DATA PROCESSOR AGREEMENT

This Data Processor Agreement is entered between the Hyxipower entity ("**Hyxipower**") and the legal person ("**Partner**") that are parties to a "Distribution Agreement" or "Hyxipower Dealer Partner Program Agreement" or any other agreement entered between the Partner and Hyxipower and under which Hyxipower needs to process Personal Data and such agreement expressly incorporates by reference the terms of this Data Processor Agreement ("**Processor Agreement**") by signing the relevant acknowledgement. (collectively hereinafter as "**Parties**" and individually as "**Party**").

Hyxipower reserves the right to update and revise the terms of this Data Processor Agreement. The relevant notice shall be published on the official Hyxipower website. The new edition of Data Processor Agreement shall be in force after two weeks after the relevant announcement made if no objections from the Partner raised.

The Parties agree that the terms of this Data Processor Agreement and its Appendices supplement the Agreement. Under the Agreement, Hyxipower may be required to Process certain Personal Data of employees, customers or suppliers from Partner. This Data Processor Agreement sets out the terms and respective rights and obligations of the Parties in respect of such Processing of Personal Data.

IT IS AGREED AS FOLLOWS:

1. Definitions

1.1. In this Processor Agreement the capitalised terms below shall be assigned the following meanings:

Agreement	refers to the "Non-Exclusive Distribution Agreement" or or any other agreement entered between the Partner and Hyxipower and under which Hyxipower needs to process Personal Data and such agreement expressly incorporates by reference the terms of this Data Processor Agreement.
Affiliated Company	means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with either Party and is acting as controller jointly with the Partner or as subprocessor of Hyxipower (if applicable).
Controller	means the party which, acting alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

Hyxipower	refers to Zhejiang Hyxi Technology Co., Ltd. a company incorporated under the laws of the People's Republic of China, with its principle place of business located at the Room 216, Block A, Building 1, No. 57 Jiang'er Road, Changhe Street, Binjiang District, Hangzhou, Zhejiang,China or any other Hyxipower entity that concluded the Agreement with the Partner.
Data Subject	means an identified or identifiable natural person.
EEA	means the European Economic Area.
EU Model Contract	means standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Commission implementing decision 2021/914 of 4 June 2021), as up-dated or replaced from time to time;
Order	has the meaning assigned to that term in Article9.1of this Processor Agreement.
Partner	means the legal person/entity referred to as *Distributor* in the “Non-Exclusive Distribution Agreement” or under any other title indicated in the Agreement.
Personal Data	means any information relating to a Data Subject.
Process or Processing	means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Processor Agreement	means this data processor agreement between Partner and Hyxipower.
Processor	means the party which Processes Personal Data on behalf of the Controller.
Regulations	means all laws and regulations applicable to the Processing of Personal Data, including, but not limited to, the General Data Protection Regulation (“**GDPR**”) and

	other applicable statutory laws and regulations related to data protection, and, to the extent applicable, any implementation act, or any privacy or telecommunications act provided by the Applicable Law.
Security Breach	has the meaning assigned to that term in Article6.3of this Processor Agreement.
Sensitive Data	means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data and biometric data Processed for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation or any Personal Data qualifying as such under applicable Regulations.
Subprocessor	means a subcontractor or affiliate engaged by Hyxipower who has, or may have, access to Personal Data.
Hyxipower Employee	means any person employed or hired by Hyxipower involved with the performance of this Processor Agreement.
Supervisory Authority	means one (or more) independent public authority(ies) which is (are) established in the jurisdiction of the Processor or the Controller pursuant to Regulations or which is (are) competent for the protection of the fundamentals rights and freedom of natural persons in relation to processing of personal data under applicable law.
Transfer	has the meaning assigned to that term in Article8.1of this Processor Agreement.

1.2. The Parties agree that in the event of a conflict between this Processor Agreement and the Agreement, the terms of this Processor Agreement shall prevail.

2. Processing of Personal Data

2.1. Hyxipower shall perform its activities pursuant to the Agreement, acting as Processor on behalf of Partner. Partner shall remain the Controller for all Personal Data which is Processed under the Agreement. The types of Personal Data, categories of Data Subjects and the purposes of the Processing by

Hyxipower are described in **Appendix 1** (Personal Data and Processing activities) and are further detailed in the Agreement.

3. Obligations of Partner

3.1. As Controller, Partner shall comply with its obligations under applicable Regulations and this Processor Agreement.

3.2. Partner shall instruct Hyxipower to Process the Personal Data on Partner's behalf and in accordance with applicable Regulations. The Processing instructions of Partner are documented in **Appendix 1** (Personal Data and Processing activities) and are further detailed in the Agreement.

3.3. Partner may act as Controller jointly with its Affiliated Companies. In such case, the Partner shall inform the Hyxipower accordingly and give the relevant details of the Affiliated Companies to Hyxipower.

3.4. Partner may issue additional instructions with regard to Hyxipower's Processing activities, or amend such instructions, if necessary at the Partner's sole discretion, provided that such instructions are consistent with the terms of the Agreement and this Processor Agreement, reasonable and in accordance with applicable Regulations. Partner shall issue any such additional or amended instructions in writing or by electronic mail [(receipt verified)] to Hyxipower. Partner shall (a) grant Hyxipower a reasonable amount of time to implement or comply with any additional or amended instructions and (b) upon request, reasonably cooperate with Hyxipower to implement or comply with such additional or amended instructions.

4. Obligations of Hyxipower

4.1. As Processor, Hyxipower shall comply with its obligations under applicable Regulations and this Processor Agreement.

4.2. Hyxipower shall ensure that it and each of its Employees (a) only Processes Personal Data on behalf of Partner and in accordance with Partner's instructions; (b) refrains from Processing the Personal Data for its own purposes or for purposes of third parties; and (c) Processes the Personal Data only in sofar as necessary to perform its activities under the Agreement; unless Hyxipower is required to do otherwise by applicable laws and regulations or EU or Member State law and it promptly notifies Partner thereof in accordance with Article 4.5.ii. Hyxipower shall document the instructions given by Partner.

4.3. During the term of this Processor Agreement, if Hyxipower receives any request from a Data Subject relating to his or her Personal Data, Hyxipower shall

promptly refer that Data Subject to Partner to submit his or her requests. Partner shall be responsible for responding to any such request. Hyxipower shall provide such assistance as Partner may reasonably specify to enable Partner to meet its obligations to respond to requests for exercising the rights of Data Subjects pursuant to applicable Regulations, including, but not limited, to requests from Data Subjects to access, correct or delete their Personal Data.

4.4. Hyxipower shall provide such assistance as Partner may reasonably specify to enable Partner to (a) carry out a data protection impact assessment and a possible subsequent prior consultation with a Supervisory Authority and (b) to respond to or defend against enquiries, requests or investigations from a Supervisory Authority.

4.5. Hyxipower shall promptly inform Partner in any of the following events if:

i. Hyxipower has any reason to believe that it cannot comply with this Processor Agreement;

ii. applicable laws and regulations or EU or Member State law prevents Hyxipower from fulfilling the instructions received from Partner, unless that law prohibits Hyxipower from providing such information on compelling grounds of public interest;

iii. Hyxipower or a Hyxipower Employee has acted in breach of this Processor Agreement or if a Subprocessor has acted in breach of the written agreement between Hyxipower and such Subprocessor; or

iv. Hyxipower has received a warning or a reprimand from a Supervisory Authority that the Processing activities are likely to infringe, or have infringed, applicable Regulations.

4.6. Upon termination of the Agreement or after the end of the provision of Processing services (whichever is earlier), Hyxipower and its Subprocessors (if any) shall, if directed by Partner, return all Personal Data to Partner and/or delete all copies of such Personal Data and notify Partner that it has done so, unless applicable laws and regulations or EU, Member State law prohibits Hyxipower from returning or deleting all or part of the Personal Data. With respect to any Personal Data that Hyxipower is unable to return or destroy following termination of the Agreement or after the end of the provision of Processing services (whichever is earlier), Hyxipower shall continue to protect such Personal Data in accordance with the terms of the Agreement and this Processor Agreement and shall not actively Process the Personal Data.

5. Subprocessors

5.1. With the signing of this Agreement, Partner acknowledges that and gives consent to Hyxipower to subcontract or assign any of its obligations under the Agreement to a Subprocessor, to the extent that the Subprocessor is an

Affiliated Company of Hyxipower. Should Hyxipower wish to engage a non-Affiliated Company as Subprocessor, Partner's prior written consent shall be needed, and Partner may not unreasonably withhold or delay such consent. Partner may attach reasonable conditions to its consent. The Subprocessors listed in **Appendix 3** (Approved Subprocessors) are hereby approved for the areas of work specified therein.

5.2. Hyxipower may only engage a Subprocessor by way of a written agreement with such Subprocessor which imposes at least the same obligations on the Subprocessor as are imposed on Hyxipower under this Processor Agreement.

5.3. Hyxipower shall prohibit the Subprocessor from accessing or using Personal Data for any purpose not related to the performance of its assigned activities under the Agreement.

5.4. Hyxipower shall remain responsible for its compliance with its obligations under the Agreement and this Processor Agreement. Hyxipower shall not be liable for damages and claims to the extent that such damages or claims arise from Partner's instructions to Hyxipower or its Subprocessors.

6. Security and Security Breaches

6.1. Hyxipower shall implement appropriate administrative, organisational, physical and technical safeguards to protect the confidentiality, integrity and availability of the Personal Data consistent with applicable Regulations, including, without limitation, to protect the Personal Data against destruction, loss, unauthorised disclosure or access, or any other form of unlawful processing. To clarify, Hyxipower shall consider the state of the art and implementation costs when considering the appropriateness of such administrative, organisational, physical and technical safeguards, and ensure that such measures offer an appropriate level of security given the risks associated with Processing and the nature of the Personal Data to be protected.

6.2. Hyxipower shall implement and maintain in any event adequate Security Measures **(Appendix 2)**. Hyxipower may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in any degradation of the level of security.

6.3. Hyxipower shall, without undue delay and, where feasible, but no later than thirty-six (36) hours after discovery, notify Partner of any actual or reasonably suspected (i) accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed; or (ii) a breach of the security measures as referred to in this Article 6 (a "**Security Breach**"). Hyxipower shall also notify Partner if a Security Breach takes place at a Subprocessor. Hyxipower shall maintain procedures aimed at detecting, responding

to and recovering from Security Breaches.

6.4. The notification shall at least:

a. describe the nature of the Security Breach, including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
b. describe whether the Personal Data are encrypted, anonymised or otherwise made incomprehensible;
c. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
d. describe the likely consequences of the Security Breach; and
e. describe the measures that Hyxipower has taken, or proposes taking, to address the Security Breach, including, where appropriate, measures to mitigate its possible adverse effects.

6.5. At Partner's written request, Hyxipower shall provide all reasonable cooperation to handling the Security Breach, such as informing Supervisory Authorities and Data Subjects (if required); provided, however, that Partner will bear the cost of any such notifications.

7. Compliance

7.1. At Partner's request, Hyxipower shall provide Partner with information about Hyxipower's Processing activities under the Agreement necessary to enable Partner to verify Hyxipower's compliance with the provisions of this Processor Agreement.

8. Transfer of Personal Data outside the EEA

8.1. The Parties acknowledge that the GDPR and/or its statutory requirements contain restrictions on transferring Personal Data from the EU Member State where the Parties are situated or another EU Member State to countries or organisations outside the EEA which do not ensure an adequate level of protection, which includes making such Personal Data accessible from any such country or organisation ("**Transfer**").

8.2. Hyxipower shall not Transfer Personal Data other than (a) as explicitly mentioned in the Standard Contractual Clauses (Appendix 4) attached herein or otherwise authorised under the Agreement or (b) with the specific prior written consent of Partner, unless it is required to do so by EU law or Member State law to which it is subject to and it promptly informs Partner thereof in accordance with Article 4.5.ii.

8.3. Subject to Article 8.1, Hyxipower shall ensure that any Transfers shall only occur on the basis of a legally recognised transfer mechanism, such as an EU Model Contract or binding corporate rules.

9. Inspection Requests

9.1. If Hyxipower or a Subprocessor receives a request or order from a Supervisory Authority to provide access to Personal Data ("**Order**"), Hyxipower shall promptly notify Partner of that fact. When responding to or otherwise addressing the Order, Hyxipower shall provide full reasonably required cooperation.

9.2. If the Order prohibits Hyxipower from complying with such obligations, Hyxipower shall promote Partner's reasonable interests. To that end, in any event, Hyxipower shall:

a. perform a legal review to determine the extent to which (i) Hyxipower is required by law to comply with the request or Order; and (ii) Hyxipower is prohibited from complying with its obligations set out in this Article 9;

b. only cooperate with the Order if this is required by applicable law and, where possible, object (at law or otherwise) to the Order enjoining it from informing Partner in this respect or from following its instructions;

c. refrain from providing any more or any other Personal Data than is strictly necessary to comply with the Order;

d. if Personal Data are transferred to a non-EEA country: if reasonably possible, comply with the data transfer rules of the Regulations;

e. inform Partner promptly once this is permitted.

10. Term and Termination

10.1. This Processor Agreement constitutes an integral part of the Agreement and shall automatically terminate upon termination of the Agreement.

APPENDICES attached to this Processor Agreement:

APPENDIX 1 - PERSONAL DATA AND PROCESSING ACTIVITIES

APPENDIX 2 - SECURITY MEASURES

APPENDIX 3 - APPROVED SUBPROCESSORS

APPENDIX 4 - STANDARD CONTRACTUAL CLAUSES

Appendix 1 - Personal data and Processing activities

Categories of Data Subjects

Partner's employees or self-employed workers; Partner's customers; Partner's partners; and shareholders or directors of all the above.

Categories of Personal Data

Name, surname, email, email text, address, telephone number, fax, account details, transaction details, passport or ID copy (if need to apply for visa to China); IP address of equipment; S/N number

Sensitive Data (if appropriate)

Processing activities

Storing, recording, organisation, use, transmission, disclosure, collection for the needs of:

Billing and delivery of products; providing technical support and after sales services; providing repair services; providing training; assisting with procedures for visit to China

Appendix 2 - Security measures

- Encrypted passwords
- SSL encryption in databases with personal data
- Use of VPN
- Firewall and Antivirus
- Automatic lock screen function for desktops and laptops after a certain period of inactivity
- Establishment of Information Security Committee consisted by the managers of each department, presided by the Chief Director of IT Department and with the CEO of Zhejiang HyxiTechnology Co., Ltd as the consultant.
- Establishment of Information Security Department, which is responsible for monitoring the implementation of the information security policy by the employees in every department with the help of a contact person of each department.
- Implementation of different policies in accordance with the requirements of ISO27001.
- Dissemination of the policies through different means such as portal, forum, announcements in elevators, posters, e-learning platform, employees' exams.
- Access provided only for authorized employees; employee's number and access date appear as watermarks when employees access company's documents; use of RMS protection based on which unauthorized users cannot open carriers of the relevant information.
- Use of subcontractors we have signed NDA agreements with.
- We have a professional PSIRT team, which is responsible for receiving, disposing and publicly revealing security vulnerability related to products and services. Meanwhile, we have established perfect incident response system and formulated SLA (Service-Level-Agreement) for different customers according to their individual requirements
- Other organisation and technical measures

Appendix 3 - Approved Subprocessors

other Hyxipower entities;

providers of IT service

providers of products supplementary to Hyxipower products

forwarders or any delivery entities of Hyxipower products

entities cooperating with Hyxipower for assemble of products

Appendix 4

STANDARD CONTRACTUAL CLAUSES

European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679

This Appendix 4 applies to the transfer related to EU data subjects to third countries and includes 2 Modules:

- Module 2 of the Standard Contractual Clauses applicable to the transfer of Partner Personal Data, whereby Partner acts as data controller and Hyxipower acts as data processor; and
- Module 3 of the Standard Contractual Clauses is applicable to the transfer of Partner Personal Data, whereby Partner acts as a data processor and Hyxipower also acts as data processor.

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

[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 of 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 […].

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

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

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

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

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

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 - Optional

Docking clause

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

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

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

SECTION II - OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

MODULE TWO: Transfer controller to processor

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the

contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive

data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union [2] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9 Documentation and compliance

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

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

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

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

---

[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.

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

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer asset out in the contractor other legal act under Union or Member State law between the controller and the data exporter[3].

8.2 Purpose limitation

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

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter 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.

8.4 Accuracy

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

[3] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, 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. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importershall carryout regular checks to ensure that these measures continue to provide an appropriate level of security.

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

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

available and further information shall, as it becomes available, subsequently be provided without undue delay.

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importershall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[4] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9 Documentation and compliance

[4] 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 purposes of these Clauses.

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

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

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

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

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

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

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

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[5] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor

[5] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

MODULE THREE: Transfer processor to processor

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

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[6] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law

[6] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

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

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

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

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

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

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

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

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

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

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

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

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

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

Clause 13

Supervision

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

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application ofRegulation (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 ofRegulation (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 andpractices 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[7];

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

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

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

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not inline 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). [For Module Three: The data exporter shall forward the notification to the controller.]

---

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

(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 [for Module Three: , if appropriate in consultation with the controller]. 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 [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exportershall 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 notificationshall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

(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.). [For Module Three: The data exporter shall forward the information to the controller.]

(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 importershall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importershall 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 sounder the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

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

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

SECTION IV - FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] 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 importershall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of_____ (*specify Member State*).]

Clause 18

Choice of forum and jurisdiction

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

(b) The Parties agree that those shall be the courts of the Member State in which the data exporter is established .

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

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

APPENDIX

ANNEX I (applicable to MODULE TWO and MODULE THREE)

A. LIST OF PARTIES

Data exporter(s):

1. Partner as data exporter (MODULE 2)

Name: Partner, as defined in the Agreement

Address: Patner, as defined in the Agreement

Contact person's name, position and contact details: Partner's contact person, as defined in the Agreement

Activities relevant to the data transferred under these Clauses: Services as described in the Agreement

Role (controller/processor): Controller

2. Partner as data exporter (MODULE 3)

Name: Partner, as defined in the Agreement

Address: Patner, as defined in the Agreement

Contact person's name, position and contact details: Partner's contact person, as defined in the Agreement

Activities relevant to the data transferred under these Clauses: Services as described in the Agreement

Role (controller/processor): Processor

Data importer(s):

1. Name: Zhejiang Hyxi Technology Co., Ltd.

Address: Room 216, Block A, Building 1, No. 57 Jiang'er Road, Changhe Street, Binjiang District, Hangzhou, Zhejiang, P.R. China

Contact person's name, position and contact details: Data Protetion Officer, psd-service@hyxipower.com

Activities relevant to the data transferred under these Clauses: Services as described in the Agreement

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

See Appendix 1 ("Personal Data and Processing activities") of the Processor Agreement.

Categories of personal data transferred

See Appendix 1 ("Personal Data and Processing activities") of the Processor Agreement.

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

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

Transfer is made on Continuaous basis

Nature of the processing

All kind of processing as defined in article 4(2) of the GDPR, meaning any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Purpose(s) of the data transfer and further processing

Transfer and processing of Personal Data by Data Importer for the provision of Services in accordance with Appendix 1 (Personal Data and Processing activities) and are further detailed in the Agreement.

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

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

See Appendix 3 ("Approved Subprocessors") of the Data Processing Agreement.

Processing will take place during the provision of the services and products as defined in the Data Processing Agreement and are further detailed in the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

Supervisory Authorities shall be one (or more) independent public authority(ies) which is (are) established in the jurisdiction of the Member State the data exporter established and located, as defined in the Agreement.

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

Technical and organisation measures including technical and organisational measures to ensure the security of the data are detailed in Appendix 2 (Security Measures) of the Processor Agreement.

ANNEX III - LIST OF SUB-PROCESSORS

The controller has authorised the use of the sub-processors as defined in Appendix 3 (Approved Subprocessors)