Data Processing Addendum (Partners)

(Revised 30 May 2022)

This Data Processing Addendum ("**DPA**") is entered into by and between GMO GlobalSign, K.K., a Japanese company located at Shibuya Fukuras 9-16F, 1-2-3, Dogenzaka, Shibuya-ku, Tokyo 150-0043, Japan acting on its own behalf and as agent for each GlobalSign Affiliate ("**GlobalSign**") and Company and forms part of the Original Agreement between GlobalSign and Company from the Effective Date of the Original Agreement.

CONTENTS

RECITALS 1

DATA SHARING ADDENDUM 3

RECITALS

A. GlobalSign has entered into a Reseller or Service Provider agreement with Company (the "Original Agreement") for the distribution of GlobalSign products or services by Company to Company's Customers (the "Services") as further detailed in the Original Agreement.

B. GlobalSign and Company wish to memorialize their arrangement regarding sharing of Personal Data belonging to Company Customers.

C. Seeking to comply with applicable data protection laws including, but not limited to, the General Data Protection Regulation (EU) 2016/679, the UK GDPR and the Data Protection Act 2018 ("**Data Protection Laws**")

and to act in the following capacities, as defined in and interpreted in accordance with the Data Protection Laws,

the parties wish to implement legal mechanisms for the following flow of Personal Data of individuals (Data Subjects), who are employees or contractors of the customers of Company, as defined in Recital D hereof:

(i) The parties treat Company's customer, a business, ("**Company Customer**") as the first Data Controller of the Personal Data;

(ii) The Company Customer, as the first Data Controller, transfers the Personal Data of its employees or contractors ("**Shared Personal Data**") to Company as the second Data Controller;

(iii) Company, as a Data Controller, transfers the Shared Personal Data to GlobalSign as its joint Data Controller on the terms of the Data Sharing Addendum hereto.

(iv) As to onward transfers of the Shared Personal Data by GlobalSign from Japan to any other jurisdiction or person, it shall be the responsibility of GlobalSign to ensure they comply with the Data Protection Laws.

D. "**Data Subject**", "**Data Controller**", "**Data Processor**", "**Personal Data**", "**Process**", "**Processed**" **or** "**Processing**" shall each have the meaning as set out in the Data Protection Laws;

E. Capitalized terms not otherwise defined in this DPA are defined in the Original Agreement or in the Data Protection Laws.

DATA SHARING ADDENDUM

This Data Sharing Addendum (this "**DPA**") is made by and between Company and GlobalSign. It forms part of the Original Agreement currently in place between Company and GlobalSign for the resale of GlobalSign's products and services (the "**Original Agreement**").

"Shared Personal Data"	• contact information, such as name, phone number, and email address;
	• billing information, such as billing name and address, and;
	• for the issuance/validation of a Certificate to Company's customer:
	  ○ IP address, and/or email address, depending on the type of Certificate;
	  ○ other personal information that may be required by the Baseline Requirements, EV Guidelines, and/or EV Code Signing Guidelines to validate and issue a Certificate to Company's customer;
	  ○ other information agreed to by the Data Subject under the Subscriber Agreement or the CPS
	• Photographs, video or other digital media.

"Agreed Purposes"	The provision of GlobalSign's services, namely, the issue and validation of security certificates and customer support

WHEREAS:
Company resells certain products and services, including GlobalSign's products and services, and Company determines the purpose and manner by which it collects Personal Data for its own internal business purposes;

GlobalSign separately determines the manner by which it will use such Shared Personal Data as may be necessary to provide the purchased GlobalSign product or service to the Company Customer;

GlobalSign and Company desire to set out the arrangement, pursuant to GDPR Articles 26 and 30, for the sharing of Personal Data between the parties as Data Controllers;

NOW, therefore, in consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as a DPA to the Original Agreement:

1. General

1.1 Shared Personal Data. GlobalSign and Company agree that

(a) Company will regularly disclose to GlobalSign Shared Personal Data collected by Company for the Agreed Purposes and that GlobalSign will from time to time disclose to Company Shared Personal Data collected by GlobalSign for the Agreed Purposes;

(b) the Personal Data to be shared between the parties shall be confined to the Shared Personal Data, and

(c) with regard to the Shared Personal Data, GlobalSign and Company are Joint Controllers, whereby:

(i) Company determines the purpose and manner by which it collects Personal Data for its own internal business purposes;

(ii) GlobalSign separately determines the manner by which it uses Shared Personal Data as may be necessary to provide the purchased GlobalSign product or service to the Company Customer;

(iii) Company shares the Shared Personal Data with GlobalSign when a Company Customer purchases a GlobalSign product and/or service; and

(iv) Company shares only that information that is necessary for GlobalSign to identify the Company Customer to provide such Company Customer with the purchased GlobalSign product and/or Service.

1.2 Effect of Non-Compliance with Data Protection Laws. Each party shall comply with all the obligations imposed on a Controller under the Data Protection Laws, and any material breach of the Data Protection Laws by one party shall, if not remedied within thirty (30) days of written notice from the other party, give grounds to the other party to terminate this DPA and the Original Agreement with immediate effect.

2. Obligations Relating to Data Sharing

2.1 Company's Obligations. Company shall

2.1.1 ensure that it has all necessary notices and consents in place to enable lawful transfer of the Shared Personal Data to the Permitted Recipients for the Agreed Purposes; and

2.1.2 ensure that each of its Company Customers purchasing a GlobalSign product or service agrees to, and affirmatively accepts, GlobalSign's Subscriber Agreement applicable to the GlobalSign's product or service.

2.2 Mutual Obligations. Each party shall:

2.2.1 give full information to any Data Subject of the nature of Processing of such Personal Data that may be Processed under this DPA, and that, on the termination of this DPA, Personal Data relating to them may be retained by or, as the case may be, transferred to one or more of the Permitted Recipients, their successors and assignees;

2.2.2 process the Shared Personal Data only for the Agreed Purposes;

2.2.3 not disclose or allow access to the Shared Personal Data to anyone other than the Permitted Recipients;

2.2.4 ensure that all Permitted Recipients are subject to written contractual or other appropriate and legally enforceable obligations concerning the Shared Personal Data (including obligations of confidentiality) which are no less onerous than those imposed by this DPA and/or the Original Agreement;

2.2.5 ensure that it has in place Appropriate Technical and Organizational Measures to protect against unauthorized or unlawful Processing of Shared Personal Data and against accidental loss or destruction of, or damage to, Shared Personal Data;

2.2.6 only make a Restricted Transfer of Shared Personal Data in compliance with clause 3 of this DPA.

2.3 Mutual Assistance. Each party shall reasonably assist the other in complying with all applicable requirements of the Data Protection Laws. In particular, each party shall:

2.3.1 consult with the other party about any notices given to Data Subjects in relation to the Shared Personal Data;

2.3.2 provide the other party with reasonable assistance in complying with any such Data Subject access request applicable to the Shared Personal Data;

2.3.3 assist the other party in responding to any request from a Data Subject and in ensuring compliance with its obligations under the Data Protection Laws with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators as it relates to Shared Personal Data;

2.3.4 notify the other party without undue delay on becoming aware of any breach of the Data Protection Laws;

2.3.5 use technology for the Processing of Shared Personal Data to ensure that there is no lack of accuracy resulting from Personal Data transfers;

2.3.6 maintain complete and accurate records and information to demonstrate its compliance with this clause 2 for ten (10) years from issuance of any Certificate issued pursuant to the Original Agreement, subject to limitations on retention of Personal Data imposed by the Data Protection Laws and notice on retention of Personal Data to Data Subjects, and contribute to audits imposed upon the other party or the other party's designated auditor; and

2.3.7 provide the other party with contact details of at least one employee as point of contact and responsible manager for all issues arising out of the Data Protection Laws, including the procedures to be followed in the event of a Personal Data Breach, and the review of the parties' compliance with the Data Protection Laws.

3. International data transfers

3.1 The parties acknowledge that transfers of Shared Personal Data are permitted under the applicable Data Protection Laws where:

3.1.1 it is transferred to an Adequate Country;

3.1.2 The Data Importer complies with the following:

(i) corporate rules approved by a relevant Supervisory Authority;

(ii) a certification scheme or code of conduct approved by a relevant Supervisory Authority.

3.1.3 a derogation under the applicable Data Protection Laws applies;

3.1.4 the Processing by the Data Importer falls within the GDPR;

3.1.5 the transfer is otherwise permitted under applicable Data Protection Laws; and/or

3.1.6 a Data Transfer Agreement applies in accordance with Clause 3.2 of this DPA.

3.2 Where there is a Restricted Transfer of Shared Personal Data (which is not otherwise permitted under clauses 3.1.1 to 3.1.5 of this DPA), then the parties agree that an applicable Data Transfer Agreement will apply. The parties agree that the following Data Transfer Agreement will apply in the circumstances described below:

3.2.1 Where the Restricted Transfer is from the European Economic Area and/or Switzerland, then the parties agree that the Swiss and EEA (Controller to Controller) SCCs will apply, where:

(i) the Data Exporter will be the 'data exporter'; and

(ii) the Data Importer will be the 'data importer'.

3.2.2 where the Restricted Transfer is from the UK, then the UK Addendum SCCs will apply, as appropriate, in connection with the Data Transfer Agreement referred to at Clause 3.2.1 above.

3.3 Onward transfers: Each party shall be responsible for compliance with applicable Data Protection Laws and any applicable Data Transfer Agreement in respect of any onward transfers of Shared Personal Data.

4. **Personnel**. The parties shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to Shared Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know and/or access the Shared Personal Data, as strictly necessary for the purposes of the Original Agreement, and to comply with Applicable Laws in the context of that individual's duties, ensuring that all such individuals are informed of the confidential nature of the Shared Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements, undertaking appropriate professional or statutory obligations of confidentiality.

5. **Security Measures**. 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 parties shall, in relation to Shared Personal Data, maintain and implement Appropriate Technical and Organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful

destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Shared Personal Data), confidentiality and integrity of Shared Personal Data, as determined by each respective party to this DPA. The Security Measures maintained and implemented by the parties shall ensure a level of security appropriate to the risk for the scope of each party's responsibility, taking into account particular risks that are presented by Processing, in particular from a Personal Data Breach, including, as appropriate, the measures referred to in article 32(1) of the GDPR. Each party shall regularly monitor compliance with these Security Measures.

6. **Indemnity**. Each party shall indemnify the other party against all liabilities, costs, expenses, damages and losses (including but not limited to any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs (calculated on a full indemnity basis) and all other reasonable professional costs and expenses) suffered or incurred by the indemnified party arising out of or in connection with the breach of the Data Protection Laws by the indemnifying party, its employees or agents, provided that the indemnified party gives to the indemnifier prompt notice of such claim, full information about the circumstances giving rise to it, reasonable assistance in dealing with the claim and sole authority to manage, defend and/or settle it. The liability of the indemnifying party under this clause 6 shall be subject to the limits set out in clause 7 below and in the Original Agreement.

7. **Liability**. Subject to the limitations of liability set out in the Original Agreement, each party shall remain fully liable for their own acts and omissions under this DPA and for the acts and omissions of their respective Processors to the same extent such party would be liable if performing the Processing services of each respective Processor directly under the terms of this DPA.

8. **Miscellaneous Terms**.

8.1 Order of Precedence. Nothing in this DPA reduces Company's or any Company Affiliate's obligations under the Original Agreement or permits Company to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Original Agreement. Subject to the above sentence, with regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including the Original Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail. In the event of any conflict or inconsistency between this DPA and Exhibit A or Exhibit B, Exhibit A or Exhibit B shall prevail.

8.2 Changes in Data Protection Laws. Either party may propose any variation or modification to this DPA, which they reasonably consider to be necessary to address the requirements of any Data Protection Laws. If either party gives notice under this section:

(a) the other party shall promptly co-operate;

(b) the other party shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by the other party to protect the parties against additional risks associated with the variations made under this section, and

(c) the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to implementing those or alternative variations designed to address the requirements identified in the notice.

8.3 Ratification. The parties ratify and confirm the terms of the Original Agreement, except as modified by this DPA, the terms of the Original Agreement shall remain in full force and effect.

8.4 Amendments. Any amendments to this DPA shall be in writing and duly signed by each party's authorized representatives.

8.5 Contact Information

Data Protection issues should be addressed to:

GlobalSign
DPO@Globalsign.com

Company
The contact details detailed in the Original Agreement.

9. **Definitions**. Capitalized terms not otherwise defined in this DPA shall have the meaning given to them in the Original Agreement. The terms, "**Appropriate Technical and Organizational Measures**", "**Controller**", "**Data Subject**", "**Joint Controllers**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly. Unless defined elsewhere in this DPA, capitalized terms used in this DPA shall have these meanings:

9.1 "**Adequate Country**" means, as appropriate, a territory which is subject to a current finding by:
(a) the European Commission and/or
(b) the UK government;
under applicable Data Protection Laws that the territory ensures adequate level of data protection;

9.2 "**Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with a party, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

9.3 "**Applicable Laws**" means (a) European Union, Member State or UK laws with respect to any Shared Personal Data in respect of which either party is subject to EU Data Protection Laws or UK Data Protection Laws; and (b) any other applicable law with respect to any Shared Personal Data in respect of which either party is subject to any other Data Protection Laws, including the laws of the Isle of Man and other jurisdictions found by the European Commission or UK government to provide adequate data protection.

9.4 "**Data Exporter**" means a party that transfers Shared Personal Data to a Data Importer when acting as a data exporter as recognised by applicable Data Protection Laws;

9.5 "**Data Importer**" means a party that receives Shared Personal Data from a Data Exporter when acting as a data importer as recognised by applicable Data Protection Laws;

9.6 "**Data Protection Laws**" means all applicable data protection and privacy laws to which the Shared

Personal Data are subject including, but not limited to, the EU Data Protection Laws and the UK Data Protection Laws.

9.7 "**Data Transfer Agreement**" means the applicable data transfer agreements referred to in Clause 3.2 of this DPA, including:
(i) EEA and Swiss (Controller to Controller) SCCs attached at Exhibit A;
(iii) UK Addendum SCCs attached hereto as Exhibit B;
(iv) any other valid and applicable standard contractual clauses adopted under applicable Data Protection Laws;
as amended and/or updated from time to time.

9.8 "**EEA**" means the European Economic Area.

9.9 "**EU Data Protection Laws**" means EU General Data Protection Regulation 2016/679.

9.10 "**GDPR**" means EU General Data Protection Regulation 2016/679 and/or the UK GDPR, as applicable.

9.11 "**Permitted Recipients**" means, the employees of each party, and the Processors of each party.

9.12 "**Processor**" means any person (including any third party and any Affiliate, but excluding an employee of GlobalSign or Company) appointed by or on behalf of a party or any party Affiliate to Process Shared Personal Data on behalf of such party exclusively with the intention for processing activities to be carried out on behalf of any such party and in accordance with its instructions, the terms of the Original Agreement, and the terms of the written subcontract.

9.13 "**Restricted Transfer**" means
(i) a transfer of Shared Personal Data from a Data Exporter to a Data Importer; and/or
(ii) an onward transfer of Shared Personal Data from GlobalSign to a Subprocessor,
in each case, where such transfer would be prohibited by the Data Protection Laws in the absence of appropriate safeguards as set out in clauses 3.1 and 3.2;

9.14 "**UK Data Protection Laws**" means the UK GDPR and the Data Protection Act 2018;

9.15 "**UK GDPR**" means the EU General Data Protection Regulation 2016/679 as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, as amended and updated from time to time.

ACCEPTANCE

GMO Globa	**Company**
By: ICHIRO CHUJO	By:
Title: CEO	Title:
Date: 2022/08/09	Date:

Exhibit A to the DPA

STANDARD CONTRACTUAL CLAUSES –
MODULE ONE: Transfer Controller to Controller (C2C)

SECTION I

Clause 1

Purpose and scope

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

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

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

(ii) Clause 8 – Clause 8.5 (e) and Clause 8.9(b);

(iii) Clause 9 – [not used in Module One (C2C) Standard Contractual Clauses];

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

(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

Docking clause – omitted

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Purpose limitation

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

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

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

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

8.2 Transparency

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

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

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

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

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

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

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

8.3 Accuracy and data minimisation

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

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

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

8.4 Storage limitation

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

8.5 Security of processing

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

particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

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

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

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

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

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

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

8.6 Sensitive data

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

8.7 Onward transfers

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

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

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

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

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

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

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

8.8 Processing under the authority of the data importer

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

8.9 Documentation and compliance

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

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

Clause 9

Use of sub-processors

[Not used in Module One (C2C) Standard Contractual Clauses]

Clause 10

Data subject rights

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

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

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

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

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

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

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

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

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

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

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

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

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

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

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

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

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

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

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State, the following section applies: 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 following section applies: 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 following section applies: 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;

(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 authorities, 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 suspensory 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 Belgium.

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 Belgium.

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

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

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s): the Data Exporter (as defined by the DPA), as applicable.

Data importer(s): the Data Importer (as defined by the DPA), as applicable.

Where the data exporter or the data importer is the Company, the following details apply:

Address: As detailed in the Original Agreement.

Contact person's name, position and contact details: As detailed in the Original Agreement.

Activities relevant to the data transferred under these Clauses: Providing the personal data necessary to execute the Original Agreement.

Signature and date: At the same time as the parties enter into the DPA, also the SCCs, which forms an integral part of the DPA, are concluded.

Role (controller/processor): Controller

Where the data exporter or the data importer is GMO GlobalSign, K.K, the following details apply:

Address: As detailed in the DPA.

Contact person's name, position and contact details: dpo@globalsign.com

Activities relevant to the data transferred under these Clauses: Processing the personal data necessary to execute the Original Agreement.

Signature and date: At the same time as the parties enter into the DPA, also the SCCs, which forms an integral part of the DPA, are concluded.

Role (controller/processor): Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The employees, representatives, contractors of Data Exporter and Data Exporter's business customers.

Categories of personal data transferred

Contact information, such as name, phone number, and email address;

- billing information, such as billing name and address, and;
- for the issuance/validation of a Certificate to Data Exporter's customer:
  - IP address, and/or email address, depending on the type of Certificate;
  - other personal information that may be required by the Baseline Requirements, EV Guidelines, and/or EV Code Signing Guidelines to validate and issue a Certificate to Data Exporter's customer;
  - other information agreed to by the Data Subject under the Subscriber Agreement or the CPS
- Photographs, video or other digital media.

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

ID may be required from Data Exporter's customer during the vetting process and GlobalSign will contact the customer for this directly. In some instances, Customer may provide ID to Data Exporter who will then transfer the ID to GlobalSign.

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

Continuous basis.

Nature of the processing

Collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Purpose(s) of the data transfer and further processing

For Data Importer to perform the Services under the Original Agreement.

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

As detailed in the DPA.

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

N/A

C. COMPETENT SUPERVISORY AUTHORITY

The supervisory authority mandated by Clause 13. If no supervisory authority is mandated by Clause 13, then the Belgian Data Protection Authority, and if this is not possible, then as otherwise agreed by the parties consistent with the conditions set forth in Clause 13.

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

GlobalSign currently abides by the security standards in this Annex. GlobalSign may update or modify these security standards from time to time provided such updates and modifications will not result in a material decrease of the overall security of the Services during the term of the Original Agreement.

1. The bodies of policy management

For its operation as a Certification Authority, GlobalSign employs two internal teams that manage policies within the company: one is the Policy Authority and the other is the Data Protection Office.

(a) Policy Authority
The Policy Authority consists of various committees focusing on specific areas that focus on strategizing, defining and managing policies and procedures, and flow those decisions down to departmental heads for implementation. Policy Authorities 3.1 - 3.10 are sub authorities that manage policies related to security, such as Information Security Policy and Principles, Physical Security Policy, Logical Security Policy, Personnel Security Policy, Third Party Management Policy, Secure Development, Change Management Policy, and Business Continuity Management policy. All of the security measures described below are implemented based on these policies.

(b) Data Protection Office
GlobalSign also maintains a task force called the Data Protection Working Group (DPWG) under the direction of the Data Protection Officer who is appointed by the GlobalSign CEO and has the delegated authority for enforcing GlobalSign personal data processing and transfer related policies.

2. Data Center & Network Security

(a) Data Centers

Infrastructure. GlobalSign maintains its systems in geographically distributed data centers in Tokyo (Japan), Singapore and London (UK), and stores all production data in a secure environment with strong physical access barriers.

Redundancy. Infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks, power systems or other necessary devices help provide this redundancy. In the event of a power outage, backup power is provided by UPS batteries and diesel generators to provide enough electrical power typically for a period of days.

Server Operating Systems. GlobalSign servers use a Linux based implementation customized for the application environment to augment data security and redundancy. GlobalSign employs a code review process to increase the security of the code used to provide the services and enhance the security products in production environments.

Businesses Continuity. GlobalSign replicates data over multiple servers across different geographical regions, and uploads encrypted data to cloud storage daily as backup to protect against accidental destruction or

loss. GlobalSign has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

(b) Networks & Transmission

Internal Networks. All the internal networks, i.e. GlobalSign intranet, are strictly isolated by firewalls from external networks to prevent unauthorized access.

Data Transmission. Data transmission between GlobalSign offices and the data centers is typically connected via high-speed private links, i.e. VPN (IPSEC with AES256), to provide secure data transfer between data centers and offices so that data can't be read, copied, altered without authorization during transfer within GlobalSign.

In addition to the above environment, the Certificate Management Protocol (CMP) is implemented between RA systems and CA systems to maintain the highest security level of industry standard.

External Attack Surface. GlobalSign employs multiple layer networks and strong filtering controls for external facing systems. Recurring vulnerability assessment (quarterly) and penetration testing exercises (annually) are conducted in addition to any in the case of significant changes to the systems.

Intrusion Detection. GlobalSign employs intrusion detection and prevention systems on both our office and data center networks. GlobalSign intrusion detection involves:

1. Employing intrusion detection, 24 X 7 monitoring service by security professionals who are tightly integrated with the GlobalSign incident response team; and
2. Employing technologies that automatically remedy certain potentially dangerous situations.

Incident Response. GlobalSign maintains security personnel, i.e. the incident response team, who monitor a variety of communication channels for security incidents, including the notification of events from intrusion detection system (IDS) professionals, and react promptly in the event of any incident.

Encryption Technologies. GlobalSign makes HTTPS encryption (RSA2048) available, as well as IPSEC for interoffice communications with AES256.

(c) GlobalSign Intranet

Managed Devices. To connect to the LAN segment of the GlobalSign intranet, the device must have a digital certificate issued by GlobalSign's IT department.

Active Directory. GlobalSign employs central authentication mechanisms, i.e. Active Directory, before access to the GlobalSign intranet resources is permitted.

Login procedures/ authentication mechanism. To access intranet resources within GlobalSign, at least the following steps must be performed correctly:

- Boot up GlobalSign managed PC
- Device authentication via digital certificate
  (PKI authentication protocol shall be performed for the device certificate)
- Insert IC-card ID, issued for individuals, and activate the IC- Card by entering password (long and strong password, mandatory combination of alpha/numeric/symbols)

- Login to AD by entering AD password (password, different from IC-Card password)
  (PKI authentication protocol shall be performed for individual certificate)
- Duo (OTP) authentication for each individual service.

Other countermeasures. To minimize the risks of malware attacks only members of the IT department have administrator privileges. Segregation of duties and other industry standard practices are in place as specified in GlobalSign internal policies.

3. Access and Site Control

(a) Site Controls

On-site Data Center Security Operation. GlobalSign maintains an on-site security operation responsible for all physical data center security functions 24 X 7. The on-site security operation personnel monitor CCTV cameras and all alarm systems.

Data Center Access Procedures. GlobalSign maintains formal access procedures for allowing physical access to the data centers. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security.

All other entrants requiring temporary data center access must: (i) obtain approval in advance for the specific data center; (ii) sign in at on-site security operations; and (iii) must be accompanied by GlobalSign authorized employees at all times.

On-site Data Center Security Devices. GlobalSign's data centers employ an electronic card key and biometric access control system that is linked to a system alarm. The access control system monitors and records each individual's electronic card key when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate.

(b) Access Control

Infrastructure Security Personnel. GlobalSign maintains a security policy for its personnel and requires specific security training as part of the training package for these personnel. GlobalSign's infrastructure security personnel are responsible for the ongoing monitoring of the security infrastructure, the review of the services, and responding to security incidents.

Access Control and Privilege Management. The GlobalSign Certification Center (GCC) account's administrators must authenticate themselves via GCC systems in order to administer the services.

Internal Data Access Processes and Policies – Access Policy. GlobalSign's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. GlobalSign designs its systems to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording.

4. Data Access and Site Control

(a) Data Storage, Isolation & Logging

GlobalSign stores data in a multi-tenant environment on GlobalSign-owned servers, as well as cloud service providers. The data and file system architectures are replicated between multiple servers. GlobalSign employs central logging server in data centers, typically isolated from application servers.

(b) Decommissioned Disks and Disk Erase Policy
Decommissioned disks are erased in a multi-step process, and recorded according to GlobalSign policies, i.e. GlobalSign Retention Policy and internal disposal and destruction standards.

5. Personnel Security

GlobalSign personnel are required to conduct themselves in a manner consistent with the GlobalSign user guidelines and other policies regarding confidentiality, appropriate usage, and professional standards.

GlobalSign conducts appropriate backgrounds checks for the personnel who deal with critical operations, i.e. Trusted Roles, to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, GlobalSign's confidentiality and privacy policies.

6. **Subprocessor Security**

Prior to onboarding Subprocessors, GlobalSign conducts security self-check questionnaires of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged.

Once GlobalSign has assessed the risks presented by the Subprocessor, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms, as described in the addendum of GlobalSign to ensure compliance with the obligations of article 28 of the General Data Privacy Regulation.

7. **Data Protection Office**

The Data Protection Office of GlobalSign can be contacted at: dpo@globalsign.com via e-mails (or other means as provided in the GlobalSign Privacy Policy).

Exhibit B to the DPA

UK Addendum to the EU Standard Contractual Clauses

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	The Effective Date of the Original Agreement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Company or GMO GlobalSign K.K., as applicable under the DPA.	Company or GMO GlobalSign K.K. as applicable under the DPA
Key Contact	For GlobalSign, contact: DPO@globalsign.com For the Company, the contact details are detailed in the Original Agreement.	For GlobalSign, contact: DPO@globalsign.com For the Company, the contact details are detailed in the Original Agreement.
Signature (if required for the purposes of Section 2)	By entering into the Original Agreement and DPA, Data Exporter is deemed to have signed this Addendum incorporated herein, as of the Effective Date of the Original Agreement.	By entering into the Original Agreement and DPA, Data Importer is deemed to have signed this Addendum, incorporated herein, as of the Effective Date of the Original Agreement.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Module 1, as set out in Exhibit A to the DPA.

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: Parties are as set forth in Annex I.A. of the EU SCCs found in Addendum to Exhibit A.
Annex 1B: Description of Transfer: Description of Transfer is as set forth in Annex I.B. of the EU SCCs found in Addendum to Exhibit A.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Set forth in Annex II to the EU SCCs found in Addendum to Exhibit A.
Annex III: List of Sub processors (Modules 2 and 3 only): N/A

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: GMO GlobalSign K.K. ☐ Importer ☐ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

        "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";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

        "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d. Clause 8.7(i) of Module 1 is replaced with:

        "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

    e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

        "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

    f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

    g. References to Regulation (EU) 2018/1725 are removed;

    h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

    i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

    j. Clause 13(a) and Part C of Annex I are not used;

    k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

    l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a its direct costs of performing its obligations under the Addendum; and/or

    b its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.