DATA PROCESSING AGREEMENT
Zyxel Nebula Cloud-Management Platform

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

Between Zyxel Network Corp., No.2 Industry East RD. IX, Hsinchu Science Park, Hsinchu 30076, Taiwan, R.O.C (the data processor) and the Nebula customer (the data controller)

each a 'party'; together 'the parties'

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

The Clauses constitutes an agreement between Zyxel Communications Corp. as the data processor for the Nebula customer. The Nebula customer can act as a data controller or as a data processor (depending on the individual Nebula customer situation). If the Nebula customer acts as a data processor, ZyXEL will have the role of a sub-processor.

How to execute the Clauses:
The Clauses have been pre-signed on behalf of Zyxel. The DPA including SCC constitutes part of the agreement between ZyXEL Communication Corp. and the Nebula Customer.

1. Table of Contents

2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation or the GDPR).

3. In the context of the provision of https://bulletin.nebula.zyxel.com/data-policies/NCC_TermsOfUse_20180731.en-us.html] or https://www.zyxel.com/de/de/Terms-of-Use.shtml, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

9. Appendix D contains Standard Contractual Clauses as a transfer tool for the transfer of data from the data controller to the data processor in a third country, cf. Article 46 of the GDPR.

10. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the GDPR or other legislation.

3. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

   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.

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

   If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

   The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

3. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

   The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

4. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

5. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the

sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

    a. transfer personal data to a data controller or a data processor in a third country or in an international organization

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

    c. have the personal data processed in by the data processor in a third country

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

    This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

    a. the right to be informed when collecting personal data from the data subject
    b. the right to be informed when personal data have not been obtained from the data subject
    c. the right of access by the data subject
    d. the right to rectification
    e. the right to erasure ('the right to be forgotten')
    f. the right to restriction of processing
    g. notification obligation regarding rectification or erasure of personal data or restriction of processing

h. the right to data portability
i. the right to object
j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

    a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

    b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

    c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

    d. the data controller's obligation to consult the competent supervisory authority, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor's notification to the data controller shall, if possible, take place within 48 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

    a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

    b. the likely consequences of the personal data breach;

c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

13. The parties' agreement on other terms

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

1. The Clauses shall become effective on the date of the data controllers' acceptance of the Terms of Use, cf. Clause 2.3.

2. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

3. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

4. Signature

On behalf of the data processor

Name	Kell Lin
Position	VP, NSBU
Date	
Signature	2022/10/19

15. Data processor contact points

1. The parties shall be under obligation continuously to inform each other of changes.

2. The data controller may contact the data processor using the following contact points:

Name	Julian Wu
Position	AVP, ICC
Date	
Signature	2022/10/19

Appendix A Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

The principal purpose of the data processing is the provision of the Nebula Control Center initiated by the data controller when logging into the Nebula Control Center portal.

Personal data may be subject to the following basic processing activities:
(a) customer service activities, such as processing orders, providing technical support and improving products
(b) delivery of the Nebula Control Center monitoring capabilities and services through which the data controller manages and configures ZyXEL networking hardware devices.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):
All the ZyXEL networking hardware devices that are manageable through the Nebula Control Center are built with the capability to collect personal data from the network, sending it to the Nebula Control Center system for computing, formatting and storage. The data processing will be initiated by the data controller through deployment of the ZyXEL networking hardware devices and integrating them to the Nebula Control Center.

A.3. The processing includes the following types of personal data about data subjects:

The Nebula Control Center collects the personal data on behalf of the data controller, which may include the following categories and can be modified through the data controllers' controls (as defined below):

- Email of the data controller and other personnel managing the Nebula Control Center portal; used for authentication, maintenance notifications and marketing bulletins about the Nebula Control Center (always).
- The IP Addresses of data subjects, in order to provide monitoring and network statistics to the data controller (always).
- Client hostname of data subjects, for the ease of network monitoring to data controller (always, but can be manually edited).
- Account information of data subjects using Nebula Control Center cloud hosted authentication server; for network authentication, monitoring and control (based on data controllers' controls).
- Sign–on authentication username and/or email address of data subjects when using certain user authentication methods, including: active directory and radius servers; for network authentication, monitoring and control (based on data controllers' controls).
- Data Subject's email, age, gender, locale when Facebook social login (as described below) authentication is configured (based on data controller's controls).

  Social Login: By default, The Nebula Control Center uses a Facebook App ID that is owned by Zyxel to facilitate the implementation of the Facebook social login authentication. Nebula Control Center's default Facebook App ID will only allow Data Subjects of 16 years old or older. As part of the data controllers' controls provided by Nebula Control Center, the data controller can also specify a self-created Facebook App ID, which could include a different age restriction.

- Access destination and URL from a Data Subject's IP address by hitting firewall rules; for a network access control (based on Customer Controls).

The data controllers' controls:
The Nebula Control Center provides data controller with a number of controls including security features and functionalities that data controller may use to ensure the protection of personal data, deliver the corresponding statement of consent and regulate the scope of data processed as described above.

The data controller may use these controls as technical and organisational measures to assist it in connection with its obligations under the GDPR.

All personal data are data subject to Article 6 GDPR.

A.4. Processing includes the following categories of data subject:

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

For as long as the data controller uses the Nebula Control Center and until data is deleted according to the Clauses.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

NAME	LEGAL ENTITY	ADDRESS	DESCRIPTION OF PROCESSING	LOCATION OF PROCESSING
AWS	Amazon Web Services, Inc.		Cloud Service Provide	Ireland

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

The parties agree that the Clauses and the Nebula Terms of Use (including the provision of instructions via configuration tools and APIs made available by the data processor for the services) constitutes data controllers instructions regarding data processors processing of personal data. The data processor will process personal data only in accordance with these instructions.

C.2. Security of processing

The level of security shall take into account:

"That the processing involves a large volume of personal data which are subject to Article 6 GDPR on 'special categories of personal data' which is why a 'high' level of security should be established."

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

The data processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

Data processor will implement and maintain appropriate technical and organizational measures to protect data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, data transmitted, stored or otherwise processed.

Data in transit over public networks between data controller and data processor is encrypted by default. In addition to use pseudonymisation technique to store data, data processor also encrypts specific, critical data stored at rest.

Data processor employs principle of least privilege to control accesses to data. Role-based access controls are employed to ensure that access required for service operations is for an appropriate purpose and approved with management oversight.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

Data processor will promptly notify data controller if it receives a request from a data subject for access to, correction, restriction, portability, or deletion of such data subject's personal data. Except as required by law, data processor will not respond to any such data subject request without data controller's prior written consent. Taking into consideration the nature of the processing, data processor will assist data controller through reasonable and appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of data controllers' obligation to respond to a data subject request to the extent data processor is legally permitted to do so and the response to such data subject request is legally required. To the extent legally permitted and outside the ordinary course and cost of business, data controller is responsible for the costs associated with any such assistance provided by data processor.

Security breach incident:
Data processor will (a) notify data controller of a security incident without undue delay after becoming aware of the security incident, and (b) take reasonable steps to mitigate the effects and to minimise any damage resulting from the security incident.

A notification will be delivered to one or more of data controllers administrators by any means the data processor selects, including via e-mail. It is data controller's responsibility to ensure that data controller's administrators maintain accurate contact information and secure transmission at all times.

Assistance:
To assist data controller in relation to any personal data breach notifications data controller is required to make under the GDPR, data processor will include in the notification such information about the security incident as data processor is reasonable able to disclose to data controller, taking into account the nature of the services, the information available to data processor, and any restrictions on disclosing such information, such as confidentiality.

Unsuccessful security incidents:
Data controller agrees that
(1) an unsuccessful security incident will not be subject to notification by the data processor. An unsuccessful security incident is one that results in no unauthorised access to personal data or to any of data processors equipment or facilities storing personal data, and may include, without limitation pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorised access to traffic data that does not result in access beyond headers) or similar incidents; and
(2) data processors obligation to report or respond to a security incident under this clause is not and will not be construed as an acknowledgement by data processor of any fault or liability of data processor with respect to the security incident.

C.4. Storage period

"Personal data is stored after which the personal data is automatically erased by the data processor.

Upon termination of the provision of personal data processing services, the data processor shall either delete or return the personal data in accordance with Clause 11.1., unless the data controller – after the signature of the contract – has modified the data controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses."

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the addresses of data processor and sub-processors, cf. Appendix 1.

C.6. Instruction on the transfer of personal data to third countries

When signing up for the Nebula Control Center, data controller transfers personal data to a third country. The transfer tool is the Standard Contractual Clauses, cf. Appendix D, pursuant to GDPR Article 46.

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

"The data processor shall annually at THE DATA PROCESSOR'S/THE DATA CONTROLLER'S expense obtain an AUDITOR'S REPORT/INSPECTION REPORT from an independent third party concerning the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The parties have agreed that the following types of AUDITOR'S REPORT/INSPECTION REPORT may be used in compliance with the Clauses:

- *ISO 27001 certification, ISO 27017 certification and ISO 27018 certification or certifications or other documentation evidencing compliance with such alternative standards as are substantially equivalent to ISO 27001, ISO 27017 and ISO 27018; and*
- *The System and Organisation Controls (SOC) 1 Report, the System and Organisation Controls (SOC) 2 report, the System and Organisation Controls (SOC) 3 Report or reports or other documentation describing the controls implemented by data processor that replace or are substantially equivalent to the SOC 1, SOC 2 and SOC 3.*

The AUDITOR'S REPORT/INSPECTION REPORT shall upon data controller's request without undue delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data controller or the data controller's representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the data controller deems it required."

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

"THE DATA PROCESSOR'S/THE DATA CONTROLLER'S expense obtain an AUDITOR'S REPORT/INSPECTION REPORT from an independent third party concerning the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The parties have agreed that the following types of AUDITOR'S REPORT/INSPECTION REPORT may be used in compliance with the Clauses:

The AUDITOR'S REPORT/INSPECTION REPORT shall without undue delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data processor or the data processor's representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the sub-processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the data processor (or the data controller) deems it required.

Documentation for such inspections shall without delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new inspection under a revised scope and/or different methodology."

If the Nebula customer acts as a data controller, the SCC in Appendix D.A. applies.

If the Nebula customer acts as a data processor towards own customers, the SCC in Appendix D.B. applies.

[the SCC including TIA should be included as Appendix D]

STANDARD CONTRACTUAL CLAUSES

Controller 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) ([i]) for the transfer of data to a third country.

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3

Third-party beneficiaries

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

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

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

(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.

Clause 7 – Optional

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 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 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 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 ([ii]) (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.

(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.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION 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 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. ([iii]) 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 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.

Clause 10

Data subject rights

(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.

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

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

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

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

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

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

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

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

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures

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

Clause 15

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

15.1 Notification

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

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

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

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

Clause 17

Governing law

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

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

Name: _____

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses:

_____

_____

Signature and date: _____

Role (controller/processor):

2. …

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

Name: _____

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses:

_____

_____

Signature and date: _____

Role (controller/processor):

2. …

ANNEX II

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

The technical and organizational measures described in the DPA are applicable.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

1. Name: …

   Address: …

   Contact person's name, position and contact details: …

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): …

2. …

ANNEX

STANDARD CONTRACTUAL CLAUSES

Processor to Sub-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

(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

[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 […].

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

(iii) Clause 9 - Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Clause 18(a) and (b);

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 - Optional

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 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[2].

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 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

[2] 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.

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[3] (in the same country as the data importer or

[3] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection

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.

(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

---

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)

GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list.

(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.[4] 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.

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.

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

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

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

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in

light of the specific circumstances of the transfer, and the applicable limitations and safeguards[5];

(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:

[5] 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.

(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.

15.2 Review of legality and data minimisation

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

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. 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 one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of 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

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): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

1. Name: …

Address: …

Contact person's name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): …

2. …

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

1. Name: …

Address: …

Contact person's name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): …

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

The technical and organizational measures described in the DPA are applicable.

The Data Importer has implemented and will maintain appropriate administrative, technical and physical safeguards to protect personal data.

1. Service Security

1.1 Architecture. Data Importer's Services are designed with multiple security layers to cover data transfer, encryption, network topology and application-level access control that are distributed across a scalable, secure infrastructure provided by the cloud service provider.

1.2 Relibaility. Data Importer's Services are designed to support high availability to be resillient against the server or software failures.

1.3 Network Security. The data transited over public network by default are protected by Transport Layer Security (TLS) standard. Firewalls are by default enabled to restrict access to all services unless they are designed to be open to the world.

2. Information Security

2.1 Poliies. Data Importer employes principle of least privledge to control the access, change, support and deletion of data and related infrastrucuture. The management of privledges is tracked systematically.

2.2 Change management. Data Importer ensures the security-related changes, includes open source software patches, have been tested and authroized prior to the deployment to the production environment.

2.3 Vulnerbility Scan. Data Importer employs a periodical scan conducted by a third-party. The third-party only scans the interfaces the customer will be using, not directly to the infrastatures that implements the services to avoid the privacy concerns.

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

1. Name: Amazon Web Services (AWS), Inc.

Address: The address for AWS specified in the agreement with data processor.

Contact person's name, position and contact details: The address for AWS specified in the agreement with data processor.

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): AWS is the cloud service provider to provide cloud services the data processor needs in order to process the data.

EU SCC Transfer Impact Assessment (TIA)

If necessary, attach documentation

for use under the EU General Data Protection Regulation (GDPR) and Swiss Data Protection Act (CH DPA), in particular for complying with the EU Standard Contractual Clauses (EU SCC)

Author: Julian Wu (https://nebula.zyxel.com/)

Draft 1.00 for public consultation (Nov. 3rd, 2021)

See the notes at the end for more information on the scope and legal basis of this document. Read them in particular if you are subject to **professional secrecy obligations**. Also consult the additional worksheets for more examples, infos and an illustration of the scenarios in which a TIA is necessary as per the EU SCC. The blue text is mere sample text; the values and reasoning do *not* necessarily represent the author's opinion and are given for illustration purposes only.

See TIA Scenarios and other worksheets

Step 1: Describe the intended transfer

a)	Data exporter[1] (or the sender in case of a relevant onward transfer):	Zyxel Networks Corporation – Worldwide Headquarters (Taiwan)	
b)	Country of data exporter:	TW (data at rest are in EU)	
c)	Data importer[2] (or the recipient in case of a relevant onward transfer):	Amazon AWS	
d)	Country of data importer:	US	
e)	Context and purpose of the transfer:	**By the request of US Government**	
f)	Categories of data subjects concerned:	User data, third parties included in user content	
g)	Categories of personal data transferred:	User content, user communications, usage data	
h)	Sensitive personal data:	None	
i)	Technical implementation of the transfer:	Within same data center	
j	Relevant onward transfer(s) of personal data (if any):[3]	None	→ perform separate TIA
k)	Countries of recipients of relevant onward transfer(s):	None	

Step 2: Define the TIA parameters

				Reasoning
a)	Starting date of the transfer:	1-十一月-16		
b)	Assessment period in years:	10		*Once we approach the end of the period or the legal situation changes , we will re-assesss the situation.*
	Ending date of the assessment based on the above:	1-十一月-26		
c)	At which point is the probability of lawful access so low that we have no reason to believe that it will happen during our assessment period? This is the case if the probability is so low that number of additional years it would take for the chance to increase to "50:50" is:	30	(= in total 40 years)	*We believe that if the probability of a prohibited lawful access to happen is so low that even after an additional 30 years in a row the chance of a prohibited lawful access occurring is still only at 50:50, it is of mere theoretical nature in a five year period which we are looking at here.*
	Probability permitted based on the above:	15.91%		
d)	Target jurisdiction for which the TIA is made:	US		(if there are additional jurisdictions, perform a separate TIA)
e)	Relevant local laws taken into consideration:	FISA Section 702		
f)	In how many cases will authorities in the target jurisdiction comply with their laws when pursuing lawful access even if not challenged?	50%		*This value is not relevant in our case. We have left it unchanged.*

Step 3: Define the safeguards in place

				Reasoning
a)	Would it be feasible, from a practical, technical and economical point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead?	No		
b)	Is the personal data transferred under one of the exemptions pursuant to applicable data protection law (e.g., Art. 49 GDPR in case of the GDPR)?	Yes	*YES?*	*We assume that US gov request is for public interest*
c)	Is the personal data at issue transmitted to the target jurisdiction in clear text (i.e. there is no encryption in-transit)?[4]	No	*Ensure that data remains encrypted*	*We assumt AWS infrastracture does support it*
d)	Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not encrypted or access to the keys to decrypt is possible)?	Yes	*Foreign lawful access is at least technically possible*	*The recipient needs access to the data in clear text in order to be able to process it. Encryption is not possible.*
e)	Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Standard Contractual Clauses in case of the GDPR, approved BCR, or - in the case of an onward transfer - a back-to-back-contract in line with the EU SCC), and can you expect compliance with it, insofar permitted by the target jurisdiction?	Yes	*Ensure that the mechanism remains in place and is complied with*	*We assume that AWS handle this*

Based on the answers given above, the transfer is: **permitted**

Step 4: Assess the risk of prohibited lawful access in the target jurisdiction[5]

*Country-specific! The following factors have been drafted for **US law**; amend as necessary for other jurisdictions.*

a) Assess the probability that during the assessment period, the following *legal arguments* will prevent the local authorities in the target jurisdiction from successfully forcing the data importer/recipient to disclose personal data at issue under the relevant local laws as identified in Step 2 above:[6]

	Probability†	Probability of possibility of a (successfull) request††	Reasoning

	The data importer/recipient is no "Electronic Communications Service Provider"[7] with regard to the processing of personal data at issue and, thus, out of scope of the relevant laws	100%	0.00%	
	The data importer/recipient has no possession, custody or control over the personal data at issue in clear text and can, thus, not be (successfully) ordered to provide or search it in clear text under the relevant laws[8]	10%	90.00%	
	The transfer of the personal data at issue or the content of the personal data will be considered communications to either a person located in the United States or a US person, which may not be "intentionally targeted" by the US authorities under the relevant laws, but such targeting would occur in the present case, and, thus, prevent such a request[9]	50%	50.00%	*The data are stored in AWS EU region, but AWS is a US company.*
	Performing a prohibited lawful access would violate the data exporter's or other applicable foreign law in a manner that is not permitted under the US law doctrine of international comity, which, thus, prevents such a request[10]	0%	100.00%	*Our data are stored in Ireland, the resulting violation of the GDPR would in our view not deter the US government from accessing it.*
	There are other legal grounds under US law that prevent a prohibited lawful access to occur in the present case	0%	100.00%	*n/a*
b)	Is the data importer/recipient contractually required to defend the personal data at issue against lawful access attempts?	Yes	100.00%	*This is a requirement under the EU SCC entered into with the data importer.*
c)	Probability that during the assessment period, the data is regarded as content that is the subject of lawful access requests at issue under the relevant local laws, based on past experience?[11] †††	5%	5.00%	*The data we have is rarely the subject of lawful access request.*
d)	Probability that during the assessment period, the data importer/recipient is technically able to on an ongoing basis search the data in plain text for selectors (i.e. search terms such certain recipients or senders of electronic communications) without the data exporter's permission as part of the lawful access requests at issue under the relevant local laws? †††	20%	20.00%	*The data are encrypted on rest and the system also implemented pseudomization thus the search in plain text is merely doable.*
f)	Are measures in place to find out if during the assessment period the circumstances taken into account in the above assessments are no longer valid?	Yes		*We are regularly monitoring the legal development in this area (and at least annually).*

Probability that legal arguments fail to prevent foreign lawful access: †††	0.00%	during the assessment period
Overall probability of a lawful access prohibited under applicable data protection laws:	0.00%	
In view of the TIA parameters, the residual risk of prohibited lawful access is:	acceptable	
Number of years it takes for a lawful access to occur at least once with a *90 percent* probability:	∞	
Number of years it takes for a lawful access to occur at least once with a *50 percent* probability:	∞	

... assuming that the probability neither increases nor decreases over time (like tossing a coin)

We have made the assessement in Step 4 on the following basis (e.g., internal legal analysis, outside legal advice, support by the data importer, legal research, public documentation, statistics): *With the help of experienced outside counsel and legal research, as indicated*

Final Step: Conclusion

In view of the above and the applicable data protection laws, the transfer is: **permitted**

Reassess at the latest by: 1-十一月-26
(or if there are any changes in circumstances)

This Transfer Impact Assessment has been made by:

Place, Date:

Signed:

By:

Note: Under the EU SCC, the TIA is to be adopted by both the data exporter and importer.

Scope of this TIA: This Transfer Impact Assessment should be used for assessing foreign lawful access risks *only for the purposes of European data protection law* , where foreign lawful access is not per se a problem, but only if it does not respect the essence of the fundamental rights and freedoms or exceeds what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of the GDPR. Accordingly, foreign lawful access requests that can be challenged before an independent and impartial court (in a European sense of the word) are permitted if they are regulated by law, are needed to safeguard the aforementioned objectives (such as prosecuting crimes), are undertaken in a proportionate manner and come with the possibility of the data subject getting legal redress. For instance, lawful access by way of the US CLOUD Act is in principle not an issue under European data protection law; in fact, it is in line with the Cybercrime Convention of the European Council. That said, there may be cross-border transfers of data where *any foreign lawful access is an issue* , for example, in where professional secrecy obligations apply. In such cases please use the spreadsheet "Cloud Computing: Risk Assessment of Lawful Access By Foreign Authorities" also from David Rosenthal, available at www.rosenthal.ch (https://bit.ly/2V9dj7V), which provides for a risk assessment also for these types of foreign lawful access. In turn, this TIA focuses on foreign lawful access where there is no possibility for recourse to an independent court, which is what has been the issue in the "Schrems II" decision by the European Court of Justice in its decision C-311/18 of July 16, 2020.

Legal Basis of this TIA: Art. 44 et seq. GDPR, Art. 6 Swiss Data Protection Act, Art. 16 et seq. revised Swiss Data Protection Act; Recommendation 01/2020 of the European Data Protection Board (Version 2.0 of June 18, 2021); Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of the European Commission (C(2021) 3972 final of June 4, 2021), Guide for checking the admissibility of data transfers with reference to foreign countries (Art. 6 para. 2 letter a FADP) of the Swiss Federal Data Protection and Information Commissioner dated June 18, 2021 (as amended on June 22, 2021).

† Example: If you believe that a particular legal argument will be found valid by three out of ten judges assessing the same case, the probability will be 30%. If you conclude that the argument is not valid, enter 0%. If you believe it will in any event be successful, put in 100%. If you don't know, put in 0%. Of course, nobody can predict the future, but this is also not necessary. For a TIA it is sufficient to undertake an diligent and professional predictive judgement following a proper protocol. To avoid noise and bias, we have already split up and structured the assessment in several independent parts. To further reduce noise and bias, ask several knowledgeable people to independently provide their assessment, then have them discuss their values, and then ask them to again provide their assessment. Use the average of the values each of them provided after the discussion (this referred to as the "Delphi" method).

†† In line of the recommendations of the EDPB, we do not assess whether the access will actually occur or not (because they are not interested in the company XY or their employees). We assess the (objective) *possibility* of it occuring. A 100% possibility means that we have to expect that a lawful access under the relevant laws will occur during the period, but it may still not happen because the relevant authorities do not believe it makes sense to order the data importer to produce the data at issue given their specific tasks, projects, etc. which we don't know about.

††† These values correspond to the values in C50, C52 and C51 of the "Cloud Computing: Risk Assessment of Lawful Access By Foreign Authorities" spreadsheet (available on www.rosenthal.ch)

[1)] The data exporter is the party being subject to the GDPR or Swiss DPA who exports personal data to a non-whitelisted third country (e.g., the US). It has the same meaning as in the EU Standard Contractual Clauses (SCC). The data exporter can be a controller, joint controller, processor or sub-processor. It is not relevant whether the data exporter is itself in Europe, a whitelisted country or a non-whitelisted country. It will always be required under the EU SCC and GDPR or Swiss DPA to perform a TIA. If the TIA is performed for the purpose of assessing a relevant onward transfer then the sender or originator of the relevant onward transfer is the "data exporter" for the purposes of this TIA.

[2)] The data importer is the party in a non-whitelisted country (e.g., the US) who receives personal data from a data exporter. The data importer can be a controller, joint controller, processor or sub-processor. It is the party with whom the data exporter will typically want to enter into the EU SCC (unless there are other grounds for the transfer). If the TIA is performed for the purpose of assessing a relevant onward transfer then the recipient of the relevant onward transfer is the "data importer" for the purposes of this TIA.

[3)] Relevant onward transfers of personal data are onward transfers of personal data by a data importer to another party in a non-whitelisted country. If this other party is a processor or sub-processor, even if the data exporter has no direct contractual relationship with it, a separate TIA has to be performed for such relevant onward transfer if the recipient is in a non-whitelisted country, because such relevant onward transfer can, as well, expose the personal data at issue to the risk of prohibited foreign lawful access. Since this TIA can be made for only one country and one recipient at a time, fill out and perform multiple TIAs for each recipient of a relevant onward transfer.

[4)] This is relevant for assessing the exposure to lawful interception of Internet backbones using selectors (upstream monitoring of communications).

[5)] In this section, the probability of a foreign authority accessing the personal data in clear text in a manner that does not respect the essence of the fundamental rights and freedoms or exceeds what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of the GDPR. The analysis only has to assess provisions of the target jurisdiction that grant public authorities access to the personal data at issue and fail to, in essence, satisfy any of the following four requirements: (1) Access is subject to the principle of legality, i.e. of clear, precise and accessible rules, (2) access is subject to the principle of proportionality, (3) there are effective means of legal redress for the data subjects to pursue their rights in the target jurisdiction in connection with an access to their personal data, and (4) any access is subject to legal recourse to an independent and impartial court (or other forms of independent recourse bodies). For example, in the US, access requests on the basis of Section 702 FISA (Foreign Intelligence Service Act) and EO 12.333 are considered *not* fulfilling in particular requirement (3) and (4). Hence, it has to verified how probable it is that there may be access requests on the basis of these two legal grounds. If the probability is so low that the exporter has "no reason to believe" that such access will occur, the transfer is permitted as per the SCC, the GDPR and the CH DPA, even though the SCC or BCR as such would not provide protection against such requests. The analysis in this section shall be based on the law applicable in the target jurisdiction and the way how it is applied by authorities and courts (including court decisions). The analysis may require obtaining a legal opinion or other forms of legal advice from counsel.

[6)] Consider all documented information on applicable legislation, case law, practices of authorities and past experience (including of the data importer, where available). You may want to ask the data importer the necessary questions (Clause 14(c) actually requires the data importer to provide "relevant information"). On this topic, see, for the EDPB recommendations 01/2020 on supplementary measures (version 2.0 adopted on May 18, 2021, available at https://bit.ly/3rSv07O), the FAQ for company of NOYB (including forms to be sent to US providers, available at https://bit.ly/2Vozeb7), the Swiss Federal Data Protection and Information Commissioner's guidance (available at https://bit.ly/37bStHs), and private publications, such as for example, Alan Charles Raul, "Why Schrems II Might Not Be a Problem for EU-U.S. Data Transfers", December 21, 2020, available at https://bit.ly/3qHNMy7 and a full paper from the same author at https://bit.ly/2V9veez with the follow-up post "Transferring EU Data To US After New Contractual Safeguards" of May 17, 2021, available at https://bit.ly/3l12oHZ.

[7)] Under U.S. law, the term is broadly understood under Section 702 FISA; it includes telcos, ISPs, email providers, cloud services and "any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored." This also covers social media providers and may even include all companies that otherwise provide their users with the ability to send or receive electronic communications; theoretically, this also includes companies that provide e-mail services to their employees (even if only for business purposes). NOYB provides a form to ask service providers whether they are ECSPs (https://bit.ly/3lgsTt5).

[8)] For a discussion of the term "possession, custody, or control" see, for example, Justin Hemmings, Sreenidhi Srinivasan, Peter Swire, Defining the Scope of "Possession, Custody, or Control" for Privacy Issues and the CLOUD Act, in: Journal of National Security Law & Policy, Vol. 10 No. 3 of January 23, 2020 (https://bit.ly/3i2xfC9). Control may exist either in the form of "legal control" (the right to request access to the data in a particular situation) or "day-to-day control" (the ability to access data in day-to-day business). See also Hogan Lovells' Demystifying the U.S. CLOUD Act: Assessing the law's compatibility with international norms and the GDPR of January 15, 2019 (https://bit.ly/3rLQfbp) with a summary of the standards of US law as to what amounts to "control".

[9)] According to Section 702, 50 U.S.C. 1881a(b), the US authorities "may not intentionally target" "any person known at the time of acquisition to be located in the United States" or "a United States person reasonably believed to be located outside the United States." A "United States person" (or "US person") is anybody who is a (i) citizen or national of the US, (ii) an alien lawfully admitted for permanent residence (e.g., green card holder), (iii) an unincorporated association with a substantial number of members who are citizens of the US or are aliens lawfully admitted for permanent residence or (iv) a corporation that is incorporated in the US (https://www.nsa.gov/about/faqs/sigint-faqs/#sigint4). See on this argument Alan Charles Raul, "Why Schrems II Might Not Be a Problem for EU-U.S. Data Transfers", December 21, 2020, available at https://bit.ly/3qHNMy7 and a full paper from the same author at https://bit.ly/2V9veez with the follow-up post "Transferring EU Data To US After New Contractual Safeguards" of May 17, 2021, available at https://bit.ly/3l12oHZ.

[10)] The doctrine of international comity, as recognized under US law, provides certain standards or rules in resolving conflicts between US and foreign laws. See, for example, William S. Dodge, International Comity in American Law, in: Columbia Law Review, Vol. 115, No. 8, December 2015 (https://bit.ly/3eVzlSq).

[11)] Here, we do not assess whether the authorities will be interested in the data of the particular data exporter at issue (e.g. company XY and its employees = subjective view), but whether the *categories* of personal data at issue are, based on the practices of the relevant authorities, the subject of their lawful accesses at issue, either because such data is the target or because it is a by-catch (= objective view). Do not consider legal arguments here, as they are considered under a) (otherwise this results in double-counting). This may not be easy to assess at first sight, but there are sources available, such as the official reports that discuss the monitoring by the relevant authorities. See, for example, the Privacy and Civil Liberty Oversight Board (PCLOB) (https://bit. ly/3yeO7us), the NSA's comments (https://bit.ly/3dFalhk), and the decisions of the Foreign Intelligence Surveillance Court (FISC) granting accesses in such cases (2019: https://bit.ly/3heBYQB). Also consider the past experience of the data importer, where available (even if not substantiated by independent reports; the inexistence of such requests to the data importer as such does not mean that the probability is 0%, though; depending on the circumstances, the inexistence may just be coincidence).

* This form and the underlying method was developped by David Rosenthal, VISCHER (Switzerland), with the contribution of Samira Studer (VISCHER). Thanks for valuable input to Caitlin Fennessy (IAPP). David Rosenthal can be reached at david@rosenthal.ch (private) or drosenthal@vischer.com (office).

EU SCC Transfer Impact Assessment (TIA)

If necessary, attach documentation

for use under the EU General Data Protection Regulation (GDPR) and Swiss Data Protection Act (CH DPA), in particular for complying with the EU Standard Contractual Clauses (EU SCC)

Author: Julian Wu (https://nebula.zyxel.com/)

Draft 1.00 for public consultation (Nov. 3rd, 2021) **(Version for transfers to Taiwan)**

See TIA Scenarios and other worksheets

Step 1: Describe the intended transfer

a)	Data exporter[1] (or the sender in case of a relevant onward transfer):	Nebula User
b)	Country of data exporter:	EU
c)	Data importer[2] (or the recipient in case of a relevant onward transfer):	Zyxel Networks Corporation – Worldwide Headquarters (Taiwan)
d)	Country of data importer:	Taiwan
e)	Context and purpose of the transfer:	**Cloud-based network management services**
f)	Categories of data subjects concerned:	User data, third parties included in user content
g)	Categories of personal data transferred:	User content, user communications, usage data
h)	Sensitive personal data:	None
i)	Technical implementation of the transfer:	Remote access of the data in EU data center (Ireland). Mirroring of user contact.
j	Relevant onward transfer(s) of personal data (if any):[3]	None
k)	Countries of recipients of relevant onward transfer(s):	None

→ perform separate TIA

Step 2: Define the TIA parameters

				Reasoning
a)	Starting date of the transfer:	1-十一月-16		
b)	Assessment period in years:	10		*Once we approach the end of the period or the legal situation changes , we will re-assesss the situation.*
	Ending date of the assessment based on the above:	1-十一月-26		
c)	At which point is the probability of lawful access so low that we have no reason to believe that it will happen during our assessment period? This is the case if the probability is so low that number of additional years it would take for the chance to increase to "50:50" is:	30	(= in total 40 years)	*We believe that if the probability of a prohibited lawful access to happen is so low that even after an additional 30 years in a row the chance of a prohibited lawful access occurring is still only at 50:50, it is of mere theoretical nature in a five year period which we are looking at here.*
	Probability permitted based on the above:	15.91%		
d)	Target jurisdiction for which the TIA is made:	Taiwan		(if there are additional jurisdictions, perform a separate TIA)
e)	Relevant local laws taken into consideration:	National Security Act, Article 2-1,		*This value is not relevant in our case. We have left it unchanged.*
f)	In how many cases will authorities in the target jurisdiction comply with their laws when pursuing lawful access even if not challenged?	50%		*Then we also delete the 50% - would at least be consistent*

Step 3: Define the safeguards in place

				Reasoning
a)	Would it be feasible, from a practical, technical and economical point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead?	No		*Given our operational structure, there is no alternative to have the personal data at issue also processed in Taiwan.*
b)	Is the personal data transferred under one of the exemptions pursuant to applicable data protection law (e.g., Art. 49 GDPR in case of the GDPR)?	No		*the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;*
c)	Is the personal data at issue transmitted to the target jurisdiction in clear text (i.e. there is no encryption in-transit)?[4]	No	*Ensure that data remains encrypted*	*All traffic over telecom lines is protected by state-of-the-art line encryption.*
d)	Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not encrypted or access to the keys to decrypt is possible)?	Yes	*Foreign lawful access is at least technically possible*	*The recipient needs access to the data in clear text in order to be able to process it. Encryption is not possible.*
e)	Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Standard Contractual Clauses in case of the GDPR, approved BCR, or - in the case of an onward transfer - a back-to-back-contract in line with the EU SCC), and can you expect compliance with it, insofar permitted by the target jurisdiction?	Yes	*Ensure that the mechanism remains in place and is complied with";"Enter into the EU SCC, for instance, and ensure compliance")*	*SCC*

Based on the answers given above, the transfer is: **permitted, subject to Step 4**

Step 4: Assess the risk of prohibited lawful access in the target jurisdiction[5]

*Country-specific! The following factors have been drafted for **US law** ; amend as necessary for other jurisdictions.*

a) Assess the probability that during the assessment period, the following *legal arguments* will prevent the local authorities in the target jurisdiction from successfully forcing the data importer/recipient to disclose personal data at issue under the relevant local laws as identified in Step 2 above:[6]

	Probability†	Probability of possibility of a (successfull) request††	*Reasoning*

	The data importer/recipient is no "Electronic Communications Service Provider"[7] with regard to the processing of personal data at issue and, thus, out of scope of the relevant laws	100%	0.00%	
	The data importer/recipient has no possession, custody or control over the personal data at issue in clear text and can, thus, not be (successfully) ordered to provide or search it in clear text under the relevant laws[8]	10%	90.00%	
	The transfer of the personal data at issue or the content of the personal data will be considered communications to either a person located in the United States or a US person, which may not be "intentionally targeted" by the US authorities under the relevant laws, but such targeting would occur in the present case, and, thus, prevent such a request[9]	50%	50.00%	*The data are stored in AWS EU region, but AWS is a US company.*
	Performing a prohibited lawful access would violate the data exporter's or other applicable foreign law in a manner that is not permitted under the US law doctrine of international comity, which, thus, prevents such a request[10]	0%	100.00%	*Our data are stored in Ireland, the resulting violation of the GDPR would in our view not deter the US government from accessing it.*
	There are other legal grounds under US law that prevent a prohibited lawful access to occur in the present case	0%	100.00%	*n/a*
b)	Is the data importer/recipient contractually required to defend the personal data at issue against lawful access attempts?	Yes	100.00%	*This is a requirement under the EU SCC entered into with the data importer.*
c)	Probability that during the assessment period, the data is regarded as content that is the subject of lawful access requests at issue under the relevant local laws, based on past experience?[11] †††	5%	5.00%	*The data we have is rarely the subject of lawful access request.*
d)	Probability that during the assessment period, the data importer/recipient is technically able to on an ongoing basis search the data in plain text for selectors (i.e. search terms such certain recipients or senders of electronic communications) without the data exporter's permission as part of the lawful access requests at issue under the relevant local laws? †††	20%	20.00%	*The data are encrypted on rest and the system also implemented pseudomization thus the search in plain text is merely doable.*
f)	Are measures in place to find out if during the assessment period the circumstances taken into account in the above assessments are no longer valid?	Yes		*We are regularly monitoring the legal development in this area (and at least annually).*

Probability that legal arguments fail to prevent foreign lawful access: †††	0.00%	
Overall probability of a lawful access prohibited under applicable data protection laws:	0.00%	during the assessment period
In view of the TIA parameters, the residual risk of prohibited lawful access is:	acceptable	
Number of years it takes for a lawful access to occur at least once with a *90 percent* probability:	∞	
Number of years it takes for a lawful access to occur at least once with a *50 percent* probability:	∞	

... assuming that the probability neither increases nor decreases over time (like tossing a coin)

We have made the assessement in Step 4 on the following basis (e.g., internal legal analysis, outside legal advice, support by the data importer, legal research, public documentation, statistics):	*With the help of experienced outside counsel and legal research, as indicated*

Final Step: Conclusion

In view of the above and the applicable data protection laws, the transfer is: **permitted**

Reassess at the latest by: 1-十一月-26
(or if there are any changes in circumstances)

This Transfer Impact Assessment has been made by:

Place, Date:

Signed:

By:

Note: Under the EU SCC, the TIA is to be adopted by both the data exporter and importer.

Scope of this TIA: This Transfer Impact Assessment should be used for assessing foreign lawful access risks *only for the purposes of European data protection law* , where foreign lawful access is not per se a problem, but only if it does not respect the essence of the fundamental rights and freedoms or exceeds what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of the GDPR. Accordingly, foreign lawful access requests that can be challenged before an independent and impartial court (in a European sense of the word) are permitted if they are regulated by law, are needed to safeguard the aforementioned objectives (such as prosecuting crimes), are undertaken in a proportionate manner and come with the possibility of the data subject getting legal redress. For instance, lawful access by way of the US CLOUD Act is in principle not an issue under European data protection law; in fact, it is in line with the Cybercrime Convention of the European Council. That said, there may be cross-border transfers of data where *any foreign lawful access is an issue* , for example, in where professional secrecy obligations apply. In such cases please use the spreadsheet "Cloud Computing: Risk Assessment of Lawful Access By Foreign Authorities" also from David Rosenthal, available at www.rosenthal.ch (https://bit.ly/2V9dj7V), which provides for a risk assessment also for these types of foreign lawful access. In turn, this TIA focuses on foreign lawful access where there is no possibility for recourse to an independent court, which is what has been the issue in the "Schrems II" decision by the European Court of Justice in its decision C-311/18 of July 16, 2020.

Legal Basis of this TIA: Art. 44 et seq. GDPR, Art. 6 Swiss Data Protection Act, Art. 16 et seq. revised Swiss Data Protection Act; Recommendation 01/2020 of the European Data Protection Board (Version 2.0 of June 18, 2021); Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of the European Commission (C(2021) 3972 final of June 4, 2021), Guide for checking the admissibility of data transfers with reference to foreign countries (Art. 6 para. 2 letter a FADP) of the Swiss Federal Data Protection and Information Commissioner dated June 18, 2021 (as amended on June 22, 2021).

† Example: If you believe that a particular legal argument will be found valid by three out of ten judges assessing the same case, the probability will be 30%. If you conclude that the argument is not valid, enter 0%. If you believe it will in any event be successful, put in 100%. If you don't know, put in 0%. Of course, nobody can predict the future, but this is also not necessary. For a TIA it is sufficient to undertake an diligent and professional predictive judgement following a proper protocol. To avoid noise and bias, we have already split up and structured the assessment in several independent parts. To further reduce noise and bias, ask several knowledgeable people to independently provide their assessment, then have them discuss their values, and then ask them to again provide their assessment. Use the average of the values each of them provided after the discussion (this referred to as the "Delphi" method).

†† In line of the recommendations of the EDPB, we do not assess whether the access will actually occur or not (because they are not interested in the company XY or their employees). We assess the (objective) *possibility* of it occuring. A 100% possibility means that we have to expect that a lawful access under the relevant laws will occur during the period, but it may still not happen because the relevant authorities do not believe it makes sense to order the data importer to produce the data at issue given their specific tasks, projects, etc. which we don't know about.

††† These values correspond to the values in C50, C52 and C51 of the "Cloud Computing: Risk Assessment of Lawful Access By Foreign Authorities" spreadsheet (available on www.rosenthal.ch)

[1)] The data exporter is the party being subject to the GDPR or Swiss DPA who exports personal data to a non-whitelisted third country (e.g., the US). It has the same meaning as in the EU Standard Contractual Clauses (SCC). The data exporter can be a controller, joint controller, processor or sub-processor. It is not relevant whether the data exporter is itself in Europe, a whitelisted country or a non-whitelisted country. It will always be required under the EU SCC and GDPR or Swiss DPA to perform a TIA. If the TIA is performed for the purpose of assessing a relevant onward transfer then the sender or originator of the relevant onward transfer is the "data exporter" for the purposes of this TIA.

[2)] The data importer is the party in a non-whitelisted country (e.g., the US) who receives personal data from a data exporter. The data importer can be a controller, joint controller, processor or sub-processor. It is the party with whom the data exporter will typically want to enter into the EU SCC (unless there are other grounds for the transfer). If the TIA is performed for the purpose of assessing a relevant onward transfer then the recipient of the relevant onward transfer is the "data importer" for the purposes of this TIA.

[3)] Relevant onward transfers of personal data are onward transfers of personal data by a data importer to another party in a non-whitelisted country. If this other party is a processor or sub-processor, even if the data exporter has no direct contractual relationship with it, a separate TIA has to be performed for such relevant onward transfer if the recipient is in a non-whitelisted country, because such relevant onward transfer can, as well, expose the personal data at issue to the risk of prohibited foreign lawful access. Since this TIA can be made for only one country and one recipient at a time, fill out and perform multiple TIAs for each recipient of a relevant onward transfer.

[4)] This is relevant for assessing the exposure to lawful interception of Internet backbones using selectors (upstream monitoring of communications).

[5)] In this section, the probability of a foreign authority accessing the personal data in clear text in a manner that does not respect the essence of the fundamental rights and freedoms or exceeds what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of the GDPR. The analysis only has to assess provisions of the target jurisdiction that grant public authorities access to the personal data at issue and fail to, in essence, satisfy any of the following four requirements: (1) Access is subject to the principle of legality, i.e. of clear, precise and accessible rules, (2) access is subject to the principle of proportionality, (3) there are effective means of legal redress for the data subjects to pursue their rights in the target jurisdiction in connection with an access to their personal data, and (4) any access is subject to legal recourse to an independent and impartial court (or other forms of independent recourse bodies). For example, in the US, access requests on the basis of Section 702 FISA (Foreign Intelligence Service Act) and EO 12.333 are considered *not* fulfilling in particular requirement (3) and (4). Hence, it has to verified how probable it is that there may be access requests on the basis of these two legal grounds. If the probability is so low that the exporter has "no reason to believe" that such access will occur, the transfer is permitted as per the SCC, the GDPR and the CH DPA, even though the SCC or BCR as such would not provide protection against such requests. The analysis in this section shall be based on the law applicable in the target jurisdiction and the way how it is applied by authorities and courts (including court decisions). The analysis may require obtaining a legal opinion or other forms of legal advice from counsel.

[6)] Consider all documented information on applicable legislation, case law, practices of authorities and past experience (including of the data importer, where available). You may want to ask the data importer the necessary questions (Clause 14(c) actually requires the data importer to provide "relevant information"). On this topic, see, for the EDPB recommendations 01/2020 on supplementary measures (version 2.0 adopted on May 18, 2021, available at https://bit.ly/3rSv07O), the FAQ for company of NOYB (including forms to be sent to US providers, available at https://bit.ly/2Vozeb7), the Swiss Federal Data Protection and Information Commissioner's guidance (available at https://bit.ly/37bStHs), and private publications, such as for example, Alan Charles Raul, "Why Schrems II Might Not Be a Problem for EU-U.S. Data Transfers", December 21, 2020, available at https://bit.ly/3qHNMy7 and a full paper from the same author at https://bit.ly/2V9veez with the follow-up post "Transferring EU Data To US After New Contractual Safeguards" of May 17, 2021, available at https://bit.ly/3l12oHZ.

[7)] Under U.S. law, the term is broadly understood under Section 702 FISA; it includes telcos, ISPs, email providers, cloud services and "any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored." This also covers social media providers and may even include all companies that otherwise provide their users with the ability to send or receive electronic communications; theoretically, this also includes companies that provide e-mail services to their employees (even if only for business purposes). NOYB provides a form to ask service providers whether they are ECSPs (https://bit.ly/3lgsTt5).

[8)] For a discussion of the term "possession, custody, or control" see, for example, Justin Hemmings, Sreenidhi Srinivasan, Peter Swire, Defining the Scope of "Possession, Custody, or Control" for Privacy Issues and the CLOUD Act, in: Journal of National Security Law & Policy, Vol. 10 No. 3 of January 23, 2020 (https://bit.ly/3i2xfC9). Control may exist either in the form of "legal control" (the right to request access to the data in a particular situation) or "day-to-day control" (the ability to access data in day-to-day business). See also Hogan Lovells' Demystifying the U.S. CLOUD Act: Assessing the law's compatibility with international norms and the GDPR of January 15, 2019 (https://bit.ly/3rLQfbp) with a summary of the standards of US law as to what amounts to "control".

[9)] According to Section 702, 50 U.S.C. 1881a(b), the US authorities "may not intentionally target" "any person known at the time of acquisition to be located in the United States" or "a United States person reasonably believed to be located outside the United States." A "United States person" (or "US person") is anybody who is a (i) citizen or national of the US, (ii) an alien lawfully admitted for permanent residence (e.g., green card holder), (iii) an unincorporated association with a substantial number of members who are citizens of the US or are aliens lawfully admitted for permanent residence or (iv) a corporation that is incorporated in the US (https://www.nsa.gov/about/faqs/sigint-faqs/#sigint4). See on this argument Alan Charles Raul, "Why Schrems II Might Not Be a Problem for EU-U.S. Data Transfers", December 21, 2020, available at https://bit.ly/3qHNMy7 and a full paper from the same author at https://bit.ly/2V9veez with the follow-up post "Transferring EU Data To US After New Contractual Safeguards" of May 17, 2021, available at https://bit.ly/3l12oHZ.

[10)] The doctrine of international comity, as recognized under US law, provides certain standards or rules in resolving conflicts between US and foreign laws. See, for example, William S. Dodge, International Comity in American Law, in: Columbia Law Review, Vol. 115, No. 8, December 2015 (https://bit.ly/3eVzlSq).

[11)] Here, we do not assess whether the authorities will be interested in the data of the particular data exporter at issue (e.g. company XY and its employees = subjective view), but whether the *categories* of personal data at issue are, based on the practices of the relevant authorities, the subject of their lawful accesses at issue, either because such data is the target or because it is a by-catch (= objective view). Do not consider legal arguments here, as they are considered under a) (otherwise this results in double-counting). This may not be easy to assess at first sight, but there are sources available, such as the official reports that discuss the monitoring by the relevant authorities. See, for example, the Privacy and Civil Liberty Oversight Board (PCLOB) (https://bit. ly/3yeO7us), the NSA's comments (https://bit.ly/3dFalhk), and the decisions of the Foreign Intelligence Surveillance Court (FISC) granting accesses in such cases (2019: https://bit.ly/3heBYQB). Also consider the past experience of the data importer, where available (even if not substantiated by independent reports; the inexistence of such requests to the data importer as such does not mean that the probability is 0%, though; depending on the circumstances, the inexistence may just be coincidence).

* This form and the underlying method was developped by David Rosenthal, VISCHER (Switzerland), with the contribution of Samira Studer (VISCHER). Thanks for valuable input to Caitlin Fennessy (IAPP). David Rosenthal can be reached at david@rosenthal.ch (private) or drosenthal@vischer.com (office).