EVERYDAY IT SUPERHEROES

Sub-processor Agreement

IT RELATION PHILIPPINES INC.

IT RELATION PHILIPPINES INC.

2nd Floor GM Bldg.
North National Highway,
Brgy Daro,
Dumaguete City,
Negros Oriental,
Philippines 6200
Company. reg. no..: 739-283-935-000
(Hereinafter “ITR-Philippines”)

and

IT Relation A/S

Dalgas Plads 7b, 1
7400 Herning
Company. reg. no.: 27 00 10 92
(Hereinafter “ITR”)

The parties are separately referred to as "Party" and jointly as "Parties".

1. BACKGROUND OF THE DATA PROCESSING AGREEMENT

1.1 ITR-Philippines delivers a number of IT-services to ITR, as described in more detail in the Parties' separate agreement(s) (the "Master Agreement"). Such services are delivered as part of one of the following situations:

a) ITR provides services to ITR's own customers (the "Customer"). For the provision of such services, ITR acts as a processor itself and is processing personal data on behalf of the Customer. In this connection ITR has engaged ITR-Philippines to assist as a sub-processor in providing services to the Customer in accordance to the respective governing main contract between ITR and the Customer.

1.2 This Data Processing Agreement specifies the Parties' obligations with regard to Art. 28 of the General Data Protection Regulation. It shall apply to all activities where ITR-Philippines processes personal data on behalf of ITR either as a sub-processor.

2. TERMS OF DATA PROCESSING

2.1 ITR-Philippines's processing of personal data on behalf of ITR will take place in accordance with the Data Processing Agreement.

2.2 The Data Processing Agreement and the Master Agreement shall be interdependent and cannot be terminated separately. The Data Processing Agreement may however – without termination of the Master Agreement – be replaced by an alternative valid data processing agreement, cf. clause 12.

2.3 This Data Processing Agreement shall take precedence over any corresponding provisions contained in the Master Agreement.

2.4 Three appendixes are attached to the Data Processing Agreement. The Appendixes form an integral part of the Data Processing Agreement.

2.5 Appendix 1 of the Data Processing Agreement contains details about the processing as well as the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

2.6 Appendix 2 of the Data Processing Agreement contains instructions on the processing that ITR-Philippines is to perform on behalf of ITR (the subject of the processing). Appendix 2 also contains a description of ITR-Philippines's technical and organizational measures as well as physical security.

2.1 Appendix 3 of the Data Processing Agreement contains the Standard Contractual Clauses entered into between ITR-Philippines and ITR..

2.2 The Data Processing Agreement and its associated Appendixes shall be retained in writing as well as electronically by both Parties.

2.3 This Data Processing Agreement shall not exempt ITR-Philippines or ITR from obligations to which the Parties are subject pursuant to the General Data Protection Regulation or any other legislation.

3. ITR-PHILIPPINES ACTS ACCORDING TO INSTRUCTIONS FROM THE ITR

3.1 ITR-Philippines as data processor shall solely be permitted to process personal data on documented instructions from ITR unless processing is required under EU or Member State law to which ITR-Philippines is subject; in this case, ITR-Philippines shall inform ITR of this legal requirement prior to the processing unless that law prohibits such information on important grounds of public interest, cf. General Data Protection Regulation, Article 28, sub-section 3, para a.

3.2 ITR-Philippines shall immediately inform ITR if instructions in the opinion of ITR-Philippines infringes the General Data Protection Regulation or data protection provisions contained in other EU or Member State law.

4. CONFIDENTIALITY

4.1 ITR-Philippines shall ensure that only those persons who are currently authorised to process personal data are able to access the personal data being processed on behalf of ITR. Access to the data shall therefore without delay be denied if such authorisation is removed or expires.

4.2 Only persons who require access to the personal data in order to fulfil ITR-Philippines obligations to ITR shall be provided with authorisation.

4.3 ITR-Philippines shall ensure that persons authorised to process personal data on behalf of ITR have undertaken to observe confidentiality or are subject to suitable statutory obligation of confidentiality.

4.4 ITR-Philippines shall at the request of ITR be able to demonstrate that the employees concerned are subject to the above confidentiality.

5. SECURITY OF PROCESSING

5.1 ITR-Philippines shall initiate all measures required pursuant to Article 32 of the General Data Protection Regulation, to secure personal data against accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to personal data against the law. ITR-Philippines shall determine the measures taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity to the rights and freedoms of natural persons.

5.2 The obligation to implement security measures means that ITR-Philippines shall perform a risk assessment in relation to the nature of the processing and thereafter implement measures to counter the identified risk. This may include, inter alia, as agreed in the Master Agreement or in Appendix 2, the following measures:

a) Pseudonymisation and encryption of personal data.

b) The ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services.

c) The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

d) A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

5.3 As of the time of entering into this Data Processing Agreement, the obligation for ITR-Philippines to implement security measures means that ITR-Philippines shall implement and maintain the level of security specified in Appendix 3 and implement the specially agreed security measures that may be specified in the Data Processing Agreement or in the Master Agreement.

6. USE OF SUB-PROCESSORS

6.1 ITR-Philippine shall not engage another processor (sub-processor) without prior specific written authorization from ITR.

6.2 If ITR-Philippines engage another sub-processor, after specific instruction from ITR, ITR-Philippines shall ensure that the sub-processor, used for the data processing on behalf of ITR, is subject to the same data protection obligations as those specified in this Data Processing Agreement on the basis of a contract or other legal document under EU law or the national law of the Member States, in particular providing the necessary guarantees that the Sub-Processor will implement the appropriate technical and organisational measures in such a way that the processing meets the requirements of the General Data Protection Regulation.

6.3 A copy of such a sub-processor agreement and subsequent amendments shall be made available to ITR on request.

6.4 If the Sub-Processor does not fulfil his data protection obligations, ITR-Philippines shall remain fully liable to ITR as regards the fulfilment of the obligations of the Sub-Processor.

7. TRANSFER OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

7.1 The use of ITR-Philippines for the processing of personal data on behalf of ITR will result in a transfer of personal data to Philippines (a third country), even though the data does not leave EU/EEA or is stored at the ITR-Philippines.

7.2 This transfer will take place within the framework of the General Data Protection Regulation/Regulation (EU) 2016/679.

7.3 For the evidence of doubt, all personal data are stored on servers within EU/EEA. ITR-Philippines works solely through a secured Citrix or similar service located in data centres within EU/EEA and will only get access to the personal data through this. No personal data will leave the EU/EEA borders in connection with the work that ITR-Philippines performs on behalf of ITR, and data will not be stored at or physically transferred to the ITR-Philippines.

7.4 The transfer of personal data to ITR-Philippines is based on the EU Commission's standard contractual clauses (2021/914) (the "Standard Contractual Clauses") attached as Appendix 3. The Standard Contractual Clauses are concluded between ITR as the data processor and ITR-Philippines as the sub-processor.

7.5 In case of conflict between the Data Processing Agreement and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

7.6 Beside from the above described transfer, ITR-Philippines shall solely be permitted to transfer (assignment, disclosure and internal use of) personal data to a third country or international organisation according to documented instructions from ITR.

7.7 However, ITR-Philippines may, exceptionally and without documented instruction from ITR, transfer personal data when required under EU or Member State law to which ITR-Philippines is subject; in such a case, ITR-Philippines shall inform ITR of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest, cf. Article 28, sub-section 3, para a.Without the instructions or approval of ITR, ITR-Philippines therefore cannot – within the framework of this Data Processing Agreement:

a) disclose personal data to a data controller in a third country or in an international organisation.

b) assign the processing of personal data to a sub-processor in a third country.

8. ITR-PHILIPPINES'S ASSISTANCE TO ITR

8.1 ITR-Philippines shall, taking into account the nature of the processing, as far as possible, assist ITR with appropriate technical and organisational measures, in the fulfilment of ITR's obligations to respond to requests for the exercise of the data subjects' rights pursuant to Chapter 3 of the General Data Protection Regulation.

8.2 On ITR's request, ITR-Philippines shall assist ITR in ensuring compliance with ITR's obligations pursuant to Articles 32-36 of the General Data Protection Regulation taking into account the nature of the processing and the data made available to ITR-Philippines.

9. NOTIFICATION OF PERSONAL DATA BREACH

9.1 ITR-Philippines shall notify ITR without undue delay after becoming aware of a personal data breach, at ITR-Philippines or any sub-processor, having effect to the personal data processed by ITR-Philippines on behalf of ITR.

9.2 ITR-Philippines shall – taking into account the nature of the processing and the data available to ITR-Philippines – on request from ITR, assist ITR in the reporting of the breach to the supervisory authority.

9.3 This may mean that ITR-Philippines is required to assist in obtaining the information listed below which, pursuant to Article 33, sub-section 3, of the General Data Protection Regulation, shall be stated in the report to the supervisory authority:

a) The nature of the personal data breach, including, if possible, the categories and the approximate number of affected data subjects and the categories and the approximate number of affected personal data records.

b) Probable consequences of a personal data breach.

c) Measures which have been taken or are proposed to manage the personal data breach, including, if applicable, measures to limit its possible damage.

9.4 If it is not possible for ITR-Philippines to provide the information in aggregate, the information may be communicated stepwise without undue delay.

10. ERASURE AND RETURN OF DATA

10.1 On termination of one or more of the services relating to ITR-Philippines's processing of personal data on behalf of ITR or when instructed by ITR, ITR-Philippines shall be under obligation, at the ITR's discretion, to erase or return any and all personal data related to such services and to erase existing copies unless EU law or Member State law requires storage of the personal data.

11. INSPECTION AND AUDIT

11.1 ITR-Philippines shall, on the request from ITR, make available to ITR all information necessary to demonstrate compliance with Article 28 of the General Data Protection Regulation and this Data Processing Agreement, and allow for and contribute to audits, including inspections performed by ITR or its Customer or another auditor mandated by ITR or its Customer.

11.2 ITR-Philippines shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to ITR's and ITR-Philippines's facilities, or representatives acting on behalf of such supervisory authorities, with access to ITR-Philippines's physical facilities on presentation of appropriate identification.

11.3 ITR determines the process and procedures for any such inspections and audit.

12. CHANGES TO THE DATA PROCESSING AGREEMENT OR THE PROCESSING

12.1 Changes to the Data Processing Agreement, including the instructions, shall be agreed in writing between the Parties.

12.2 Both Parties shall also be entitled to require a renegotiation of this Data Processing Agreement if changes to the law or inexpediency of the provisions contained herein should give rise to such renegotiation.

13. TERM AND TERMINATION

13.1 This Data Processing Agreement shall become effective on the date of both Parties' signature of the Agreement.

13.2 The Data Processing Agreement shall remine in force until it is either replaced by another data processing agreement between the Parties in accordance with clause 12 or until the processing activities under the Master Agreement have ceased and ITR's personal data has been erased and, if necessary, returned to ITR in accordance with the terms of the Data Processing Agreement.

14. SIGNATURES

For ITR

Date: 02-05-2022

Bo Duholm Hansen, Compliance Manager

Name, position

Bo

Signature

For ITR-Philippines

Date: 03-05-2022

Roderick B. Kinilitan, Country Manager

Name, position

Signature

APPENDIX 1 – INFORMATION ABOUT THE PROCESSING

1. PURPOSE

The purpose of ITR-Philippines's processing of personal data on behalf of ITR is:

ITR-Philippines providing different services to ITR as further specified below and in the Master Agreement.

2. NATURE OF THE PROCESSING

ITR-Philippines performs the following processing activities on behalf of ITR:

- Service Desk
  - Support in English
- Cloud Operation
  - NOC Centre 24/7/365 monitoring, alarm handling, trend analysis of services such as: OS, network, storage, backup, patch, applications, performance etc.
  - OS image and software package builds.
  - Build and manage automatic services.
  - Remote operations on central infrastructure services.
  - Incident processing.
  - Installation tasks.
- Solving specific tasks for ITR or ITR's Customer
  - Development tasks on Microsoft SharePoint and Microsoft CRM.
- Administrative tasks
  - License and SPLA management.

3. TYPES OF PERSONAL DATA

The processing may include the following types of personal data about data subjects:

General personal data (see Article 6 of the General Data Protection Regulation):
☒ General personal information

Sensitive personal information (see Article 9 of the General Data Protection Regulation):
☒ Racial or ethnic background
☒ Political conviction
☒ Religious conviction
☒ Philosophical conviction
☒ Professional Association
☒ Health conditions, including drug abuse, drugs, alcohol, etc.
☒ Sexual relationships

Information about individuals' private affairs (see Article 6 and 9 of the General Data Protection Regulation):
☒ Offenses
☒ Significant social problems
☒ Other purely private matters not mentioned above:

Other private matters not mentioned above

☒Other private matters

Information on CPR number (see Article 87 of the General Data Protection Regulation):
☒CPR number

4. CATEGORIES OF DATA SUBJECTS

The processing includes the following categories of data subjects:
Categories of registered, identified or identifiable physical persons that the ITR-Philippines's processing deals with:
☒ Employees at ITR or the Customer
☒ Children
☒ ITR's Customer
☒ ITR's Customer's own customers
☒ Other categories as specified.

APPENDIX 2 – INSTRUCTION FOR THE PROCESSING OF PERSONAL DATA

1. THE SUBJECT OF/INSTRUCTION FOR THE PROCESSING

ITR-Philippines's processing of personal data on behalf of ITR shall be carried out in connection to ITR-Philippines performing of the following tasks:

- Service Desk
- Cloud Operation
- Solving specific tasks for ITR or ITR's Customer
- Administrative tasks

2. STORAGE PERIOD/ERASURE PROCEDURES

Personal data are stored on servers within EU/EEA. ITR-Philippines works solely through a secured Citrix or similar service located in data centres within EU/EEA and will only get access to the personal data through this.

No personal data will leave the EU/EEA borders in connection with the work that ITR-Philippines performs on behalf of ITR, and data will not be stored at or transferred to the ITR-Philippines.

3. SECURITY LEVEL AND MEASURES

ITR-Philippines carries out security measures consistent to the security measures implement at ITR.

ITR-Philippines is subject to IT Relations security policies and procedures. Thus, ITR-Philippines is not permitted and not able to remove, take out or copy personal data from ITR's IT-systems. All personal data is only - and must at any time - stored on servers within EU/EEA.

In case ITR-Philippines is required under the Philippines law to transfer personal data to the Philippines authorities, ITR will within the limits of EU or Member State law seek to prevent such transfer.

APPENDIX 3 – TRANSFER BASIS FOR PROCESSING PERSONAL DATA TO ITR-PHILIPPINES

STANDARD CONTRACTUAL CLAUSES[1]

Processor to 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)[2] 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.

[1] This document was generated based on the text available at:
https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc12-L_2021199EN.01003701-E0012

[2] 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.

(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(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);
(iii) Clause 9(a), (c), (d) and (e);
(iv) 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 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.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

(a) The data exporter 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 as set out in the contract or 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.

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

[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.

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 importer shall carry out 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 importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall 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 importer shall 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

(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.

[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.

(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

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 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.[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 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.

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

(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.

Clause 10

Data subject rights

(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 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) 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 subject shall 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/their responsibility 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) 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.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

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

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

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

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

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

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

(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, 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 the controller or 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.

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.). 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.

(f) In case ITR-Philippines is required under the Philippines law to transfer personal data to the Philippines authorities, ITR will within the limits of EU or Member State law seek to prevent such transfer.

15.2 Review of legality and data minimization

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

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

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 Denmark.

(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

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: IT Relation A/S

Address: Dalgas Pl. 7B, 1. Sal, 7400 Herning

Contact person's name, position and contact details:

Compliance and Security
compliance@itm8.com
+ 45 70 26 29 88

Activities relevant to the data transferred under these Clauses: The data controller, ITR's Customers, determine the subject-matter of the processing. In order to deliver the services to the data controller in accordance with the DPA, ITR uses ITR-Philippines as a sub-processor and exports personal data to ITR-Philippines. The processing activities carried out by ITR-Philippines are the following: delivery of cloud operation, solving of specific tasks and delivery of a Service Desk.

Signature and date:

02-05-2022

Role (controller/processor): Processor

Data importer(s):

Name: IT Relation Philippines Inc.

Address: 2nd Floor GM Bldg., North National Highway, Brgy Daro, Dumaguete City, Negros Oriental, Philippines 6200

Contact person's name, position and contact details:

Country Manager

Roderick B. Kinilitan

rokin@itrelation.dk

+63 9171253909

Activities relevant to the data transferred under these Clauses: The processing activities carried out by ITR-Philippines are the following: delivery of cloud operation, solving of specific tasks and delivery of a Service Desk.

Signature and date:

03-05-2022

____

Role (controller/processor): Sub-processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

Please refer to the categories of data subjects as set in in Appendix 1 of the DPA.

Categories of personal data transferred

Please refer to the categories of personal data as set in in Appendix 1 of the DPA.

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.

Please refer to the categories of personal data and the list of Philippines's technical and organizational measures set in in Appendix 1 and 2 of the DPA.

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

Continuous.

Nature of the processing

Please refer to the nature of the processing as set in in Appendix 1 of the DPA.

Purpose(s) of the data transfer and further processing

Please refer to the purpose as set in in Appendix 1 of the DPA.

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

Please refer to the storage period/erasure procedures as set in in Appendix 2 of the DPA.

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

Please refer to the list of sub-processors as set in in Appendix 3, annex 3, of the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
Denmark
Phone: + 45 33 19 32 00
dt@datatilsynet.dk

ANNEX II

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

EXPLANATORY NOTE:
Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Please refer to the description of IT Relation Philippines's technical and organizational measures as well as physical security as set in in appendix 2.

ANNEX III

LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

ITR-Philippine shall not engage another processor (sub-processor) without prior specific written authorization from ITR.