HUAWEI Ads Advertising Services Agreement

Last Modified: December 21, 2020

The HUAWEI Advertising 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 Developer Service Agreement** and the **HUAWEI Partner Paid Service Agreement** and together control your relationship with HUAWEI when you use HUAWEI Advertising 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 Developer 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 Developer 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 other entity, You represent and warrant that You have full legal authority to bind Your employer or such entity to this Agreement. If You do not have the requisite authority, You may not accept the Agreement on behalf of Your employer or other entity.

1. Definitions

"**HUAWEI**": refers to the applicable HUAWEI entity(ies) listed in the clause of "Distribution Area and Signing HUAWEI entity" (Clause 8) of the HUAWEI Partner Paid Service Agreement.

"**HUAWEI AdsPlatform**" (or "AdsPlatform"): refers to a mobile internet platform **https://ads.huawei.com/usermgtportal/home/index.html#/** and its entrance platform **https://developer.HUAWEI.com/consumer/** developed and operated by HUAWEI and /or its Affiliates, which is designed to provide HUAWEI Advertising Services to you by using its professional data processing algorithms.

"**HUAWEI Advertising Services**" (or "**Services**") refers to advertising programs and services provided by HUAWEI to Customer through AdsPlatform under this Agreement. Services shall fall under the scope of the term "Paid Service" defined in the HUAWEI Partner Paid Service Agreement.

"**Ads Policies**" refers to the Ads Content Policies and other policies related to the Services available at https://developer.huawei.com/consumer/en/doc/distribution/promotion/ads-introduction as modified from time to time.

"**Ads**" refers to advertising materials Customer provided through AdsPlatform and authorized HUAWEI to place on any Property provided by HUAWEI or its Affiliates on behalf of HUAWEI or, as applicable, a third Party ("**Partner**"), including but not limited to texts, pictures, animations, videos, audios, webpages, URLs.

"**Products**": defined in Clause 2.2 herein.

"**Property**" or "**Properties**": means any mobile application software (with contents therein) or other digital contents on which Ads can be placed and displayed, which are provided by HUAEWEI or its affiliates on behalf of HUAWEI or, as applicable, a third Party ("**Partner**").

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, then Customer will 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 is submitted by Customer to HUAWEI Ads Platform for distribution pursuant to the terms of this Agreement either before or after the Huawei Ads Services is rendered hereunder, and at its sole discretion decide whether to provide the Customer with the HUAWEI Advertising Services for such Products or Ads.

2.6 Notwithstanding the foregoing, HUAWEI's reviewing of Customer's Products and Ads shall not relieve the Customer from its responsibilities and liabilities arising from or in connection with the Products or Ads hereof. In case 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 from the Property.

3. Ad Serving

Customer 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.

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. Cancelled Ads will generally cease serving within 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 Service, including CPM (cost per impressions), CPC (cost per click), CPD (cost per download), CPI (cost per install), CPT (cost per time), other billing criteria made available by Huawei for the Client to select in a specific IO and etc. All charges are VAT-inclusive.

5.2 The Services are provided in a prepaid mode, and/or credit card payment mode (which is specifically applicable for some determined countries/regions excluding Chinese Mainland), as available on the Customer interface of the Ads Platform. Customer shall enroll for Paid Services to have the Paid Service account ("**Account**") enabled for its HUAWEI ID.

(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 Customer placed. HUAWEI has the right to adjust the minimum top-up amount and subscription renewal amount from time to time.

(b) Credit card payment mode: Customer add 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 60 days after the invoice date ("Claim Period"), after which HUAWEI will issue the credits following claim validation which must be used within 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 retailing to any service charges unless 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.

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 current 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 does not contain any virus, worm, Trojan horse, time bomb, malicious code, malicious advertisement, or any software that damages, interferes with, intercepts, or confiscates any system data or personal information, and does not contain any fee deduction mechanism 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 involves 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 in 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 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 You, as data controller, authorize Huawei to conduct the following processing activities on behalf of you:

(a) Send Ads to target groups defined by you. After receiving the personal data shared by you, Huawei will select one or more people groups that meet your request based on your shared personal data as per your instructions, so that you may send Ads to target groups through the AdsPlatform.

(b) Create reports based on user data collected from your Ads landing pages (or comparable) or transferring such data directly to you via AdsPlatform. If you collect or transfer data via AdsPlatform by using any cookies or trackers, you are solely responsible of the lawfulness of such use of cookies and trackers and need to ensure that user has given valid consent for use of such technologies in accordance with applicable laws.

(c) Create reports based on data you have collected for attribution analysis and effect evaluation pursuant to Section 7.2, which you (or Ads tracking platform operating on behalf of you) transfer back to the AdsPlatform

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

7.2 You may collect personal data as data controller from AdsPlatform to perform attribution analysis and effect evaluation of the launched Ads based on the data that the AdsPlatform reports in accordance with the following terms:

(a) Your products and services shall respect the privacy of users and comply with applicable data protection laws and regulations.

(b) You undertake to collect and process the data that only for the purposes and requirements specified in this Agreement. Without Huawei's consent, you shall not use such data for any other purposes. For sake of clarity, any personal data, including Open Advertising ID, IP address, advertiser account ID, application ID, advertising task ID, creative ID, and user behavior (such as Ads display, clicks, and downloads) cannot be used for ads personalization or any other kind of profiling of the users.

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

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

(e) If you designate a third party company to conduct the processing on your behalf, the third party company is acting as your data processor and you shall ensure that the third party complies with the applicable laws, regulations and requirements. You are liable to any non-compliance of such third party.

(f) You shall have a publicly stated privacy policy in compliance with applicable laws and regulations, which accurately describes what personal data of the end user that you

collect and how you collect, use, disclose, and protect the information, and how end users may access their personal data. The privacy policy shall be displayed prominently in your applications and other services.

(g) You shall be solely responsible for resolving the privacy and security protection issues that occur between you and the users in respect to your products and services.

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

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

(j) When Aspiegel Limited is providing the Service to you and you receive personal data as a controller to outside European Union / European Economic Area to any country not recognized by the European Union 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 event of any discrepancies or conflicts between Attachment 2 and this Agreement.

(k) When Huawei Services (Hong Kong) Co., Limited is providing the service to you and you receive personal data as a controller to outside Singapore to any country (except Russia), the DATA TRANSFER AGREEMENT (Attachment 3) shall be an integral part of this Agreement.

(l) When Huawei Services (Hong Kong) Co., Limited is providing the service to you and you are processing the personal data that are 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 constitute an integral part of this Agreement.

7.3 Execution of this Agreement shall constitute and be deemed signature on each page of the Attachments and their respective annexes and appendices.

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.

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 Developer 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 , or does not intend to enter an agreement with you on providing the Service 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 AdsPlatform. The changes to this Agreement will not apply retroactively and will become effective 7 days after posting. However, changes made for legal reasons will 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.

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.

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 supersede 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.

13.6 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.

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

AND IN WITNESS WHEREOF, the Parties hereto have executed this Agreement as of the date written below.

Signed for and on behalf of **Aspiegel**Signed for and on behalf of **Huawei Services (Hong Kong) Co., Limited**

……

Date:Date:

Signed for and on behalf of: **Customer**

……

Print name:

Position:

Date:

Witness:

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.

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.

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, the Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the 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 to 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 to 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 the 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 to 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 Standard Contractual Clauses in Annex 2 or the Data Transfer Agreement in Annex 3, to which both Huawei and Customer conform, and hereby agree to. 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 the 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, the Customer shall obtain the necessary approval prior to such transfer. The 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 in 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 the Customer, to enter into a data processing agreement with such Sub-Processor that incorporates the Data Transfer Agreement as provided by Annex 3, unless Applicable Laws and Regulations requires entering into Standard Contractual Clauses as provided by Annex 2, in which case the data processing agreement shall incorporate such clauses. Huawei shall clearly indicate in the Data Transfer Agreement or Standard Contractual Clauses, as applicable, that it acts on behalf of the Customer. 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 the 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 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 the 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 is 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 are 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 (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

Customer as defined in the Agreement

(the data exporter)

And

Name of the data importing organisation:

Huawei

(the data importer)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1: Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95 /46/EC;

(d)'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss,

alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2: Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3: Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4: 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 data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that 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;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised 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;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5: Obligations of the data importer

The data importer agrees and warrants:

(a) to 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;

(b) 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 contract 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 the Clauses, 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/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data 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 accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in Agreements with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor Agreements it concludes under the Clauses to the data exporter.

Clause 6: Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7: Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8: Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9: Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established,

Clause 10: Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11: Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written Agreements with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written Agreements the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such Agreements.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing Agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12: Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor 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.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

The 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.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

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.

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 (please specify):

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 under Agreement.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

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 organisation:

Customer as defined in Agreement

(the data exporter)

And

Name of the data importing organisation:

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", “Subprocessing”, “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 Subprocessing, 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 defence 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 fulfil 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: the 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 organisational 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

EU Standard contractual clauses (controller-to-controller)

Commission Decision C(2004)5721

SET II

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

Data transfer agreement

between

Huawei

a limited liability company, duly established and constituted under the laws of Ireland, having its registered office at First Floor, Simmonscourt House, Simmonscourt Road,

Dublin 4, D04 W9H6, Ireland, with company number 561134, at the Companies Registration Office, Ireland

hereinafter “data exporter”

and

The entity identified as “Customer” in Agreement

hereinafter “data importer”

each a “party”; together “the parties”.

Definitions

For the purposes of the clauses:

“personal data”, “special categories of data/sensitive data”, “process/processing”, “controller”, “processor”, “data subject” and “supervisory authority/authority” shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby “the authority” shall mean the competent data protection authority in the territory in which the data exporter is established);

“the data exporter” shall mean the controller who transfers the personal data;

“the data importer” shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country’s system ensuring adequate protection;

“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.

The details of the transfer (as well as the personal data covered) are specified in Annex B, 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 have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

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 to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

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.

II. Obligations of the data importer

The data importer warrants and undertakes that:

a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised 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 authorises 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 authorised 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 (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

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

e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing 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 fulfil 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, at its option, in accordance with:

i. the data protection laws of the country in which the data exporter is established, or

ii. the relevant provisions of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data, or

iii. the data processing principles set forth in Annex A.

Data importer to indicate which option it selects: iii

Initials of data importer: <When the Agreement is signed, this section shall be considered as signed with legal effect by data importer>;

i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

i. the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

ii. the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

iii. 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, or

iv. with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

III. Liability and third party rights

a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party 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(c), 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).

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

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 the data exporter's country of establishment 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 these 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 the data exporter's country of establishment 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 Article 25(6) of Directive 95/46/EC (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 (ii) Directive 95/46/EC (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 B, 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 B. The parties agree that Annex B 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 B may, in the alternative, be drafted to cover multiple transfers.

ANNEX A: DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised 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 organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation 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 organisations 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 them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have 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. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.

7. Data used for marketing purposes: Where data are 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.

8. 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 B: 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 Huawei Ads platform.

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)

Sensitive data (if appropriate)
The personal data transferred concern the following categories of sensitive data:
N/A

Data protection registration information of data exporter (where applicable)
Not Applicable

Additional useful information (storage limits and other relevant information)
None

Contact points for data protection enquiries

Data importer

Data importer's contact information shall be the same as used for creating Importer's Huawei Developer account.

Name: ……

Role: ……

Address: ……

Mail: ……

Data exporter

Name: **datamanagement@aspiegel.com**

Role: Leader of Data Operation Team

Address: First Floor, Simmonscourt House, Simmonscourt Road, Dublin 4, D04 W9H6, Ireland

Mail: **datamanagement@aspiegel.com**

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 and having its registered address at Room 03, 9/F, Tower 6, the Gateway, No. 9 Canton Road, Tsim Sha Tsui, Kowloon, Hong Kong ("**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 theses 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 have 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 provide 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 clauses 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 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 terminated 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 work 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, amendment. Notification of any rectification, amendment to third parties to whom the data have 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 are 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 Huawei Ads platform or Customer’s ads landing pages or comparable locations.

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 Customer transfer to AdsPlatform.

Create reports based on data collected from Customer’s ads landing pages or comparable locations or transferring such data to Customer via Huawei Ads Platform.

Categories of data
The personal data transferred concern the following categories of data:

Data reported by Huawei ads platform: 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).

Any other data Customer decides to collect from its ads landing pages or comparable sites via Huawei Ads platform.

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, 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 Developer Service Agreement and HUAWEI Partner Paid Service Agreement, which together control relationship between Huawei and the Company when HUAWEI Advertising 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 Huawei Ads platform.

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.