful security incidents like DDoS, viruses, code injections or other malware that can alter the functionality of the systems, or confidentiality, integrity or availability of information and systems, through industry best practice security controls like malware protection, DDoS protection, IDS/IPS, firewalls, vulnerability scanning, patch management.

•Ensure network and information systems and services are subject to regular security testing (e.g. penetration testing, vulnerability scanning, static and dynamic application security testing), including for major upgrades, to identify vulnerabilities that could expose your service to increased risk of malicious intrusion, modification, and unauthorized access to sensitive data.

•Implement a patch management process to ensure updates are performed on systems with critical and high risk vulnerabilities addressed immediately, with all other system flaws, weaknesses or deficiencies identified, reported and remediated in a timely manner.

•Antivirus software must be loaded and operational on all systems processing personal data. Other malware detection techniques should be used where possible (e.g., email scanning, file system scanning, internet traffic scanning, etc.).

•Assets are inventoried, classified and updated when changes occur (i.e. new systems /software introduced, systems decommissioned).

•Establish change and configuration management procedures for key network and information systems to manage configuration securely.

•Implement network and information systems security event logging and monitoring for the offered service using Security Operations Center (SOC), Security Information and Event Management (SIEM), agents to report anomalous behavior at both network and host level.

•Protect logs against modification or tampering.

•Protect the service infrastructure from unauthorized software being installed.

Attachment 3

Data Transfer Agreement

This Agreement is made and entered into

Between

Huawei Services (Hong Kong) Co., Limited (Company registration number: 1451551), a company incorporated under the laws of Hong Kong (China) and having its registered address at Room 03, 9/F, Tower 6, the Gateway, No. 9 Canton Road, Tsim Sha Tsui, Kowloon, Hong Kong (China) ("**Data Exporter**")

And

The entity identified as "Customer" in Agreement ("**Data Importer**")

Each a "party"; together "the parties".

WHEREAS

(a) the Data Exporter is a global telecommunication equipment supplier;

(b) the Data Exporter and Data Importer wish to enter into this Agreement in good faith for civil use purpose;

NOW, THEREFORE, in consideration of the promises and mutual covenants contained in this Agreement and for other good and valuable consideration, the receipt and sufficiency of which is hereby mutually acknowledged, in reliance upon all the files, information, data, written and oral representation or promise provided by each Party shall be true, accurate, complete and not misleading, Parties hereto agree as follows:

Definitions

For the purposes of the clauses:

(a) "individual", "personal data", "processing" shall have the same meaning as in Personal Data Protection Act (No. 26 of 2012) of Singapore;

(b) "**Data Exporter**" shall mean the organization who transfers the personal data;

(c) "**Data Importer**" shall mean the organization who agrees to receive in a country or territory outside Singapore the personal data transferred to it by or on behalf of the Data Exporter for processing in accordance with the terms of these clauses;

(d) "**Data Subject**" shall mean the Data Subject that is particularly described in Annex D herein below;

(e) "**clauses**" shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements;

(f) "**PDPA**" shall mean the Personal Data Protection Act (No. 26 of 2012) of Singapore.

The details of the transfer (as well as the personal data covered) are specified in Annex D, which forms an integral part of the clauses.

I. Obligations of the Data Exporter

The Data Exporter warrants and undertakes that:

(a) The personal data has been collected, processed and transferred in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the country where the Data Exporter is established).

(b) It has used reasonable efforts to determine that the Data Importer is able to satisfy its legal obligations under these clauses.

(c) It will provide the Data Importer, when so requested, with copies of relevant data protection laws or references or any requirements set out in any advisory or other guidelines issued from time to time by Personal Data Protection Commission of Singapore ("**PDPC**") to them (where relevant, and not including legal advice).

(d) It will respond to enquiries from Data Subjects and the authority concerning processing of the personal data by the Data Importer, unless the parties have agreed that the Data Importer will so respond, in which case the Data Exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the Data Importer is unwilling or unable to respond. Responses will be made within a reasonable time.

(e) It will make available, upon request, a copy of the clauses to Data Subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the Data Exporter shall inform Data Subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the Data Exporter shall abide by a decision of the authority regarding access to the full text of the clauses by Data Subjects, as long as Data Subjects have agreed to respect the confidentiality of the confidential information removed. The Data Exporter shall also provide a copy of the clauses to the authority where required.

(f) It has instructed and throughout the duration of the personal data processing services will instruct the Data Importer to process the personal data transferred only on the Data Exporter's behalf and in accordance with the applicable data protection law and the clauses.

II. Obligations of the Data Importer

The Data Importer warrants and undertakes that:

(a) It will have in place appropriate technical and organizational measures to provide a standard of protection, that is comparable to the protection required by the PDPA and

any requirements set out in any advisory or other guidelines issued from time to time by the PDPC, to the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

(b) It will have in place procedures so that any third party it authorizes to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the Data Importer, including a data processor shall be obligated to process the personal data only on instructions from the Data Importer. This provision does not apply to persons authorized or required by law or regulation to have access to the personal data.

(c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the Data Exporter if it becomes aware of any such laws.

(d) It will process the personal data for purposes described in Annex D, and has the legal authority to give the warranties and fulfill the undertakings set out in these clauses.

(e) It will identify to the Data Exporter a contact point within its organization authorized to respond to enquiries concerning of the personal data, and will cooperate in good faith with the Data Exporter, the Data Subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the Data Exporter, or if the parties have so agreed, the Data Importer will assume responsibility for compliance with the provisions of clause I(e).

(f) At the request of the Data Exporter, it will provide the Data Exporter with evidence of financial resources sufficient to fulfill its responsibilities under clause III (which may include insurance coverage).

(g) Upon reasonable request of the Data Exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and /or certifying by the Data Exporter (or any independent or impartial inspection agents or auditors, selected by the Data Exporter and not reasonably objected to by the Data Importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the Data Importer, which consent or approval the Data Importer will attempt to obtain in a timely fashion.

(h) It will process the personal data, in accordance with:

i. The data protection laws of Singapore, and the relevant regulations, provisions or other requirements issued by PDPC; and

ii. The data processing principles set forth in Annex C.

(i) It will not disclose or transfer the personal data to a third party organization located outside Singapore unless with prior consent of the Data Exporter on the transfer and

i. The third party organization processes the personal data in accordance with requirements prescribed under PDPA finding that the third party organization provides a standard of protection to personal data so transferred that is comparable to the protection under PDPA;

ii. Data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards.

(j) It will process the personal data only on behalf of the Data Exporter and in compliance with its instructions and the clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the Data Exporter of its inability to comply, in which case the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract.

III. Liability and third party rights

(a) The Data Importer shall be liable to the Data Exporter for damages it causes by any breach of these clauses. Liability as between the parties is including but not limited to actual damage suffered and penalties imposed by government or local authority. The Data Importer shall be liable to Data Subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the Data Exporter under its data protection law.

(b) The parties agree that a Data Subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the Data Importer or the Data Exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the Data Exporter's country of establishment. In cases involving allegations of breach by the Data Importer, the Data Subject must first request the Data Exporter to take appropriate action to enforce his rights against the Data Importer, if the Data Exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the Data Subject may then enforce his rights against the Data Importer directly. A Data Subject is entitled to proceed directly against

a Data Exporter that has failed to use reasonable efforts to determine that the Data Importer is able to satisfy its legal obligations under these clauses (the Data Exporter shall have the burden to prove that it took reasonable efforts).

(c) The Data Importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

IV. Law applicable to the clauses

These clauses shall be governed by the law of the Singapore.

V. Resolution of disputes with Data Subjects or the authority

(a) In the event of a dispute or claim brought by a Data Subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

(b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

(c) Each party shall abide by a decision of a competent court of Singapore or of the authority which is final and against which no further appeal is possible.

VI. Termination

(a) In the event that the Data Importer is in breach of its obligations under these clauses, then the Data Exporter may temporarily suspend the transfer of personal data to the Data Importer until the breach is repaired or the contract is terminated.

(b) In the event that:

i. The transfer of personal data to the Data Importer has been temporarily suspended by the Data Exporter for longer than one month pursuant to paragraph (a);

ii. Compliance by the Data Importer with theses clauses would put it in breach of its legal or regulatory obligations in the country of import;

iii. The Data Importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

iv. A final decision against which no further appeal is possible of a competent court of Singapore or of the authority rules that there has been a breach of the clauses by the Data Importer or the Data Exporter; or

v. A petition is presented for the administration or winding up of the Data Importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the Data Importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs,

then the Data Exporter, without prejudice to any other rights which it may have against the Data Importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the Data Importer may also terminate these clauses.

(c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Singapore PDPA 2012 (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the Data Importer, or any superseding text becomes directly applicable in such country.

(d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex D, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex D. The parties agree that Annex D may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the

authority where required. Annex D may, in the alternative, be drafted to cover multiple transfers.

ANNEX C: DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex D or subsequently authorized by the Data Subject.

2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the Data Exporter.

4. Security and confidentiality: Technical and organizational security measures must be taken by the organization that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, presented by the processing. Any person acting under the authority of the organization, including a processor, must not process the data except on instructions from the Data Exporter.

5. Rights of access, correction and objection: As provided under the PDPA, Data Subjects must, whether directly or via a third party, be provided with the personal information about them that an organization holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the Data Exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the Data Importer or other organizations dealing with the Data Importer and such interests are not overridden by the interests for fundamental rights and freedoms of the Data Subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual

would be violated. Data subjects must be able to have the personal information about the rectified, amended where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organization may require further justifications before proceeding to rectification or amendment. Notification of any rectification, amendment to third parties to whom the data has been disclosed need not be made when this involves a disproportionate effort. A Data Subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation.

6. Data used for marketing purposes: Where data is processed for the purposes of direct marketing, effective procedures should exist allowing the Data Subject at any time to "opt-out" from having his data used for such purposes.

7. Automated decisions: For purposes hereof "automated decision" shall mean a decision by the Data Exporter or the Data Importer which produces legal effects concerning a Data Subject or significantly affects a Data Subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The Data Importer shall not make any automated decisions concerning Data Subjects, except when:

(a) i. such decisions are made by the data importer in entering into or performing a contract with the data subject, and
ii. the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

or

(b) where otherwise provided by the law of the data exporter.

ANNEX D: DESCRIPTION OF THE TRANSFER

Data subjects
The personal data transferred concern the following categories of data subjects:
Users interacting with Customer's ads served with Petal AdsPlatform.

Purposes of the transfer(s)
The transfer is made for the following purposes:
Perform attribution analysis and effect evaluation of the launched advertisement based on the data that the Platform reports.

Categories of data
The personal data transferred concern the following categories of data:
Open Advertising ID (OAID, the device ID generated by Huawei), advertiser account ID, application ID, advertising task ID, creative ID, and user behavior (such as advertisement display, clicks, and downloads).

Recipients
The personal data transferred may be disclosed only to the following recipients or categories of recipients:
Data importer (or 3rd party authorized by data importer)

Data exporter

Role: Leader of Data Operation Team

Mail: **privacy_hshk@huawei.com**

Attachment 4

Data Transfer and Processing Agreement

Huawei Services (Hong Kong) Co., Limited, Room 03, 9/F, Tower 6, the Gateway, No.9 Canton Road, Tsim Sha Tsui, KL, Hong Kong (China), hereinafter referred to as Huawei,

And

Customer, hereinafter referred to as "the Company", hereinafter individually referred to as "party", and collectively as "the parties"; Huawei and the Company act as data controllers for personal data, including for the data processed for the purpose of this Agreement, HUAWEI Developers Service Agreement and HUAWEI Partner Paid Service Agreement, which together control relationship between Huawei and the Company when Petal Ads Services are used, have entered into this Data Transfer and Processing Agreement as follows.

Personal data shall mean any information that is defined as personal data by the applicable laws of the Russia and transferred to the Company by Huawei, including:

• Open Advertising ID (OAID, the device ID generated by Huawei),

• Advertiser account ID,

• Application ID,

• Advertising task ID,

• Creative ID, and user behavior (such as advertisement display, clicks, and downloads).

The personal data transferred belong to users who interact with Customer's ads served with Petal AdsPlatform.

The transfer is made for performing attribution analysis and effect evaluation of the launched advertisement based on the data that the Platform reports.

No data transfer shall be considered by the parties as the instruction to process personal data.

Both parties shall keep confidential the personal data received under the Agreement, shall comply with the requirements and regulations of the Federal Law on Personal Data under N 152-FZ of 27 July 2006, and shall be fully responsible for taking appropriate legal, technical and organizational measures to provide protection to the personal data against accidental or unlawful access, destruction, alteration, blocking, copying, disclosure or other unauthorized activities.

The transferring party shall be responsible for validity and accuracy of personal data transferred to the other party for the purpose of this Agreement, and for obtaining from data subjects their prior consent to transfer of their personal data to the other party, as required by the laws of the Russia.

The party that receives personal data from the other Party shall bear no responsibility for giving notice about processing of such personal data to the relevant data subjects, since the responsibility for giving appropriate notice during the process of obtaining consent to transfer shall be borne by the party that transfers such personal data.

Attachment 5

(* This Attachment is applicable only if Customer's Business Area is the territory of the Russian Federation)

Fulfillment of the obligation to mark and record online advertising in the territory of the Russian Federation

On September 1, 2022, amendments to the Federal Law of the Russian Federation "On Advertising" of 13.03.2006 No. 38-FZ (hereinafter referred to as the "Law on Advertising") came into force.

This law applies to relations in the field of advertising, regardless of the place of its production, if the distribution of advertising is carried out in the territory of the Russian Federation (that is, advertising is placed on Internet sites registered in domain zones .SU, .RU and .RF, as well as on Russian-language pages of websites in other zones, since the information is intended for consumers in Russia).

Main responsibilities

(1) **Labeling of advertising materials**

Internet advertising must contain an "Advertising" mark, as well as (a) an indication of the advertiser of such advertising and/or (b) the website and the web page in the information and telecommunications network (Internet) containing information about the advertiser of such advertising.

The responsibility for the absence of advertising labeling lies with the advertising distributor.

(2) **Transfer of information to Roskomnadzor (control body) through Advertising Data Operators**

In order to ensure the traceability of advertising on the Internet, the federal executive authority exercising control and supervision functions in the field of mass media, mass communications, information technology and communications (hereinafter, "Roskomnadzor") records, stores, and processes information about advertising distributed on the Internet, including information about advertisers and advertising distributors of such advertising, and operators of advertising systems.

Advertisers, advertising distributors, and advertising system operators who have placed advertisements on the Internet aimed at attracting the attention of advertising consumers located in the territory of the Russian Federation and who meet the criteria defined by the Government of the Russian Federation are obligated to provide information or ensure the provision of information about such advertising to Roskomnadzor through the owners of programs for electronic computers designed to establish the fact of distributing advertising on the Internet (hereinafter referred to as the "Advertising Data Operator" or ORD).

The responsibility for transmitting information about online advertising to Roskomnadzor lies with each of the subjects.

Thus:

(1)Prior to the distribution of Advertising, **Customer undertakes to ensure that the Ads are appropriately marked** (independently or with the help of another authorized person), otherwise Huawei has the right to refuse to provide services for such Advertising.

(2)Huawei, in order to fulfill the obligation to provide Roskomnadzor with information about Advertising distributed on the Internet in accordance with the Law on Advertising, **will provide at the expense of Customer the necessary information about advertising distributed by Customer on the Internet in the ORD** in the amount and within the time limits established by applicable regulations of the Russian Federation. **Detailed conditions on the cost of the ORD services will be determined separately;**

(3)Huawei has the right, at its discretion, to choose an ORD to provide information to Roskomnadzor;

(4)Customer provides Huawei with unconditional consent to provide information about themselves, their clients (if Advertising is placed in their interests), as well as

information about Advertising placed under this Agreement, to the extent prescribed by the Law on Advertising and other applicable regulations.

(5)Huawei, in turn, **has the right to request the necessary information from Customer** , and Customer, in turn, undertakes to provide such information at Huawei's request no later than ten (10) working days before the deadline for providing the relevant information to Huawei (in any case, no later than at Huawei's request after three (3) business days from the date of the relevant Huawei request). At the same time, Customer is responsible for the accuracy of the Huawei information that they provided.

(6)The Parties agree that Huawei's transfer of information to the ORD will not be deemed as a violation of the provisions on confidential information.

List of information about the subjects of advertising, which is subject to transfer through the ORD to Roskomnadzor

About advertiser	**About advertising distributor**	**About advertising system operators**
		(a) Full and abbreviated (if any) name, organizational and legal form of a legal entity or surname, first name, patronymic (if any) of an individual entrepreneur or individual; (b) Taxpayer identification number — for a Russian national; (c) Subscriber's mobile phone number and/or the number of the electronic means of payment — for a foreign individual;

	(a) Full and abbreviated (if any) name, organizational and legal form of a legal entity or surname, first name, patronymic (if any) of an individual entrepreneur or individual; (b) Taxpayer identification number — for a Russian national; (c) Subscriber's mobile phone number and/or the number of the electronic means of payment — for a foreign individual; (d) Main state registration number of a legal entity or the main state registration number of the record of state registration as an individual entrepreneur — for a Russian legal entity or individual entrepreneur; (e) Location and address of a legal entity or the address of the place of residence (stay) of an individual entrepreneur or an individual; (f) Surname, first name, patronymic (if any) and position of the person entitled to act on behalf of	(d) Main state registration number of a legal entity or the main state registration number of the record of state registration as an individual entrepreneur — for a Russian legal entity or individual entrepreneur; (e) Location and address of a legal entity or the address of the place of residence (stay) of an individual entrepreneur or an individual; (f) Surname, first name, patronymic (if any) and position of the person entitled to act on behalf of a legal entity without a power of attorney — for a Russian legal entity; (g) Information about the person who has concluded an agreement with the advertiser, the advertising distributor, or their representatives and intermediaries acting at the expense and on behalf of the operator of the advertising system for the provision of services (works) using the advertising system, or performing actions on behalf of and at the expense of the advertising system operator in order to organize the
(a) Full and abbreviated (if any) name, organizational and legal form of a legal entity or surname, first name, patronymic (if any) of an individual entrepreneur or individual; (b) Taxpayer identification number of a legal entity or individual entrepreneur, as well as an individual — for a Russian national; (c) Subscriber's mobile phone number and/or the number of the electronic means of payment — for a foreign individual; (d) Main state registration number of a legal entity or the main state registration number of the record of state registration as an individual entrepreneur — for a		

Russian legal entity or individual entrepreneur; (e) Location and address of a legal entity or the address of the place of residence (stay) of an individual entrepreneur or an individual; (f) Surname, first name, patronymic (if any) and position of the person entitled to act on behalf of a legal entity without a power of attorney — for a Russian legal entity; (g) Information about the person who has concluded an agreement with the advertising distributor, the operator of the advertising system, or their representatives and intermediaries acting at the expense and on behalf of the advertiser for the distribution of advertising on the Internet and/or for the provision of services (works) using an advertising system, or performing actions on behalf of and at the expense of the advertiser for the purpose of distributing advertising on the Internet, or acting in the interests of the advertiser when distributing advertising on the Internet as a	a legal entity without a power of attorney — for a Russian legal entity; (g) Information about the person who has concluded an agreement with the advertiser, the operator of the advertising system, or their representatives and intermediaries acting at the expense and on behalf of the advertising distributor for the distribution of advertising on the Internet and/or the provision of services (works) using an advertising system, or performing actions on behalf of and at the expense of the advertising distributor for the purpose of distributing advertising on the Internet, or acting in the interests of the advertising distributor when distributing advertising on the Internet as a commercial representative or other intermediary, including: description of the actions carried out, including the conclusion of contracts, and actions for the purpose of advertising distribution, commercial representation, and other mediation;	distribution of advertising on the Internet, or acting in the interests of the advertising system operator in organizing the distribution of advertising on the Internet as a commercial representative or other intermediary, including: description of the actions carried out, including the conclusion of contracts, and actions for the purpose of advertising distribution, commercial representation, and other mediation; full and abbreviated (if available) name of the legal entity or surname, first name, patronymic (if available) of an individual entrepreneur or an individual; location and address of a legal entity or address of the place of residence (stay) of an individual entrepreneur or an individual; subscriber's mobile phone number and/or the number of the electronic means of payment — for a foreign individual; main state registration number of a legal entity

commercial representative or other intermediary, including:

description of the actions carried out, including the conclusion of contracts, and actions for the purpose of advertising distribution, commercial representation, and other mediation;

full and abbreviated (if available) name of the legal entity or surname, first name, patronymic (if available) of an individual entrepreneur or an individual;

location and address of a legal entity or address of the place of residence (stay) of an individual entrepreneur or an individual;

subscriber's mobile phone number and/or the number of the electronic means of payment — for a foreign individual;

main state registration number of a legal entity or main state registration number of a state registration record as an individual entrepreneur — for a Russian legal entity or individual entrepreneur;

full and abbreviated (if available) name of the legal entity or surname, first name, patronymic (if available) of an individual entrepreneur or an individual;

location and address of a legal entity or address of the place of residence (stay) of an individual entrepreneur or an individual;

subscriber's mobile phone number and/or the number of the electronic means of payment — for a foreign individual;

main state registration number of a legal entity or main state registration number of a state registration record as an individual entrepreneur — for a Russian legal entity or individual entrepreneur;

taxpayer identification number — for a Russian national;

registration number or its analogue and/or taxpayer number or its analogue in the country of registration — for a foreign legal entity;

or main state registration number of a state registration record as an individual entrepreneur — for a Russian legal entity or individual entrepreneur;

taxpayer identification number — for a Russian national;

registration number or its analogue and/or taxpayer number or its analogue in the country of registration — for a foreign legal entity;

country code of registration of a legal entity in accordance with the All-Russian Classifier of countries of the world — for a foreign legal entity;

(h) Information about the information system and/or the program for electronic computers that are intended and used by the operator of the advertising system to organize the distribution of advertising on the Internet through information resources owned by third parties, including:

network address, domain name, web page index on the Internet or other form

taxpayer identification number — for a Russian national; registration number or its analogue and/or taxpayer number or its analogue in the country of registration — for a foreign legal entity; country code of registration of a legal entity in accordance with the All-Russian Classifier of countries of the world — for a foreign legal entity; (h) Information about the identified inconsistencies in the advertising data provided by the advertiser to the operator or directly to the authorized body about the advertising distributed on the Internet (if available); (i) Information about the established facts of non-compliance by the advertiser with the requirements for the distribution of advertising on the Internet (if available); (j) Registration number or its analogue and/or taxpayer number or its	country code of registration of a legal entity or individual entrepreneur in accordance with the All-Russian Classifier of countries of the world — for a foreign legal entity or individual entrepreneur; (h) Information about the identified inconsistencies in the information provided by the advertiser to the advertising data operator or directly to the authorized body about the advertising distributed on the Internet (if available); (i) Information about the means of distributing advertising of the advertising distributor on the Internet (the name of the site, and/or the web page on the Internet, and /or the information system, and/or the program for electronic computers (if available), their network address, domain name, index of the web page on the Internet or another form of identification); (j) Information about the placement of programs for electronic computers of the advertising distributor, through which	of identification of an information system and/or a program for electronic computers on the Internet, which are intended and used by the operator of the advertising system to organize the distribution of advertising on the Internet; information about information resources belonging to third parties, through which the operator of the advertising system provides access to advertising on the Internet (the name of the site, and /or the pages of the site on the Internet, and/or the information system, and /or programs for electronic computers (if available), their network address, domain name, web page index on the Internet or other form of identification); information about the placement of programs for electronic computers belonging to third parties, through which the operator of the advertising system provides access to advertising on the Internet, in order to install such programs for electronic computers on the equipment of end users located in the

analogue in the country of registration — for a foreign legal entity; (k) Country code of registration of a legal entity in accordance with the All-Russian Classifier of countries of the world — for a foreign legal entity.	Internet access to advertising is provided, in order to install such programs for electronic computers on the equipment of end users located in the territory of the Russian Federation; (k) Information about the established facts of non-compliance by the advertiser with the requirements for the distribution of advertising on the Internet (if any); (m) Registration number or its analogue and/or taxpayer number or its analogue in the country of registration — for a foreign legal entity; (h) Country code of registration of a legal entity or individual entrepreneur in accordance with the All-Russian Classifier of countries of the world — for a foreign legal entity or individual entrepreneur.	territory of the Russian Federation; (i) Information about the identified inconsistencies in the information provided by the operator of the advertising system to the operator of advertising data or directly to the authorized body about the advertising distributed on the Internet (if available); (j) Information about the established facts of non-compliance by the operator of the advertising system with the requirements for the distribution of advertising on the Internet (if any); (k) Registration number or its analogue and/or the taxpayer number of a legal entity or its analogue in the country of registration, the taxpayer number of an individual in the country of residence (stay) — for a foreign person; (m) Country code of registration of a legal entity, residence (stay) of an individual in accordance with the All-Russian Classifier of countries of the world — for a foreign person.

Information about Advertising that is subject to transfer to Roskomnadzor

(a) Information intended to ensure the traceability of the distribution of advertising on the Internet using unique numerical designations of distributing and/or distributed advertising;

(b) General description of the advertising object in Russian;

(c) Main type of advertising campaign on the Internet, determined based on:

the cost equal to the product of the number of actions of advertising consumers determined by the advertiser, and the cost of one action of the advertising consumer;

the cost equal to the product of the number of ad impressions to advertising consumers and the cost of one impression;

the cost equal to the product of the number of access facts (transitions) of advertising consumers to information about the advertised object or the advertised object itself (hereinafter referred to as the access fact) and the cost of one access fact; or

another type of advertising campaign on the Internet, including those related to the peculiarities of its cost formation;

(d) Information about the means of advertising distribution on the Internet used for the distribution of advertising on the Internet (website and/or web page on the Internet, information system, and program for electronic computers), as well as about advertising systems (when using an advertising system);

(e) Information about the volume and distribution of advertising impressions on the Internet on information resources administered and/or used by the advertising distributor, the operator of the advertising system, as well as about access facts (if available) through such information resources, and about the volume of advertising impressions and access facts (if available) using advertising systems and distribution of such ad impressions and access facts (if any) between advertising systems;

(f) Information about the form of advertising distribution on the Internet, including all types of banners, text or text-graphic block, all types of videos, audio recordings, and audio and/or live video broadcasts;

(g) Term of advertising on the Internet or the start date of the advertising campaign in the case of advertising as part of copyrighted works in the form of a text or text-graphic block, or video or audio recording;

(h) Parameters of the advertising audience, taking into account gender, age, territory of residence (location), and other socio-demographic parameters of differentiation (if such information is available);

(i) Information about the agreement (agreements) concluded between the advertiser and /or the advertising distributor and/or the operator of the advertising system and/or their representatives and intermediaries for the distribution of advertising on the Internet and /or the provision of services (works) using an advertising system, performing actions on their behalf and at their expense, commercial mediation, and other mediation in their interests for the purpose of distributing or organizing the distribution of advertising on the Internet, including:

information about the parties to the agreement (contracts) as part of information from Russian and foreign state and trade registers about advertisers, advertising distributors, advertising system operators, and their representatives and intermediaries;

information about the subject of the agreement(s);

date and number of the agreement(s) (if any);

price of the contract(s) (if available);

parameters of the target audience of advertising, taking into account gender, age, territory of residence (location), and other socio-demographic parameters of differentiation (if any);

information about the performance of the contract (date and number of the act(s) of delivery and acceptance of services rendered, or other documents confirming the provision of services under the contract(s), as well as the document content), including the cost and quantity of services rendered, the cost of one unit of services (advertising display, access fact, and actions of the advertising consumer defined by the advertiser), the period of their provision, the type of advertising campaign on the Internet, the characteristics of the audience covered by advertising, taking into account gender, age, territory of residence (location), and other socio-demographic parameters of differentiation (if such information is available).

Endnote

[1]: Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

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

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

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

[5]: The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

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