HUAWEI Ads Terms and Conditions

Last updated: June 15, 2022

The HUAWEI Ads Terms and Conditions (hereinafter referred to as the "**Agreement**") is a legally binding agreement signed between you (also referred to as "**Customer**") and Huawei to establish your rights and obligations when you use HUAWEI Ads Services. By registering for the HUAWEI Ads Services under this Agreement, or using any HUAWEI Ads Services under this Agreement, it shall be deemed that you have agreed to be bound by the terms of this Agreement as of the date of such registration or use (" **Effective Date**"). If you are agreeing to be bound by this Agreement on behalf of your employer or any other entity, you represent and warrant that you have full legal authority to bind your employer or said entity to this Agreement. If you do not have the requisite authority, you may not accept the Agreement on behalf of your employer or any other entity.

1. Definitions

"**Huawei**" means the applicable Huawei entity(ies) listed in the clause "Distribution Area and Signing Entities" (Clause 17) in the Agreement.

"**HUAWEI Ads Platform**" (hereinafter also referred to as the "**Ads Platform**" or the " **Platform**") means the mobile Internet platform and the associated portal platform thereof (**https://ads.huawei.com**) that are developed and operated by Huawei and/or its Affiliates to provide HUAWEI Ads Services.

"**HUAWEI Ads Services**" (hereinafter also referred to as the "**Services**") means advertising programs and services provided by Huawei to Customer through the Ads Platform under this Agreement.

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

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

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

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

"**HUAWEI Dynamic Tag Manager Service**" or "**DTM Service**" means the tag management service provided by Huawei through DTM Kit and DTM Server for developers, which helps developers easily deploy and update tracking tags in a web-based user interface and report data to third-party analytics platforms.

"Segments" means a grouping of identifiers that share the same or similar attributes.

2. Services and Policies

2.1 To use the Services, you need to create a HUAWEI ID and said HUAWEI ID must be approved by Huawei. Huawei has the right to refuse or restrict your use of the Services.

2.2 Customer is solely responsible for all: (i) Ads, (ii) Ads trafficking or targeting decisions (collectively, "**Targets**"), (iii) destinations where viewers are directed by Ads (e.g., landing pages and mobile apps) along with the related URLs, waypoints, and redirects (collectively, "**Destinations**"), and (iv) services and products advertised on Destinations (collectively, "**Products**"). By using Services, Customer authorizes Huawei to use automated tools to format Ads and launch Ads on Properties upon Customer's insertion orders ("**IO**") on the user interface of the Services. Huawei may also make certain optional features of the Services available to Customer to assist Customer in selecting Targets, Ads, or Destinations. Customer may opt in to or opt out of using these features. However, if Customer uses these features, Customer shall be solely responsible for the Targets, Ads, and Destinations. Huawei and its Affiliate or Partners may reject or remove a specific Target, Ad, or Destination at any time for any or no reason. Huawei also has the right to refuse an IO. Huawei may modify or cancel Services at any time. Customer acknowledges that Huawei or its Affiliates may participate in the auctions of the Services to support their 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 in accordance with the Ads Terms.

2.4 Customer shall not nor 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 forms of scraping or data extraction to access, query, or otherwise collect HUAWEI Ads-related information from any Properties except as expressly permitted by Huawei, or (iv) attempt to interfere with the functioning of the Services. Customer shall only communicate with Huawei about the Ads launched through Huawei's own Properties and/or those through Partner's Properties under Clause 2 "Services and Policies" herein.

2.5 Huawei reserves the right to review the Products and Ads which are 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 to decide whether to provide the Customer with the HUAWEI Ads Services for such Products or Ads.

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

3. Ad Serving

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

3.2 Customer grants 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.

3.3 Customer allows Huawei and its Affiliates to use its logos, business names, and trademarks for the purpose of cooperation under this Agreement. If Customer believes that Huawei has misused any of the aforementioned items, Customer has the right to raise an objection, and Huawei shall take corrective actions after Customer and Huawei reach an agreement through negotiation.

3.4 Customer can choose to use the Segments provided by a third-party data management platform (DMP) in an IO for targeted advertising, and pay Huawei

according to CPM. Further details are available at: **https://developer.huawei.com/consumer/en/doc/distribution/promotion/audience-targeting-0000001249248257**.

4. Ad Cancellation

4.1 Unless an Ads Policy or an IO provides otherwise, either Party may cancel any Ad at any time before the Ad auction or placement, whichever comes first, 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), Customer is then responsible for any and all cancellation fees communicated by Huawei to Customer, and the Ad may still be published. Canceled Ads will generally cease serving within eight (8) business hours or as described in a Policy or IO, and Customer remains obligated to pay all charges resulting from served Ads.

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

5. Payments

5.1 The Services are charged in accordance with the applicable billing criteria, including but not limited to CPM (cost per impressions), CPC (cost per click), CPD (cost per download), CPT (cost per time), and other billing criteria made available by Huawei for the Customer to select in a specific IO. All charges are VAT-inclusive.

5.2 To use the Services, Customer has to enable Paid Services by providing valid tax-related information for Huawei to invoice the purchase of the Services. After the Paid Services are activated, Customer will be assigned a Paid Services account (hereinafter, "**Account**") on the Ads Platform. The Services can be paid for via prepayment and/or credit card payment. The credit card payment method is only available in certain countries and regions. The available payment method or methods will be displayed on the Customer interface of the Ads Platform. Customer must ensure that the name of the account that it uses for making payments is the same as its company name, or else Huawei has the right to suspend the provision of the Services to Customer.

(a) Prepaid mode: Customer shall top up the Account in advance in accordance with the top-up rules to use the Services for the charges of the IOs that Customer placed. Huawei has the right to adjust the minimum top-up amount and subscription renewal amount

from time to time. Customer shall comply with any and all applicable foreign exchange control policies and regulations when Customer is making cross-border remittances (if any). If customer does an offline top-up of more than USD 1,000 or EUR 1,000 at a time, Huawei will bear the handling fee ("**Waiver Policy**") of the intermediary bank. If there are any refunds, Huawei will only refund the actual amount received. Huawei reserves the right to adjust the above-mentioned Waiver Policy from time to time.

(b) Credit card payment mode: Huawei supports credit card payments in certain countries to Partners upon invitation only at Huawei's sole discretion. An invited Partner may add a valid corporate credit card opened in its name to the "Shared Account" under the Account and then purchase Paid Services afterwards. Huawei has the right to stop providing Paid Services immediately if identity theft happens to such a credit card, and Customer shall compensate for any and all losses incurred therefrom upon Huawei. Huawei will debit said credit card one (1) official unit of currency for verification, and refund said debited amount after Customer deletes said credit card from its Account. Huawei will charge Customer's credit card when the purchase reaches the USD 500 threshold (or an equivalent amount in another currency) or every seven (7) calendar days (whichever comes first).

(c) Payment mode priorities. The Platform will debit from the top-up balance of the Account first, and then debit the credit card if the top-up balance is insufficient. Customer will not be able to use the Services if both payment modes are unavailable.

(d) Huawei may freeze or close Customer's Account temporarily or permanently depending on specific circumstances if its Account is involved in identity theft or fraudulent transactions for payments under this Agreement. If the Account is frozen or closed for such reasons, Customer will not be able to purchase any Services. In addition, Customer will not be able to open a new Account on the Ads Platform.

(e) If Customer's credit card company or Customer's issuer bank files a chargeback case to Huawei for any purchase in connection with Customer's Account, Huawei may have to freeze or close Customer's Account. Customer may apply to unfreeze/reopen its Account after Customer remits the payable amount to Huawei.

(f) If above-mentioned payment issues result in the failure of the Services to receive the amount payable for the Services which have already been provided, Huawei has the right to deduct such a payable amount from Customer's Account or other payment accounts that Customer registered on any Huawei Platforms.

5.3 Reconciliation: Customer may check the Account balance and Account details on the Platform after using the Services. Huawei will not send any reconciliation report.

5.4 The charges will be settled in real time upon each display in accordance with the applicable billing criteria at the price agreed by Customer and Huawei and the terms of IO. The charges will be directly deducted from the balance of Customer's 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 Customer's Account or any quota Customer set for an IO (if any).

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

5.7 In the event of a refund, to get a refund of the balance in Customer's Account:

(1) Customer shall file a refund application to Huawei for the balance of its Account after Customer pays any and all payable amounts. The refund process will be initiated after the application passes Huawei's review.

(2) Customer shall comply with any and all applicable foreign exchange control policies and requirements of the country or region where Customer is located during an international refunding process, and Customer shall bear any and all reasonable costs incurred during the refund, including but not limited to handling fees charged by banks for international remittance, exchange loss, and Huawei's taxes and fees.

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

(a) Huawei may specify the reward policy by email or through announcements on the Ads Platform or by other proper means, including but not limited to the reward amounts, reward recipients, and reward methods.

(b) Under no circumstances shall such rewards be redeemed for cash. Huawei does not issue any invoice for such rewards. Rewards are not reflected in the advertiser

consumption invoices on the Ads Platform, and shall be automatically invalidated when the validity period thereof expires.

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

6. Taxation and Invoicing

6.1 Customer and Huawei shall respectively bear the taxes levied upon Customer and Huawei in accordance with applicable tax laws/regulations. Any and all settlement amounts under this Agreement include the value-added tax (VAT), withholding tax (WHT), and digital services tax. Customer shall provide Huawei with correct tax information, such as Customer's qualification as a taxpayer and the tax registration number of direct taxes such as VAT, goods and services tax (GST), or other taxes of similar nature. Any and all payments that Customer makes to Huawei shall not be subject to any set-off, counter-claim, or required withholding or deduction. If a withholding tax or deduction is required by applicable laws, Customer shall remit such a withholding tax to relevant tax authorities in the full amount and pay to Huawei the amount net of such tax. Customer shall obtain the tax payment certificate from the competent tax authorities after Customer pays such tax or a deduction, and provide said certificate to Huawei within sixty (60) days after said payment. Huawei shall top up Customer's Account and issue invoices based on the amount that it received and the WHT amount specified in the aforesaid tax payment certification.

6.2 If the tax information that Customer provides to Huawei is incorrect, such as Customer's qualification as a taxpayer and the tax registration number of indirect taxes such as VAT, GST, or other taxes of a similar nature, or if Customer does not or fails to withhold or deduct an amount from the payment to Huawei under this Agreement while such a withholding tax or deduction should have been performed in accordance with the auditing result, Customer shall be liable to assume any such withholding tax or deduction and any and all surcharges and penalties incurred therefrom and levied upon by competent authorities.

6.3 Customer may apply for an invoice on the Platform for the Services or for topping up Customer's Account after Customer registers or updates the information necessary for issuing such an invoice. Huawei will issue an invoice for Customer that contains the amount of Customer's order within a specified period after the completion of the order. If Customer does not request an invoice within fourteen (14) days after the completion of the order, the Platform will automatically trigger an invoicing request and the invoice will be issued with the information that Customer registers on the Platform. If the

invoice contains one or more errors due to Customer's information being outdated, Customer shall bear any and all losses incurred therefrom. See Attachment 6 for invoice types and relevant information that Customer needs to provide to Huawei.

7. Representations and Warranties

7.1 Customer hereby represents, warrants, and covenants that:

(a) Customer possesses any and all necessary rights and authorizations to enter into this Agreement, and the conclusion and performance of this Agreement does not violate any agreement signed by and between Customer and a third party, or infringe upon any third-party rights, nor violate any applicable laws and regulations.

(b) The activities that Customer conducts or engages in on the Platform, the use of the Services, the Ads Products that Customer provides or promotes via the Platform will not: (i) violate any applicable laws, regulations, policies, common industry practices, or pertinent provisions, guidelines or common practices in the relevant jurisdictions; (ii) infringe upon Huawei's or any third party's legal rights (including but not limited to the right of privacy, intellectual property rights, right of reputation, right of portrait, and trade secrets); or (iii) contain any illegal content or other content that Huawei deems at its reasonable discretion to be inappropriate.

(c) Customer shall comply with any and all applicable laws and regulations regarding network security, and Customer may not conduct or engage in any activities that interfere with, disrupt, damage, or access in an unauthorized manner the devices, servers, networks, software, or other properties or services of Huawei or any third party.

(d) Customer shall not disrupt or attempt to disrupt the operations of the Platform.

(e) Customer shall at all times comply with the terms of this Agreement and, when applicable, comply with management policies and other policies, guidelines, and rules provided along with and regarding the Services, released by Huawei from time to time on the Platform.

(f) Customer shall not engage in any activity, conduct, or omission that: (i) violates any applicable laws and regulations; (ii) causes or induces Huawei to violate applicable laws; or (iii) exposes Huawei to penalties, liabilities, sanctions, or restrictions under applicable laws.

(g) 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;

(h) All information and authorizations provided by Customer are true, legal, complete, correct, and up to date and Customer shall be solely responsible for any and all legal liabilities thereto. Customer is responsible for ensuring the authenticity and accuracy of the displayed content.

(i) Ads and Products do not contain any viruses, worms, Trojan horses, time bombs, malicious code, malicious advertisements, or any software that damages, interferes with, intercepts, or confiscates any system data or personal information, or any fee deduction mechanisms that can be implemented without the permission of end users.

(j) If Huawei is punished by the competent authority of the country where Products are sold or is subject to claims from end user or any other third party because Customer violates one or more of the preceding terms, Customer will indemnify and hold harmless Huawei against and from any and all of said punishment, claims from the end user or third party, and any other economic losses caused by Customer's violation of this clause. In addition, Huawei reserves the right to take any and all reasonable measures to protect the rights and interests of end users, and to terminate this Agreement immediately in the event of any such occurrence described herein.

(k) If Customer's Products are apps, Customer warrants that said Products have been distributed on HUAWEI AppGallery and such Products publicized in Ads are of the same version as those distributed on HUAWEI AppGallery.

(l) Customer warrants that its collection, use, transmission, and processing of personal data as well as use of cookies and other similar technologies in connection with the Services conform to any and all applicable laws and regulations.

7.2 In the event that Customer, Customer's Ads, or Customer's Products are investigated by the competent authorities or are the subject of complaints, or Customer violates 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 Customer to modify the content until it meets relevant requirements;

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

(d) Suspending or restricting Customer's use of the Services (for example, freezing Customer's account and suspending the review of Customer's content);

(e) Removing or shielding all of Customer's displayed content;

(f) Deducting an amount from Customer's Account to compensate for user losses and any other reasonable expenses;

(g) Deducting all of the balance of Customer's Account as liquidated damages, which is non-refundable (if Customer's Account balance is insufficient for the compensation, Customer shall make up for it);

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

7.3 If Customer receives any complaints from Users or third parties about Customer's display content and Customer fails to properly resolve such a complaint within three (3) working days of receiving such a complaint, 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) Advancing the expenses to settle disputes and compensate for losses. Huawei has the right to directly deduct such expenses from Customer's Account or claim compensation from Customer separately;

(b) Deducting from the balance of Customer's Account as liquidated damages, or using such balance to settle disputes and compensate for losses;

(c) Cooperating with the user or competent authorities to investigate the complaint (including but not limited to providing Customer's materials);

(d) Taking other measures in accordance with this Agreement.

8. Personal Data and Privacy Protection

8.1 As data controller, Customer may, in some circumstances, authorize Huawei to conduct the following processing activities on behalf of Customer:

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

(b) Create reports based on user data collected from Customer's Ads landing pages or comparable sites or transfer such data directly to Customer via the Ads Platform.

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

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

8.1.3 To use the DTM Service, Customer must clearly identify parties who may collect, receive, and/or use personal data of end users due to Customer's use of the DTM Service. Customer must disclose such parties to end users, and inform end users of the personal data collected by said parties and their purposes of using such personal data. Customer must obtain and record end users' valid consent for, e.g., the use of cookies or other technologies of the similar kind, where applicable. Customer must record such consent and provide end users with a method to withdraw their consent. If Customer violates this provision, we may restrict or suspend Customer's use of the DTM Service. Customer shall not upload any information that can be used to identify end users (such as names, email addresses, device identifiers, or invoices) to the DTM server.

8.1.4 The Data Processing Agreement (Attachment 1) is applicable to the processing described in Clause 8.1 herein.

8.2 As the data controller, Customer may, in some circumstances, collect personal data related to served Ads, including but not limited to the Open Advertising ID (OAID, the device ID generated by Huawei), the Google Advertising ID (GAID, the device ID generated by Google), User Agent (UA, a browser user agent), advertiser account ID, app ID, advertising task ID, creative ID, user behavior (such as Ads display, clicks, and downloads), and information about users' device and network, to perform attribution

analysis, conversion tracking, remarketing, fraud protection, and effect evaluation in accordance with the following terms:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9. Indemnification

9.1 To the maximum extent permitted by applicable laws, Customer shall defend, hold harmless, and indemnify Huawei and its Affiliates, subsidiaries, executives, directors of the board, employees, agents, partners, subcontractors, contractors, and licensors (collectively, the "Huawei Parties") against and from any and all claims, demands, suits, actions, and proceedings arising out of or in relation to any of the following events:

(a) Customer breaches any provisions of this Agreement;

(b) Customer breaches any of Customer's representations, warranties, or undertakings;

(c) Customer or Customer's Products infringe upon the intellectual property rights or other rights of Huawei or any third party;

(d) Customer or Customer's Products violate any applicable laws and regulations; and

(e) There are disputes between Customer and End Users.

9.2 Customer's indemnity to Huawei in Clause 9 shall include any and all liabilities, fines, penalties, damages, expenses, litigation costs, and attorney's fees arising from such claims, suits, or actions (whether under contract, tort, negligence, or restitution, or otherwise). Customer undertakes and agrees to promptly assist and cooperate as fully as reasonably required by any of the Huawei Parties in the defense of any such claims or requests. Huawei may, at its own expense, exclusively assume the defense and control of any and all matters subject to indemnification by Customer.

9.3 Customer shall assume any and all the risks from Customer's access and use of the Services to the maximum extent permitted by applicable laws. The full and maximum liability of the Huawei Parties, and the sole and only remedy for any and all of the compensation, claims, legal proceedings, responsibilities, obligations, losses, damages, costs, and/or property losses incurred due to Customer's use or failure to use the Services or any third-party service under this Agreement, shall be based on the actual loss that Customer has suffered, which shall not exceed the fees that Customer paid to use the Services within thirty (30) days before the event which caused the actual loss to the Customer, whether the basis for such alleged liability or remedy is in contract, tort (including negligence), restitution, or under any other legal theory or doctrine. Customer expressly acknowledges and agrees that the Huawei Parties do not assume any liability for any data loss or damage, profit loss, loss of business or goodwill, business disruption and/or any indirect, collateral, special, consequential, or punitive damage (even if Huawei has been informed of the possibility of such damage).

9.4 Nothing in this Agreement shall operate to limit the liabilities of either Party which cannot be limited or excluded by law.

10. DISCLAIMER

10.1 THE HUAWEI PARTIES DO NOT PROVIDE ANY EXPLICIT OR IMPLICIT REPRESENTATIONS OR WARRANTIES IN RESPECT OF THE SERVICES, INCLUDING BUT NOT LIMITED TO MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, AND NON-INFRINGEMENT. IF THE LOCAL LAWS AND/OR REGULATIONS IN FORCE DETERMINE THAT THE EXCLUSION OF CERTAIN STATUTORY PROVISIONS IS INVALID, HUAWEI'S LIABILITY FOR BREACH OF SUCH LAWS AND REGULATIONS WILL BE LIMITED TO THE MINIMUM EXTENT PERMITTED BY LAW.

10.2 THE SERVICES ARE PROVIDED ON AN "AS-IS" AND "AS AVAILABLE" BASIS AND ARE SUBJECT TO CHANGE WITHOUT NOTICE, AND CUSTOMER SHALL ASSUME ANY AND ALL RISKS ASSOCIATED WITH THE CONTENT AND/OR INFORMATION DOWNLOADED, OBTAINED, OR ACCESSED VIA THE SERVICES, AS WELL AS THE RISKS OF DEVICE/DATA DAMAGE AND CONTENT LOSS DUE TO THE USE OF THE SERVICES OR ANY THIRD-PARTY SERVICES. TO THE MAXIMUM EXTENT PERMITTED BY LAW, HUAWEI DOES NOT PROMISE TO NOTIFY CUSTOMER OF DEFECTS OR ERRORS.

11. Breach and Termination

11.1 Either Party (a "Non-Defaulting Party") may suspend the provision or use of the Services or terminate this Agreement by giving a written notice to the other Party (a "Defaulting Party") if the Defaulting Party:

(a) is in material breach of this Agreement, and the Defaulting Party explicitly refuses to remedy the breach, or such breach remains un-remedied within the period of time specified by the Non-Defaulting Party, which shall not be less than thirty (30) days after the Defaulting Party receives a written notice requiring it to take remedial measures from the Non-Defaulting Party;

(b) has ceased or threatened to cease carrying on its business;

(c) has a receiver, administrator, or any similar officer appointed for all or part of its assets or undertakings;

(d) makes any arrangement for the benefit of its creditors;

(e) goes into liquidation except for the purpose of a genuine merger or reconstruction;

(f) is declared bankrupt as an individual;

(g) has its operations banned by a government authority or applicable laws and/or regulations; or

(h) is in violation of, causes or induces Huawei to violate, or makes Huawei exposed to penalties, liabilities, sanctions, or restrictions under applicable laws or regulations.

11.2 Either Party may terminate this Agreement without a reason by providing a written notice to the other Party at least thirty (30) days prior to said termination. However, (i) Ads campaigns not cancelled under Clause 4 and new Ads campaigns may be run and reserved, and (ii) the continued use of the Services is, in each case, subject to this Agreement (available on the Ads Platform) effective from that time.

Huawei may suspend Customer's ability to participate in the Services at any time. In all cases, the running of any Customer Ad campaigns after the termination is at Huawei's sole discretion.

11.3 Any and all provisions of this Agreement which expressly or by their nature are intended to survive the termination of the Agreement shall remain in full force and effect subsequent to and notwithstanding such termination, until such provisions are satisfied or by their nature expire.

12. Changes to This Agreement

12.1 Notwithstanding any other provisions of the Agreement, Huawei may make non-material changes to this Agreement at any time without notice, but Huawei will provide advance notice of any material changes to this Agreement. The Agreement will be posted on the Ads Platform. The changes to this Agreement will not apply retroactively and will become effective 7 days after posting. However, changes made for legal reasons shall be effective immediately upon notice.

13. Confidentiality

13.1 A Party that receives or becomes aware of ("Receiving Party") any and all non-public information or data (including but not limited to technical information, trade secrets, and the content of this Agreement) ("Confidential Information") of the other Party ("Disclosing Party") shall keep strictly confidential such Confidential Information, and may not disclose any such Confidential Information to any third party without the prior written consent of the Disclosing Party. The Receiving Party agrees that it shall use such Confidential Information only for the purpose of performing this Agreement, and

agrees to adopt necessary and reasonable measures, no less stringent than the security measures adopted to protect its own Confidential Information, to protect the Disclosing Party's Confidential Information. The Receiving Party warrants that its personnel shall keep strictly confidential said Confidential Information to the extent that they need to access any Confidential Information for the purpose of performing the Receiving Party's obligations under this Agreement, and are bound by related Non-Disclosure Agreement with respect to said Confidential Information.

13.2 The Receiving Party shall, after this Agreement is terminated or upon the Disclosing Party's request, immediately return to the Disclosing Party any and all Confidential Information and the copies thereof that it has received from the Disclosing Party, unless the Receiving Party is unable or prohibited from doing so under this Agreement, or because of a legal requirement or direction, or because of legal proceedings, or to protect the legitimate rights and interests of the Receiving Party and third parties. In any event, the Receiving Party shall inform the Disclosing Party of the reason why it retains such Confidential Information and what Confidential Information it has retained.

14. Force Majeure

14.1 Neither Party shall be deemed to be in breach of this Agreement upon the occurrence of a Force Majeure Event which affects its ability to perform any of this Agreement. Notwithstanding this, the affected Party shall notify the other Party of the Force Majeure Event without undue delay and use its best commercial efforts to mitigate and remedy the negative effects thereof. For the purposes of this Agreement, a "Force Majeure Event" means (1) acts of God, lightning strikes, earthquakes, floods, droughts, storms, blizzards, snowstorms, mudslides, water erosion, explosions, fires, epidemics and other natural disasters; (2) acts of government, acts of war, acts of public enemy, terrorist activities, riots, commotions, and strikes, with the exception of labor disputes.

15. Export Controls

15.1 Customer hereby represents and warrants that Customer shall comply with any and all applicable laws and regulations regarding export controls and economic sanctions of the United Nations, the United States, the European Union, and other countries and regions. Customer shall obtain any and all necessary authorization and licenses as required by law at Customer's own cost. Customer undertakes NOT to use the Services for any purposes prohibited by applicable export controls laws, NOR to use the Services to upload, synchronize, or transmit any software, technologies (including technical data), and/or any other materials that are subject to the U.S. Export Administration Regulations (EAR). To the maximum extent permitted by law, Huawei is not liable for any losses or penalties that Customer may incur or suffer in connection with Customer's breach of the preceding representations, warranties, and undertakings.

16. Financial Compliance

16.1 Both Parties shall comply with any and all applicable domestic and international laws and regulations on economic sanctions, anti-money laundering and counter-terrorism financing.

16.2 Customer represents, warrants, and undertakes to Huawei that:

(a) neither Customer nor any of Customer's subsidiaries, directors of the board, executives, or, to Customer's best knowledge, any of Customer's shareholders, Affiliates, agents, or employees is an individual or body corporate ("Entity"), that is, or is controlled or owned (via shareholding) by Entities that are the subject/target ("Object of Sanction") of any economic sanctions, embargoes, or other restrictive measures enacted, administered, imposed, or enforced by the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC), the U.S. Department of State, the United Nations Security Council, the European Union, the People's Republic of China, and/or any other relevant governmental institutions, agencies, or authorities;

(b) none of the funds provided or to be provided by Customer under this Agreement are or have been directly or indirectly connected with any Object of Sanction or any activities that may violate any applicable laws/regulations, and that none of the funds received or to be received by Customer under this Agreement are or have been used to support or assist any activities that violate any applicable laws/regulations; and

(c) the bank account information provided by Customer is accurate, and Customer's bank account is registered in accordance with any and all applicable laws and regulations of the place (country/region) where Customer is located and/or where Customer's business is registered and Customer's bank account is opened.

17. Distribution Area and Signing Entities

17.1 Customer may select the countries and/or regions ("Business Area") to display Customer's Ads on the Platform when Customer uses the Services.

17.2 If Customer's Business Area is the Chinese mainland specified in Part I of Attachment 5 hereto, Customer is entering into and concluding this Agreement with Huawei Software Technologies Co., Ltd. which is legally established and incorporated in the People's Republic of China, and Customer designates Huawei Software Technologies Co., Ltd. as Customer's agent in the Chinese mainland.

17.3 If Customer's Business Area is one or more country(ies) and/or region(s) listed in Part II of Attachment 5 hereto, Customer is entering into and concluding this Agreement

with Aspiegel SE (formerly known as Aspiegel Limited) which is legally established and incorporated in Ireland, and Customer designates Aspiegel SE as Customer's agent in such countries and regions.

17.4 If Customer's Business Area is one or more country(ies) and/or region(s) listed in Part III of Attachment 5 hereto, Customer is entering into and concluding this Agreement with Huawei Services (Hong Kong) Co., Limited which is legally established and incorporated in Hong Kong (China), and Customer designates Huawei Services (Hong Kong) Co., Limited as Customer's agent in such countries and regions.

17.5 If Customer's Business Area covers countries and/or regions listed in more than one Part of Attachment 5 hereto, Customer shall enter into and conclude this Agreement with the corresponding Huawei entities respectively, in accordance with Clause 17.1-17.4 herein, and Customer shall respectively designate such Huawei entities as Customer's agent in the corresponding countries and/or regions. Any and all liabilities and obligations of each Huawei entity under each respective Agreement are several, and NOT joint, and in no event will any such Huawei entity be liable for any breach, liability, or other obligation of another Huawei entity with whom Customer has a separate Agreement.

18. Governing Laws and Dispute Resolution

18.1 If Customer is concluding this Agreement with Huawei Software Technologies Co., Ltd., Customer agrees that the establishment, jurisdiction, and interpretation of this Agreement shall be governed by the laws of the People's Republic of China. Customer agrees that this Agreement is signed in Longgang District, Shenzhen, China. Any and all disputes, compensation claims, and causes of action arising out of or in relation to performing this Agreement or receiving Huawei Services under this Agreement shall be resolved in a court with jurisdiction over the place where this Agreement is signed.

18.2 If Customer is concluding this Agreement with Aspiegel SE, Customer agrees that the establishment, jurisdiction, and interpretation of this Agreement shall be governed by the laws of Ireland. Customer also agrees that any and all disputes, compensation claims, and causes of action arising out of or in relation to performing this Agreement or receiving Huawei Services under this Agreement shall be submitted to the Irish Courts with jurisdiction in Dublin, Ireland, for litigation in the English language, without applying the United Nations Convention on Contracts for the International Sale of Goods.

18.3 If Customer is concluding this Agreement with Huawei Services (Hong Kong) Co., Limited, Customer agrees that the establishment, jurisdiction, and interpretation of this Agreement shall be governed by the laws of Hong Kong (China). Customer also agrees that any and all disputes, compensation claims, and causes of action arising out of or in relation to performing this Agreement or receiving Huawei Services under this

Agreement shall be submitted to the courts in Hong Kong (China) for litigation in the English language, without applying the United Nations Convention on contracts for the International Sale of Goods.

19. Miscellaneous

19.1 The contact persons of Customer and Huawei shall take charge of the liaison and coordination between Customer and Huawei during the fulfillment of this Agreement. All notices relating to this Agreement shall be in written form.

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

19.3 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 the Services.

19.4 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. Customer shall not transfer Customer's rights and obligations under this Agreement without Huawei's prior written consent.

19.5 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.

19.6 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.

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

19.8 The translations of this Agreement are for reference only. In accordance with Clause 17 herein, if Customer is concluding this Agreement with Huawei Software Technologies Co., Ltd., the standard version of this Agreement shall be in the Chinese language; if Customer is concluding this Agreement with Aspiegel SE and/or Huawei Services (Hong Kong) Co., Limited, the standard version of this Agreement shall be in the English language. In the event of any inconsistency between the translations of this Agreement and the standard version thereof, the standard version shall prevail.

19.9 In accordance with the applicable laws, including the Electronic Signature Law of the People's Republic of China, the Electronic Commerce Law of the People's Republic of China, the Electronic Transactions Ordinance (Cap. 553) of Hong Kong (China), the Electronic Commerce Act 2000 of Ireland and/or EU Regulation 910/2014 (on electronic identification and trust services for electronic transactions), the Parties hereby agree that they may execute this Agreement using electronic means, including the use of electronic acceptance by Customer or Huawei, which shall have the full force and legal effect as if traditional hand-written signatures had been affixed hereto. Customer acknowledges that Customer has the ability to retain this Agreement either by printing or saving it.

Attachment 1

Data Processing Agreement

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

2. Definitions

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

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

Customer Data means Personal Data provided by Customer.

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

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

EEA means the European Economic Area.

GDPR means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

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

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

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

Security Measures has the meaning given in Clause 4.1.1.

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

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

Sub-processors means third parties authorized under this DPA to have logical access to and Process

Customer Data in order to provide parts of the Services.

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

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

3. Roles, Scope of Processing, and General Obligations

3.1 The Parties acknowledge and agree that:

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

3.1.2 Each Party undertakes to comply with its obligations under the Applicable Laws and Regulations. Each Party is solely responsible for compliance with the obligations of the Applicable Laws and Regulations which apply to it. As between the Parties, 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 on Huawei) for any audit under Clause 4.4.2. Huawei will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

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

5. Personal Data Breach

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

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

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

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

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

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

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

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

5.5 Huawei will not assess the contents of Customer Data in order to identify information subject to any specific legal requirements. Without prejudice to Huawei's obligations under this Clause 6 (Assistance to the Controller), Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third party notification obligations related to any Data Incident(s).

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

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

6. Assistance to the Controller

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

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

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

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

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

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

6.3 Where required by Applicable Laws and Regulations, Huawei shall maintain a record of all categories of Processing activities carried out on behalf of 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 on Huawei for any assistance which Huawei considers to go beyond the aforementioned cooperation and assistance measures.

8. Data Location and Transfers

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

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

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

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

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

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

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

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

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

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

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

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

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

- The competent supervisory authority is the Irish Data Protection Commission

For avoidance of doubt, the Data Transfer Agreement applies only if the GDPR does not apply to the Processing. Without prejudice to Clause 9.2, Huawei may transfer data if it is required by applicable law to which Huawei is subject, provided that Huawei informs 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 at **https://developer.huawei.com/consumer/en/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. If, Applicable Laws and Regulations requires entering into Standard Contractual Clauses, MODULE THREE: "Transfer processor to processor" of the Standard Contractual Clauses with the

Sub-processors established in Third Countries is incorporated. Huawei's Sub-processors will act as "data importers" and Huawei will act as "data exporter" according to Clause 1 and Annex 1 of the Standard Contractual Clauses. Customer shall take into account Clause 8.3.

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

9.4 For the avoidance of doubt, in the event Huawei uses Sub-Processors, Huawei shall, pursuant to Applicable Laws and Regulations, remain fully liable to 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 are handled by the Data Center operator.

3. Access Control

3.1 Data Access by Customer

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

3.2 Internal Data Access Policy.

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

4. Personnel Security

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

4.2 Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Huawei's confidentiality and privacy policies. Personnel are provided with security training and their knowledge of security and privacy policies are evaluated periodically. Furthermore the latest security news from the world are delivered to personnel periodically to improve their awareness. Personnel handling Customer Data are required to complete additional requirements appropriate to their role (e.g., Huawei Cyber Security Certification). Huawei's personnel will not process Customer Data without authorization.

ANNEX 2:

STANDARD CONTRACTUAL CLAUSES
MODULE FOUR

Processor to Controller

SECTION I

Clause 1

Purpose and scope

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

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of

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

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

Clause 3

Third-party beneficiaries

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

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

(ii) Clause 8.1 (b) and Clause 8.3(b);

(iii) N/A

(iv) N/A

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18.

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016 /679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose (s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

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

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

N/A

Clause 10

Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11

Redress

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

Clause 12

Liability

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

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

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

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

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

Clause 13

Supervision

N/A

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

Clause 14

Local laws and practices affecting compliance with the Clauses

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and

practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

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

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

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

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

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

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

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

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g., technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall

suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

15.1 Notification

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

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

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

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the

data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

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

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

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

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

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

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

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

Clause 17

Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of Ireland with jurisdiction in Dublin.

APPENDIX

ANNEX I

A. LIST OF PARTIES

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

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

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

Signature and date: _____

Role (controller/processor): processor

Data Importer(s): 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.

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

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

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

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

Signature and date: _____

Role: controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Customer End Users

Categories of personal data transferred

Customer's conversion data

Customer-created target group data.

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

N/A

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

On a continuous basis when Customer decides to use HUAWEI Ads analytics, conversion tracking, and targeting features based on Customer's data.

Nature of the processing

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

Purpose(s) of the data transfer and further processing

As defined in Section 7.1 of the Agreement.

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

Customer can manage and erase data via Huawei Ads.

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

Data Center and operations and maintenance related sub-processors:

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

C. COMPETENT SUPERVISORY AUTHORITY

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

Irish Data Protection Commission

ANNEX II

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

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

ANNEX 3: Data Transfer Agreement (Processors)

Only when GDPR does not apply

Name of the data exporting organization:

Customer as defined in Agreement

(the data exporter)

And

Name of the data importing organization:

Huawei

(the data importer)

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

Clause 1: Definitions

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

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

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

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

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

(e) "Personal Data", "Special Categories of Data", "Process/Processing", "Controller", "Processor", "Data Subject", "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 defense and settlement of the claim.

Clause 6: Governing Law

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

Clause 7: Sub-processing

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

data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the Sub-processor's obligations under such agreement.

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

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

Clause 8: Data Transfers

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

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

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

Clause 10: Supplemental Provisions

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

APPENDIX 1 - DESCRIPTION OF TRANSFER

Data exporter

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

Attachment 2

STANDARD CONTRACTUAL CLAUSES

Controller to Controller

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of personal data to a third country.

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

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

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

(iii) N/A

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

(v) Clause 13;

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

(vii) Clause 16(e);

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

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 – Optional

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

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

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

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

8.2 Transparency

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

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

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

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

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

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

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

8.3 Accuracy and data minimisation

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

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

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

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation ([2]) of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

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

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

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

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

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

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

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union ([3]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

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

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

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

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

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

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible

risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

8.8 Processing under the authority of the data importer

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

8.9 Documentation and compliance

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

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

Clause 9

Use of sub-processors

N/A

Clause 10

Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. ([4]) The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

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

(i) provide confirmation to the data subject as to whether personal data concerning him /her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

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

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

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

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

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

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

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

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

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

Clause 11

Redress

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

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body ([5]) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

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

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

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

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

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

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

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

Clause 12

Liability

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

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

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

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

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

Clause 13

Supervision

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

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

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its

Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([6]);

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

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

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

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

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

Clause 15

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

15.1 Notification

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

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

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

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

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

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

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

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial

authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

Clause 17

Governing law

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

Clause 18

Choice of forum and jurisdiction

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

(b) The Parties agree that those shall be the courts of _Ireland_____ (specify Member State).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: Aspiegel SE

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

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

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

Signature and date: _____

Role (controller/processor): controller

Data importer(s): The Customer

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

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

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

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

Signature and date: _____

Role (controller/processor): controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Users interacting with Customer's ads served with HUAWEI Ads Platform.

Categories of personal data transferred

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

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

N/A

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

Whenever User interacts with Customer's ads.

Nature of the processing

Passing on ads behavior data to Customer.

Purpose(s) of the data transfer and further processing

To perform attribution analysis, conversion tracking, remarketing, anti-cheating, and effect evaluation.

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

Determined by each data controller separately

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

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

C. COMPETENT SUPERVISORY AUTHORITY

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

Irish Data Protection Commission

ANNEX II

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

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

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

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

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

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

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

•Manage access to protect personal data and systems or services that process and store personal data from unauthorized access following separation of duties and least privilege principles. Access controls should include identity management, authentication of users incorporating a strong password policy, authorization, accountability, network segregation, regular access reviews (i.e., rights and privileges) and access revocation where access is no longer necessary.

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

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

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

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

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

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

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

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

•Protect logs against modification or tampering.

•Protect the service infrastructure from unauthorized software being installed.

Attachment 3

Data Transfer Agreement

This Agreement is made and entered into

Between

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

And

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

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

WHEREAS

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

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

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

Definitions

For the purposes of the clauses:

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

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

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

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

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

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

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

I. Obligations of the Data Exporter

The Data Exporter warrants and undertakes that:

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

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

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

(d) It will respond to enquiries from Data Subjects and the authority concerning processing of the personal data by the Data Importer, unless the parties have agreed that the Data Importer will so respond, in which case the Data Exporter will still respond to

the extent reasonably possible and with the information reasonably available to it if the Data Importer is unwilling or unable to respond. Responses will be made within a reasonable time.

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

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

II. Obligations of the Data Importer

The Data Importer warrants and undertakes that:

(a) It will have in place appropriate technical and organizational measures to provide a standard of protection, that is comparable to the protection required by the PDPA and any requirements set out in any advisory or other guidelines issued from time to time by the PDPC, to the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

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

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

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

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

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

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

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

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

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

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

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

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

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

III. Liability and third party rights

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

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

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

IV. Law applicable to the clauses

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

V. Resolution of disputes with Data Subjects or the authority

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

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

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

VI. Termination

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

(b) In the event that:

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

ii. Compliance by the Data Importer with 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 Singapore or of the authority rules that there has been a breach of the clauses by the Data Importer or the Data Exporter; or

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

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

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

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

VII. Variation of these clauses

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

VIII. Description of the Transfer

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

ANNEX C: DATA PROCESSING PRINCIPLES

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

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

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

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

5. Rights of access, correction and objection: As provided under the PDPA, Data Subjects must, whether directly or via a third party, be provided with the personal information about them that an organization holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the Data Exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the Data Importer or other organizations dealing with the Data Importer and such interests are not overridden by the interests for fundamental rights and freedoms of the Data Subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about the rectified, amended where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organization may require further justifications before proceeding to rectification or amendment. Notification of any rectification, amendment to third parties to whom the data has been disclosed need not be made when this involves a disproportionate effort. A Data Subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation.

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

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

a) i. such decisions are made by the data importer in entering into or performing a contract with the data subject, and
ii. the data subject is given an opportunity to discuss the results of a relevant automated

decision with a representative of the parties making such decision or otherwise to make representations to that parties.

or

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

ANNEX D: DESCRIPTION OF THE TRANSFER

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

Data exporter

Role: Leader of Data Operation Team

Mail: privacy_hshk@huawei.com

Attachment 4

Data Transfer and Processing Agreement

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

And

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

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

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

• Advertiser account ID;

• Application ID;

• Advertising task ID;

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

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

Attachment 5

List of Countries/Regions

No.	**Countries/Regions**
Part I	Chinese mainland
Part II	Aland Islands, Albania, Andorra, Australia, Austria, Belgium, Bonaire, Bosnia and Herzegovina, Bulgaria, Canada, Croatia, Curacao, Cyprus, Czech Republic, Denmark, Dutch Caribbean, Estonia, Faroe Islands, Finland, France, Germany, Gibraltar, Greece, Greenland, Guernsey, Hungary, Iceland, Isle of Man, Israel, Italy, Jersey, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Monaco, Montenegro, Netherlands, New Zealand, North Macedonia, Norway, Poland, Portugal, Ireland, Romania, Saba, Saint Vincent and the Grenadines, San Marino, Serbia, Sint Eustatius, Sint Maarten, Slovakia, Slovenia, Spain, St. Martin, St. Pierre and Miquelon (France), Sweden, Switzerland, Turkey, Ukraine, United Kingdom, United States, Vatican City
Part III	Other countries and regions

Attachment 6

Invoice Types and Relevant Information

1. If Customer's Place of Registration and distribution area are the Chinese mainland, Huawei will issue Chinese VAT invoices to Customer.

1.1 If Customer is a general taxpayer, Huawei will issue a special VAT invoice to Customer. If Customer is a small-scale taxpayer or an individual, Huawei will issue a general VAT invoice to Customer.

1.2 Customer must provide the following information for Huawei to issue such VAT invoices:

(1) The copy of Customer's latest company business license (which shall be acquired after the three-in-one reform by integrating the business license, certificate of organization code, and certificate of taxation registration, including the purchaser's name and tax payer ID).

(2) Information about the account and the bank where the account was opened.

(3) Information about the invoice recipient, including but not limited to the recipient's name, receiving address, contact phone number, and email address.

2. Please refer to the table below for time of invoicing.

	Place of Registration	**Distribution Area**	**Signing Huawei Entity**	**Invoicing Date**
1	The Chinese mainland	Part I of Exhibit A of Attachment 5	Huawei Software Technologies Co., Ltd.	Within thirty (30) days after Partner top-up
	The EU, Russia, Switzerland, Serbia, Albania,			

2	Liechtenstein, Saudi Arabia, the United Arab Emirates, and Saskatchewan and British Columbia of Canada (subject to change based on changes of tax laws or taxpayer identity)	Part II of Exhibit A of Attachment 5	Aspiegel SE	Within three (3) days after Partner top-up
3	Russia, Malaysia, Saudi Arabia, the United Arab Emirates, South Africa, Morocco, Mexico, Chile, the EU, Kenya, Colombia, Oman, Switzerland, Thailand and Georgia (subject to change based on changes of tax laws or taxpayer identity)	Part III of Exhibit A of Attachment 5	Huawei Services (Hong Kong) Co., Limited	Within fourteen (14) days after Partner top-up
4	Others		Huawei Software Technologies Co., Ltd./Aspiegel SE /Huawei Services (Hong Kong) Co., Limited	Within the next month after the use of purchased Paid Services

ENDNOTE

[1.]Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when

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

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

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

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

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

6. As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements

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