Agreement on Use of Huawei APIs

Last updated: September 27, 2021

Thank you for using Huawei's APIs, associated services and software (collectively referred to as "APIs"). The following terms and conditions (the "Agreement") constitute a legally binding agreement between you and Huawei. By clicking the "I Agree" button (or any other similar button) below this Agreement, or by accessing or using any of the APIs, you shall be deemed to have fully understood and accepted this Agreement. Additional terms (including but not limited to terms in the accompanying documentation like the EU Standard Contractual Clauses and any applicable policies and guidelines) may apply to you, depending on the specific APIs you used. Said additional terms will be available with the relevant APIs, and become an integral part of this Agreement if you use those APIs (this Agreement and said additional terms are collectively referred to as the "APIs Agreements").

The APIs Agreements are supplementary agreements to the HUAWEI Developers Service Agreement between you and Huawei, and together with the latter govern your use of the APIs as a Huawei Developer. If you use the APIs as an interface to, or in conjunction with other Huawei products or services, then the terms for those other products or services shall also apply.

Any matters not addressed herein shall be subject to the HUAWEI Developers Service Agreement. In the event of any conflict between the APIs Agreements and the HUAWEI Developers Service Agreement, the APIs Agreements shall prevail with respect to any matters concerning your use of the APIs.

1. Definitions

Capitalized terms not defined in this Agreement shall have the same meanings ascribed to them in the HUAWEI Developers Service Agreement. The following terms shall have the following meanings when used in the APIs Agreements.

1.1 "APIs" means Huawei's APIs, associated services and software (including but not limited to APIs, SDKs and kits). APIs are managed by Huawei and/or its Affiliates; certain APIs are managed by AppTouch Providers when such APIs (as set forth here and may be updated from time to time) are integrated in your API Clients distributed via Huawei AppTouch platforms. APIs fall under the scope of "Huawei Services" as defined in the HUAWEI Developers Service Agreement.

1.2 "API Client(s)"; as defined in Clause 3.1. API Client(s) fall under the scope of "Products" as defined in the HUAWEI Developers Service Agreement.
1.3 "Data Controller" means any natural persons, body corporates, public institutions, government agencies, or other organizations that, by themselves or with other entities, determine the purposes and means of processing Personal Data.

1.4 "AppTouch Provider" means the entity that operates HUAWEI AppTouch.

1.5 "Data Processor" means any natural persons, body corporates, public institutions, government agencies, or other organizations that process Personal Data for and on behalf of a Data Controller.

1.6 “EEA” means the European Economic Area, consisting of the Member States of the European Union and Iceland, Liechtenstein and Norway.


1.8 “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.

1.9 "Huawei", "we", "our" or "us" means the signing entity determined in accordance with Clause 9 herein which provides services to you under the APIs Agreements.

1.10 "Huawei AppTouch" or "AppTouch" means the distribution platforms (a) for which Huawei cooperates with third parties, including but not limited to telecom carriers, in operations and branding, (b) developed and for which technical support is provided by Huawei, and (c) that allow Developers to showcase and distribute Products, such as apps and games, to End Users, in order to increase exposure, traffic, monetization opportunities, and users for the Products. The HUAWEI AppTouch list is set forth here. Huawei may update the list from time to time upon prior notice to you. If you have any comments or questions about the distribution of your Products on HUAWEI AppTouch, you may contact Huawei through your account manager at Huawei or via apptouch@huawei.com. Huawei will respect your choice.

1.11 “Parties” means you and Huawei (see definition above).

1.12 “Personal Data” means any information relating to an identified or identifiable natural person in so far as it is processed under this Agreement.
1.13 **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. Using Our APIs

2.1 License to You

Subject to the terms and conditions of the APIs Agreements, Huawei grants you a limited, revocable, non-exclusive, non-transferable, and non-sublicensable license to integrate, copy, and use the APIs in your API Clients.

2.2 Your End Users

You shall require your End Users to comply with (and not knowingly enable them to violate) applicable laws, regulations, and the APIs Agreements.

2.3 Compliance with Laws, Third-Party Rights, and Other Agreements with Huawei

You shall comply with any and all applicable laws, regulations, and third-party rights (including but not limited to laws regarding the import or export of data or software, privacy, and local laws). You may not use the APIs to encourage or promote illegal activities or violation of third-party rights. You may not violate any other agreements you made with Huawei or its Affiliates as a Huawei Developer (collectively "Huawei Agreements").

2.4 Permitted Access

You shall only access (or attempt to access) an API by the means described in the documentation of that API. If Huawei assigns you developer credentials (for example, passwords, keys, and client IDs), you shall use them with the applicable APIs. You may not misrepresent or mask either your identity or your API Client's identity when using the APIs or your Developer Account.

2.5 API Limitations

Huawei may set and enforce limits on your use of the APIs (for example, limiting the number of API requests that you may make or the number of End Users you may serve), in our sole discretion. You agree to, and will not attempt to circumvent, such limitations.

2.6 Open Source Software
Some of the software required by or included in our APIs may be offered under an open source license. Open source software licenses constitute separate written agreements. For certain APIs, open source software is listed in the documentation of the APIs. To the limited extent the open source software license expressly supersedes the APIs Agreements, the open source license instead sets forth your agreement with Huawei for the applicable open source software.

2.7 Feedback

If you provide feedback or suggestions about our APIs, then we may use such information without liability to you.

2.8 Non-Exclusivity

The terms of the APIs Agreements are non-exclusive. You shall acknowledge that Huawei may develop products or services that may compete with your API Client or any other products or services.

2.9 Charging Standards and Payment Policies

The charging standards and payment policies of a given API (if any) will be subject to relevant information provided with that API on the Website.

3. Your API Clients

3.1 API Clients

The APIs are designed to help you enhance your websites and applications ("API Client(s)"). You agree that Huawei may monitor the use of the APIs to ensure quality, improve products and services, and verify your compliance with the APIs Agreements. This monitoring may include Huawei’s access to and use of your API Client, for example, identifying security issues that may affect Huawei or its users. You may not interfere with this monitoring. Huawei may use any technical means to overcome such interference. Huawei may suspend access to the APIs by you or your API Client without notice if we reasonably believe that you are in violation of the APIs Agreements.

3.2 Security

You shall make commercially reasonable efforts to protect user information collected by your API Client, including Personal Data, from unauthorized access or use. The
protection standards shall be higher than or equal to Huawei's privacy protection standards. You shall promptly report to your End Users any unauthorized access or use of such information to the extent required by applicable laws.

3.3 Ownership

Huawei does not acquire ownership in your API Client, and by using our APIs, you do not acquire ownership of any rights in our APIs or the content that is accessed through our APIs.

4. Prohibitions and Confidentiality

4.1 API Prohibitions

When using the APIs, you may not (or allow those acting on your behalf to) violate the HUAWEI Developers Service Agreement, and you may not:

a. sublicense an API for use by any third party. Consequently, you may not create an API Client that functions substantially the same as the APIs and offer it for use by third parties.

b. perform an action with the intent of introducing to Huawei products and services any viruses, worms, defects, Trojan horses, malware, or any items of a destructive nature.

c. reverse engineer or attempt to extract the source code from any API or any related software, except to the extent that this restriction is expressly prohibited by applicable laws.

d. use the APIs for any activities where the use or failure of the APIs could lead to death, personal injury, or environmental damage (such as the operation of air traffic control, or life support systems).

e. remove, obscure, or alter any terms of the APIs Agreements or any links to or notices of those terms.

4.2 Confidential Matters

a. Developer credentials (such as passwords, keys, and client IDs) are intended to be used by you and identify your API Client. You shall keep your credentials confidential and secure and take all reasonably necessary measures to prevent and discourage other API Clients from using your credentials. Developer credentials may not be embedded in open source projects.
b. Our communications to you and our APIs may contain Huawei's Confidential Information or AppTouch Providers' Confidential Information, as applicable. If you receive such Confidential Information, you may not disclose it to any third parties without prior express consent in writing by Huawei or relevant AppTouch Providers (as applicable). This clause 4.2.b shall survive the termination of the APIs Agreements.

5. Content

5.1 Content Accessible Through Our APIs

Our APIs contain some third-party content in various forms (such as text, maps, images, videos, audio, or software) for which we are not responsible, but we may review content from time to time to determine whether it is illegal or violates our policies or the APIs Agreements, and we may remove or refuse to display content. Huawei is not responsible for the accuracy or political stance of any third-party content. You understand that the APIs provide content interfaces only. You may determine whether to use the content within your control. Huawei shall not be liable for any and all losses and liabilities caused by third-party content.

Content accessible through our APIs may be subject to intellectual property rights, and, if so, you may not use it unless you are licensed to do so by the owner of that content or are otherwise permitted by law. Your access to the content provided by the APIs may be restricted, limited, or filtered in accordance with applicable laws, regulations, and policies.

5.2 Submission of Content

Some of our APIs allow the submission of content. Huawei does not acquire any ownership of any intellectual property rights in the content that you submit to our APIs through your API Client, unless otherwise specified in the APIs Agreements. For the sole purpose of enabling Huawei to provide, secure, and improve the APIs (including the related service(s)) and only in accordance with the applicable Huawei privacy policies, you hereby grant to Huawei a perpetual, irrevocable, worldwide, sublicensable, royalty-free and non-exclusive license to use the content submitted, posted, or displayed to or from the APIs through your API Client. When you submit content to our APIs through your API Client, you also represent and warrant that you have all the necessary rights (including the necessary rights from your End Users) required to grant us the license for use of said content for the purposes of the APIs Agreements.

5.3 Retrieval of Content
When a user's non-public content is obtained through the APIs, you may not expose that content to any other users or third parties without appropriate legal base (such as explicit opt-in consent from that user if applicable).

5.4 Prohibitions on Content

Unless expressly permitted by the content owner or by applicable law, you may not, and may not permit your End Users or others acting on your behalf to, perform the following operations with the content returned from the APIs:

a. scrape data, build databases, or otherwise create permanent copies of such content, or keep cached copies longer than permitted by the cache header;

b. copy, translate, modify, and create derivative work of, sell, lease, lend, convey, distribute, publicly display, or sublicense to any third party;

c. misrepresent the source or ownership; or

d. remove, obscure, or alter any copyright, trademark, or other proprietary rights notices; or falsify or delete any author attributions, legal notices, or other labels of the origin or source of materials

6. Privacy Protection

6.1 Personal Data Generated during End User's Use of Products and Services of Huawei or within AppTouch:

a. Upon prior authorization of an End User, or upon other applicable legal basis of Personal Data processing, your corresponding API Client, when integrated following APIs, may obtain relevant Personal Data generated during the use by such End User of products and services provided by Huawei, or otherwise generated during the use of products and services provided within AppTouch as follows:

(i) Account API: your API Client can obtain relevant account data such as End User's name, and avatar, to allow the login;

(ii) In-App Purchase API: your API Client can obtain relevant transaction information, such as order ID, and order details to finalize the purchase;

(iii) Game Service API: your API Client can obtain relevant player's stats, rankings and achievements. You must not display the Game service data of an End User to other End Users without said End User's authorization;
(iv) AppGallery Connect API: If you provide services for Huawei Developers and help them use the services of AppGallery Connect, your API Client can obtain the data of the Huawei Developers in AppGallery Connect, such as information about their HUAWEI ID, team account, contact information, credentials, device commissioning, projects, apps, operational reports, products, and game service configurations;

(v) Location API: When you are using the location services provided by Huawei in connection with your Products, we may share location information of End Users (such as longitude and latitude as well as the accuracy information) with you. When using our location services, you shall further comply with the terms of the **HUAWEI Location Service Agreement**.

b. By using relevant APIs in accordance with Clause 6.1.a herein, you are the Data Controller of the Personal Data of corresponding End User your API Client obtained from Huawei or AppTouch Providers (as applicable) as referred to in Clause 6.1.a. For clarity's sake, when your API Clients are distributed via any platform of AppTouch, the relevant AppTouch Provider is the Data Controller of Personal Data processed for the provision of services of such AppTouch, and Huawei is the data processor of such data. You and Huawei, or you and said AppTouch Provider, are independent Data Controllers. Each Party shall observe any and all applicable privacy laws and regulations.

c. Further, in accordance with Clause 9 herein:

(i) if

(1) you are contracting the APIs Agreements with Aspiegel SE, and you are located in a Third Country, or
(2) Personal Data is transferred between relevant AppTouch Provider established in EEA and you (as applicable), when you are located in a Third Country,

then Huawei and you, or relevant AppTouch Provider and you (as applicable), shall comply with the EU Standard Contractual Clauses provided in Attachment A for export and import of such Personal Data. The Parties shall be deemed to have executed the EU Standard Contractual Clauses, according to the process described in the preamble of this Agreement, such that:

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

• Huawei (or the relevant AppTouch Provider, as applicable) is the “data exporter” and You are the “data importer” referred to in the EU 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 Irish law;

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

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

• in case of discrepancy with any provision in the APIs Agreements, the EU Standard Contractual Clauses shall prevail.

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

(ii) if you are contracting the APIs Agreements with Huawei Services (Hong Kong) Co., Limited, and your Business Area is not Russia, and your servers to receive such data are located outside of Singapore, then Huawei and you, or relevant AppTouch Provider and you (as applicable), shall comply with the Data Transfer Agreement as provided in Attachment B for export and import of such Personal Data.

(iii) if you are contracting the APIs Agreements with Huawei Services (Hong Kong) Co., Limited, and your Business Area is Russia, and your servers to receive such data are located in Russia, then Huawei and you, or relevant AppTouch Provider and you (as applicable), shall comply with the Data Transfer Agreement in Compliance with Russian Legislation as provided in Attachment C for export and import of such Personal Data.

6.2 Personal Data Generated during the Use of API Client by End User

In relation to services provided by Huawei, where you are collecting End Users' Personal Data directly from End Users as a Data Controller, Huawei processes such Personal Data as your data processor in accordance with the AppGallery Connect Data Processing Addendum, which is an integral part of the APIs Agreements.

6.3 You shall select your data processing location when you are using some services as a Data Controller, so that Huawei may process the data of your API Client and End Users at the location that you selected. You shall ensure that the data processing location that you selected complies with any and all applicable laws and regulations of the place where you and your End Users are located.
6.4 Protection of End Users' Personal Data

You warrant and undertake to protect Personal Data of all End Users. You and your API Clients shall comply with all applicable privacy laws and regulations including those applying to Personal Data. You shall provide and adhere to a conspicuous privacy policy for your API Client that clearly and accurately describes to End Users of your API Client what End User information you will collect and how you will use and share such information (including for advertising) with Huawei and third parties.

You warrant and undertake to ensure that Personal Data of End Users are only collected and used for the limited purpose which is deemed to be necessary and processed lawfully in accordance with applicable laws, and only retained for the minimum necessary period. Personal Data in your possession shall be kept safe and secure from any actual or potential abuses.

7. Termination

7.1 Termination

a. Upon termination of the HUAWEI Developers Service Agreement by either Party, the APIs Agreements shall terminate automatically on the same day. However, termination of the APIs Agreements by either Party will not result in the termination of the HUAWEI Developers Service Agreement.

b. You may stop using our APIs at any time with or without notice. If you desire to terminate the APIs Agreements, you shall provide Huawei with prior written notice and cease your use of the applicable APIs. Huawei reserves the right to terminate the APIs Agreements for a given API or all APIs with you or discontinue the APIs or any portion or feature thereof or your access thereto for any reason and at any time without liability or other obligation to you.

7.2 Your Obligations after Termination

Upon any termination of the APIs Agreements or discontinuation of your access to an API, you shall immediately stop using that API, and delete any cached or stored content that was permitted by the cache header under Clause 5 herein. Huawei may independently communicate with any account owner whose account(s) is/are associated with your API Client and developer credentials to provide notice of the termination of your right to use an API.

7.3 Surviving Provisions
When the APIs Agreements come to an end, those terms that by their nature are intended to continue indefinitely will continue to apply, including but not limited to Clauses 4.2, 5, 7, and 8 herein.

8. Liability for Our APIs

8.1 LIMITATION OF LIABILITY

To the fullest extent permitted by law:

- Huawei Parties (including AppTouch Providers) shall not be responsible for lost profits, revenues, or data; financial losses; or indirect, special, consequential, exemplary, or punitive damages.

- Huawei shall not be liable for any losses (direct or indirect) or damages arising out of or relate to your use of the APIs.

- You understand and agree that said Huawei Parties shall not be liable for any failure to save, modify, delete, or store your information and data generated by your API Clients, or any third-party information.

- In all cases, said Huawei Parties shall not be liable for any expense, loss, or damage that is not reasonably foreseeable.

8.2 Indemnification

Unless prohibited by applicable laws, you shall defend and indemnify said Huawei Parties and Huawei's users from and against any and all liabilities, damages, losses, costs, fees (including legal fees), and expenses relating to any allegation or third-party legal affairs to the extent arising from your violation of your representations, warranties, covenants, and undertakings in the HUAWEI Developers Service Agreement and/or the APIs Agreements, as well as the following:

a. your or your End Users' misuse or illegal use of the APIs;

b. your violation or your End Users' violation of the APIs Agreements;

c. any content or data imported into or used with the APIs by you, those acting on your behalf, or your End Users;

d. your violation of your privacy compliance and cyber security obligations to any third party.
8.3 Procedure for Handling

You understand and agree that Huawei has the right to check for your violations upon its reasonable judgment. You irrevocably accept the results and evidence of any violations (including but not limited to the electronic evidence collected by Huawei and/or its Affiliates through technical means) regarding your use of the APIs. The actions that Huawei takes against your violations in accordance with the APIs Agreements shall not exempt you from the legal liabilities that you shall bear in accordance with the APIs Agreements as well as applicable laws and regulations.

If Huawei suspects you to have been in breach of the APIs Agreements, you shall at Huawei's request provide information and/or evidence to explain your suspected breach. If you fail to do so, or if Huawei reasonably believes that you are in breach of the APIs Agreements, Huawei may take one or more of the following measures:

a. block, remove, and/or delete data, algorithms, models, and/or information, or disconnect links;

b. require you to replace and/or modify the content in violation immediately;

c. restrict, suspend, or terminate your use of relevant APIs and/or your Account (including but not limited to suspending some or all of relevant services, and stopping the provision of relevant resources);

d. take other reasonable measures that Huawei deems appropriate.

9. Contracting Entity

9.1 The Parties hereby acknowledge and agree that, for and only for the Huawei Services in relation to APIs under the APIs Agreements, the content of Clause 14.1 (Distribution Area and Signing Huawei Entity) of the HUAWEI Developers Service Agreement shall be replaced with following content:

"14.1 You may select the countries and/or regions ("Business Area") to display and/or distribute your Products on Huawei Platforms when you use Huawei Services. If you have not displayed and/or distributed your Products when you use Huawei Services, the country or region that you registered in your identity verification profile shall be deemed as your Business Area. However, if you are required to select on a Huawei Platform a storage location of data generated in the use of a Huawei Service integrated in your Product, the storage location you selected shall be deemed as your Business Area in relation to the use of such Huawei Service."
9.2 For the avoidance of doubt, the original Clause 14 of the HUAWEI Developers Service Agreement shall remain unchanged for and still govern any Huawei Services other than those in relation to APIs which are provided under the APIs Agreements.

10. Governing Law and Dispute Resolution

Please refer to the Clause headed "Governing Law and Dispute Resolution" of the HUAWEI Developers Service Agreement.

Attachment A: EU Standard Contractual Clauses

Standard contractual clauses for the transfer of personal data from the EEA to Third Countries (controller to controller transfers)

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

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.
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.

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 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 (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
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.
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.

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.

(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;
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).
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.

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.

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 with jurisdiction in
Dublin.

(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.
Endnotes:

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 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.

3 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.
ANNEX I

A. LIST OF PARTIES

Data exporter(s):

**Name:** shall be Aspiegel SE, or the relevant AppTouch Provider listed [here](#) (as applicable)

**Address:** shall be the address of Aspiegel SE (1F, Simmonscourt House, Ballsbridge, Dublin, D04 W9H6, Ireland) or the address of relevant AppTouch Provider, as listed [here](#) (as applicable)

**Contact person’s name, position and contact details:** Joerg Thomas, Director, DPO
Office [dpo@huawei.com](mailto:dpo@huawei.com)

**Activities relevant to the data transferred under these Clauses:** provision of the different APIs and the related services provided to the data importer by the data exporter, in particular the processing of Personal Data based on the APIs described under clause 6.1.a of the API’s Agreement.

Signature and date:

**Role:** Controller

Data importer(s):

**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: your contact details and information as you have provided them in context of the AGC services and registration of your Developer account

Activities relevant to the data transferred under these Clauses: use of the different APIs and the related services provided to the data importer by the data exporter, in particular the processing of Personal Data based on the APIs described under clause 6.1. a of the API’s Agreement.

Signature and date:

Role: Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

• Data subjects of the data exporter who have signed both the AppGallery and IAP user agreements (or other similar agreements in case the data subject is using the services of AppTouch Provider) and made in-app purchases;

• Data subjects of the data exporter who have signed both the AppGallery and IAP user agreements (or other similar agreements in case the data subject is using the services of AppTouch Provider) and have an active subscription within the importer service.

• Data subjects of the data exporter who have authorized the importer to access their account information (including in relation to the services provided by AppTouch Providers).

• Data subjects of the data exporter who have signed the AppGallery user agreement (or similar agreement in case the data exporter is AppTouch Provider), enabled the Game Service feature and authorized the disclosure to the importer.

• Data subjects of the data exporter who have authorized the importer to access AppGallery Connect information.
• Data subjects of the data exporter who have signed the Agreement on Use of Huawei APIs and authorized the disclosure to the importer.

• Data subjects of the data exporter who have authorized the data exporter to disclose and the data importer to access their location information in relation to the applications or services provided by the data importer.

**Categories of personal data transferred:**

• Payment information except bank card information, such as the order number, amount, subscription information (subscription ID), and currency (including also in relation to services of AppTouch Providers)

• HUAWEI ID or AppTouch account information (as applicable)

• Game Service data, such as player ID, rankings, achievements, purchases, player stats (including also in relation to services of AppTouch Providers)

• AppGallery Connect data, such as information about HUAWEI ID, team account, contact information, credentials, device commissioning, projects, apps, operational reports, products, and game service configurations.

• Data subject's location (the precision of the GNSS coordinate and relevant location data).

• Geo fence information (regarding whether a user has entered, left, or stayed in a geo fence and related information).

**Sensitive data transferred and applied restrictions or safeguards:**

N/A

**The frequency of the transfer:**

The data transfers are triggered by use of the services by the data subjects, in particular by certain action taken by the data subject (such as making an In-App purchase in services of Huawei or AppTouch Providers or logging in with Huawei ID account or AppTouch account information) and may also happen on a continuous basis if e.g. the data subject has enabled some feature (such as enabling location services for the product of the Customer).
Nature of the processing

The data is transferred through the API channels to Customer to enable the provision of the relevant features and services.

Purpose(s) of the data transfer and further processing

• Allow the settlement between data exporter and Developer.

• Allow the management of an active subscription to the data importer service.

• Allow the data subjects to log in on the importer application with their respective accounts and enable importer to provide account functionalities relying on access to data subject's account related information (e.g. access security events for maintaining account security, access basic profile information and address information to create and maintain user profile information, etc.).

• Allow the data subjects to use the Game Service features available on the importer application. Additionally, to allow the importer to improve its service when authorized by the data subjects.

• Allow the data subjects to log in on the importer application with their respective account and enable importer to provide functionalities relying on access to data subject's AppGallery Connect related information (e.g. managing project information, developing and testing apps, submitting applications to be released, viewing operation reports, managing product information, and managing game service configurations, etc.).

• Allow the data importer to provide location-based services and features for the data subjects within the applications or services of the data importer.

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

In accordance with the privacy policies and data retention practices of the data importer, subject to the applicable data protection laws.
C. COMPETENT SUPERVISORY AUTHORITY

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

As set out in Section 6 above.

ANNEX II

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

The following measures are the minimum required to be implemented by the data importer on the transferred Personal Data:

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

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

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

• Manage supplier relationships including security requirements, SLAs, outsourcing agreements for contracts being used as part of the service provision including data processing agreements in place with the sub-processors you use to deliver the services or products in accordance with the GDPR.
• Perform appropriate background checks on personnel (employees, contractors and third party users) before hiring, when needed and legally permitted.

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

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

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

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

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

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

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

• Assets are inventoried, classified and updated when changes occur (i.e. new systems/software introduced, systems decommissioned).
• Establish change and configuration management procedures for key network and information systems to manage configuration securely.

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

• Protect logs against modification or tampering.

• Protect the service infrastructure from unauthorized software being installed.

• Ability to restore the availability and access to the Personal Data in a timely manner in the event of a physical or technical incident (i.e. security incidents and/or data breaches) through effective detection, response and reporting capabilities.

• Provide continuity for the services offered, ability to recover from data loss, protection against compromise, provision of appropriate failover, necessary data retention and an effective data backup policy.

• Use pseudonymisation and encryption to protect the confidentiality of personal data and other sensitive data while in transit or at rest. Encryption should meet industry standard requirements like NIST FIPS 140.

• Ensure personal data removal, deletion and sanitization measures meet appropriate levels of security.

• Service software is developed in a secure way through secure coding practices, following industry best practices (i.e. OWASP Top 10, Secure Coding Standards) including vulnerability analysis.

• Ensure perimeter and internal network protection, maintain physical or logical separation between the perimeter network and internal networks containing personal data. Development and test environments are secured and separated from live production environments.

• Ensure physical security of locations at which personal data is processed including reasonable steps to protect against unauthorized access.

• Devices used for handling Personal Data should not permit data to be written to removable media or to have data read from same nor should they allow printing of
Personal data to an unauthorized printer. Such devices should have password protected screensavers implemented and be locked as a matter of course when the user leaves the workstation.

• All important and confidential documentation is removed from the desk and locked away when items are not in use or an employee leaves his/her workstation; and

• Remote access to network and information systems is secured through VPN connection while using devices that have been adequately secured against compromise (e.g. through the use of antivirus software and patching devices with available security fixes)

Attachment B: Data Transfer Agreement

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

This Agreement is made and entered into

Between

Name of data exporting organization: Huawei Services (Hong Kong) Co., Limited ("Huawei")

Address: Room 03, 9/F, Tower 6, the Gateway, No. 9 Canton Road, Tsim Sha Tsui, Kowloon, Hong Kong.

Company registration number: 1451551

and/or relevant AppTouch Provider outside both EU/EEA and Russia

hereinafter "data exporter"

And
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 B 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 B, which forms an integral part of the clauses.

I. Obligations of the Data Exporter

The Data Exporter warrants and undertakes that:

(a) The personal data 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.

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, which 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 B, 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 processing of the personal data, and will cooperate in
good faith with the Data Exporter, the Data Subject and the authority concerning all such
enquiries within a reasonable time. In case of legal dissolution of the Data Exporter, or if
the parties have so agreed, the Data Importer will assume responsibility for compliance
with the provisions of clause I(e).

(f) At the request of the Data Exporter, it will provide the Data Exporter with evidence
of financial resources sufficient to 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 A.
(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

(1) 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;

(2) 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.

### 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).

### IV. Law applicable to the clauses

These clauses shall be governed by the laws of Singapore.
V. Resolution of disputes with Data Subjects or the authority

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

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

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

VI. Termination

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

(b) In the event that:

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

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

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

(iv) A final decision against which no further appeal is possible of a competent court of Singapore or of the authority rules that there has been a breach of the clauses by the Data Importer or the Data Exporter; or
(v) A petition is presented for the administration or winding up of the Data Importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the Data Importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs then the Data Exporter, without prejudice to any other rights which it may have against the Data Importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the Data Importer may also terminate these clauses.

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

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

VII. Variation of these clauses

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

VIII. Description of the Transfer

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

DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently 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, 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 B to the Data Transfer Agreement

DESCRIPTION OF THE TRANSFER

Data subjects
The personal data transferred concern the following categories of data subjects:

•Data subjects of the data exporter who have signed both the AppGallery and IAP user agreements and made in-app purchases;

•Data subjects of the data exporter who have signed both the AppGallery and IAP user agreements and have an active subscription within the importer service.

•Data subjects of the data exporter who have authorized the importer to access their respective account information.

•Data subjects of the data exporter who have signed the AppGallery user agreement, enabled the Game Service feature and authorized the disclosure to the importer.
• Data subjects of the data exporter who have authorized the importer to access AppGallery Connect information.

• Data subjects of the data exporter who have signed the Agreement on Use of Huawei APIs and authorized the disclosure to the importer.

• Data subjects of the data exporter who have authorized the data exporter to disclose and the data importer to access their location information in relation to the applications or services provided by the data importer.

Purposes of the transfer(s)
The transfer is made for the following purposes:

• Allow the settlement between Exporter and Developer.

• Allow the management of an active subscription to the importer service.

• Allow the data subjects to log in on the importer application with their respective accounts and enable importer to provide account functionalities relying on access to data subject's account related information (e.g. access security events for maintaining account security, access basic profile information and address information to create and maintain user profile information, etc.).

• Allow the data subjects to use the Game Service features available on the importer application. Additionally, to allow the importer to improve its service when authorized by the data subjects.

• Allow the data subjects to log in on the importer application with their respective accounts and enable importer to provide functionalities relying on access to data subject's AppGallery Connect related information (e.g. managing project information, developing and testing apps, submitting applications to be released, viewing operation reports, managing product information, and managing game service configurations, etc.).

• Allow the data importer to provide location-based services and features for the data subjects within the applications or services of the data importer.

Categories of data
The personal data transferred concern the following categories of data:
• Payment information except bank card information, such as the order number, amount, subscription information (subscription ID), and currency.

• HUAWEI ID or relevant AppTouch account information (as applicable).

• Game Service data, such as player ID, rankings, achievements, purchases, player stats.

• AppGallery Connect data, such as information about HUAWEI ID, team account, contact information, credentials, device commissioning, projects, apps, operational reports, products, and game service configurations.

• Data subject's location (the precision of the GNSS coordinate and relevant location data).

• Geo fence features (regarding whether a user has entered, left, or stayed in a geo fence and relevant information).

**Recipients**
The personal data transferred may be disclosed only to the following recipients or categories of recipients:

• Data importer

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

**Data protection registration information of data exporter (where applicable)**
N/A

**Additional useful information (storage limits and other relevant information)**
Contact points for data protection enquiries

Data importer  Data exporter
Attachment C: Data Transfer Agreement in Compliance with Russian Legislation

This Agreement is made and entered into between

Name of data exporting organization

Huawei Services (Hong Kong) Co., Limited (Room 03, 9/F, Tower 6, the Gateway, No. 9 Canton Road, Tsim Sha Tsui, Kowloon, Hong Kong) ("Huawei")

and/or relevant AppTouch Provider in Russia

hereinafter "data exporter"

And

Developer who signed the Agreement on Use of Huawei APIs with Huawei and part of the Agreement, hereinafter "data importer",

each a "party" and together "the parties".

Each of the parties is a personal data operator, including personal data processed as part of the fulfillment of obligations provided within the Agreement on Use of Huawei APIs.

For the purposes of the Agreement, personal data refers to information that is in accordance with the legislation of the Russian Federation, to be transferred by data exporter to data importer and includes the following data:

• Payment information except bank card information, such as the order number, amount, subscription information (subscription ID), and currency.
• HUAWEI ID or AppTouch account information (as applicable).

• Game Service data, such as player ID, rankings, achievements, purchases, player stats.

• AppGallery Connect data, such as information about HUAWEI ID, team account, contact information, credentials, device commissioning, projects, apps, operational reports, products, and game service configurations.

• Data subject's location (the precision of the GNSS coordinate and relevant location data).

• Geo fence features (regarding whether a user has entered, left, or stayed in a geo fence and relevant information).

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

• Data subjects who have signed both the AppGallery and IAP user agreements and made in-app purchases;

• Data subjects who have signed both the AppGallery and IAP user agreements and have an active subscription within service of data importer.

• Data subjects who have authorized data importer to access their respective account information.

• Data subjects who have signed the AppGallery user agreement, enabled the Game Service feature and authorized the disclosure to data importer.

• Data subjects who have authorized data importer to access AppGallery Connect information.

• Data subjects who have signed the Agreement on Use of Huawei APIs and authorized the disclosure to data importer.

The transfer is made for the following purposes:

• Allow the settlement between data exporter and Developer.

• Allow the management of an active subscription to data importer's service.
• Allow the data subjects to log in on data importer's application with their respective accounts and enable data importer to provide account functionalities relying on access to data subject's account related information (e.g. access security events for maintaining account security, access basic profile information and address information to create and maintain user profile information, etc.).

• Allow the data subjects to use the Game Service features available on data importer's application. Additionally, to allow data importer to improve its service when authorized by the data subjects.

• Allow the data subjects to log in on data importer's application with their respective accounts and enable data importer to provide functionalities relying on access to data subject's AppGallery Connect related information (e.g. managing project information, developing and testing apps, submitting applications to be released, viewing operation reports, managing product information, and managing game service configurations, etc.).

• Allow the data importer to provide location-based services and features for the data subjects within the applications or services of the data importer.

The transfer of personal data is not considered by the Parties as an instruction to process personal data.

Each of the parties shall ensure the confidentiality of personal data received within the framework of the Agreement, compliance with the requirements for personal data processing established by Federal Law No. 152-FZ of July 27, 2006 "On Personal Data" and regulatory acts adopted in its execution, and shall be responsible for taking all necessary legal, organizational and technical measures to protect personal data from unauthorized or accidental access to them, destruction, modification, blocking, copying, dissemination of personal data as well as other illegal actions such data.

The party that provides personal data shall be responsible for the legality and accuracy of provided data to other party for the purpose of executing the Agreement, as well as for obtaining the consent of the data subjects to transfer their personal data to the other party in the manner prescribed by the legislation of the Russian Federation personal data.
The party that received personal data from the other party does not assume the obligation to inform the data subjects whose personal data has been transferred about the beginning of their processing, since the party that transfers personal data must bear the obligation to inform the data subjects accordingly.

The party receiving personal data has the right to engage in processing the received personal data of third parties for the purpose of executing the Agreement in the necessary volume only if the other party provides confirmation of receipt of the relevant consent from the personal data subject. In any case, a party is obliged, upon the request of the other party, to provide information about third parties who were provided with personal data or who had access to them: their full and abbreviated names, address of the location (place of registration and residence), information about which particular personal data what particular subjects and for what purposes were transferred to third parties.