Data Processing Addendum

(Revised 30 May 2022)

This Data Processing Addendum ("DPA") is made 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 (herein called "**GlobalSign**") and Customer acting on its own behalf and as agent for each Customer Affiliate and forms part of the Original Agreement from the effective date of the Original Agreement.

WHEREAS:

(A) GlobalSign or a GlobalSign Affiliate has entered into a certain agreement with Customer or a Customer Affiliate (the "Original Agreement") for the provision of products or services by GlobalSign or a GlobalSign Affiliate to or on behalf of Customer or a Customer Affiliate (the "Services") as further detailed in the Original Agreement.

(B) The parties agree that pursuant to the Services, GlobalSign and/or a GlobalSign Affiliate might receive or have access to certain Personal Data held by and controlled by Customer or a Customer Affiliate.

(C) The parties wish to be compliant with the Data Protection Laws, hence establish this DPA to describe the terms and conditions for the Processing activities in the context of the Services.

NOW THEREFORE, the parties agree as follows:

1. Definitions

1.1 In this DPA, the following terms shall have the meanings set out below:

1.1.1 "**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;

1.1.2 "**Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with another entity , 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;

1.1.3 **“Customer Group Member”** means Customer or any Customer Affiliate;

1.1.4 "**Customer Personal Data**" means any Personal Data Processed by GlobalSign on behalf of Customer in connection with the Original Agreement;

1.1.5 “**Data Exporter**” means a party that transfers Customer Personal Data to a Data Importer when acting as a data exporter as recognised by applicable Data Protection Laws;

1.1.6 “**Data Importer**” means a party which receives Customer Personal Data from a Data Exporter when acting as a data importer as recognised by applicable Data Protection Laws;

1.1.7 "**Data Protection Laws**" means all applicable data protection and privacy laws to which the Customer Personal Data are subject including, but not limited to, the General Data Protection Regulation (EU) 2016/679, the UK GDPR and the Data Protection Act 2018;

1.1.8 “**Data Transfer Agreement**”: means the applicable data transfer agreements referred to in Clause 8 of this DPA, including:

(i) EEA and Swiss (Controller to Processor) SCCs attached at Exhibit D;

(ii) UK Addendum SCCs attached hereto as Exhibit E;

(iii) any other valid and applicable standard contractual clauses adopted under applicable Data Protection Laws;

as amended and/or updated from time to time.

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

1.1.10 **“GlobalSign Group Member”** means GlobalSign or a GlobalSign Affiliate;

1.1.11 "**Subprocessor**" means any person (including any third party and any GlobalSign Group Member, but excluding an employee of GlobalSign or any of its sub-contractors) appointed by or on behalf of GlobalSign to Process Customer Personal Data on behalf of any Customer Group Member in connection with the Original Agreement;

1.1.12 "**Restricted Transfer**" means:

(i) a transfer of Customer Personal Data from a Data Exporter to a Data Importer; and/or

(ii) an onward transfer of Customer 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 3.5.2 and 8.2 below; and

1.1.13 **"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.

1.2 The terms, "**applicable data protection laws**", "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", **"Processor"** and "**Supervisory Authority**" shall have the same meaning as in the GDPR.

2. Processing of Customer Personal Data

2.1 The parties agree that in respect of any Customer Personal Data processed in connection with the Original Agreement the Customer shall be the Controller and GlobalSign shall be the Processor.

2.2 GlobalSign shall process the Customer Personal Data only to the extent, and in such a manner, as is necessary for the purposes of the Original Agreement and in accordance with the Customer's lawful written instructions as set out in this DPA, including its Exhibits unless Processing is required by applicable laws to which GlobalSign is subject. GlobalSign must promptly notify the Customer if, in its opinion, the Customer's instruction would not comply with the Data Protection Laws.

2.3 The Customer retains control of the Customer Personal Data and remains responsible for its compliance obligations under Data Protection Laws.

2.4 Customer instructs GlobalSign (and authorises GlobalSign to instruct each Subprocessor) to Process Customer Personal Data and, in particular, transfer Customer Personal Data to any country or territory, as reasonably necessary for the provision of the Services and consistent with the terms of the Original Agreement and this DPA.

3. Subprocessing

3.1 Customer authorises GlobalSign to appoint Subprocessors in accordance with this clause 3 and any restrictions in the Original Agreement.

3.2 To the extent that any Subprocessor appointed by GlobalSign processes Customer Personal Data then, GlobalSign will remain responsible to the Customer for the Subprocessor's obligations under this DPA.

3.3 GlobalSign may continue to use those Subprocessors already engaged by GlobalSign as at the date of this DPA as identified in the Subprocessor list which can be accessed on GlobalSign's Legal Repository webpage at https://www.globalsign.com/en/repository/GlobalSign-Subprocessors.pdf. For the avoidance of doubt, Customer specifically authorises the engagement of GlobalSign Affiliates as Subprocessors.

3.4 GlobalSign shall give Customer prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor by updating the Subprocessor list which is available in the GlobalSign Legal Repository. If, within ten (10) days of receipt of that notice via the mechanism set out in this clause 3.3, Customer notifies GlobalSign in writing of any objections (on reasonable grounds) to the proposed appointment GlobalSign shall not appoint (or disclose any Customer Personal Data to) that proposed Subprocessor until reasonable steps have been taken to address the

objections raised by Customer and Customer has been provided with a reasonable written explanation of the steps taken. If the objection cannot be resolved by the parties within thirty (30) days of receipt by GlobalSign of the objection, GlobalSign shall not be in breach of the Original Agreement to the extent that it cannot provide the Services or otherwise comply with its obligations as a result.

3.5 With respect to each Subprocessor, GlobalSign shall:

3.5.1 ensure that the arrangement between (a) GlobalSign, or (b) the relevant GlobalSign Affiliate; and the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Customer Personal Data as those set out in this DPA, in particular in relation to requiring the Subprocessor to implement appropriate technical and organisational measures, and meet the requirements of article 28(3) of the GDPR;

3.5.2 if that arrangement involves a Restricted Transfer, ensure that appropriate safeguards as set out in clause 8.2 and clause 8.5 of this DPA are at all relevant times in place between (a) GlobalSign, or (b) the relevant GlobalSign Affiliate; and the Subprocessor; and

3.5.3 provide to Customer for review such copies of the GlobalSign or GlobalSign Affiliate's agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this DPA) as Customer may request from time to time.

3.6 GlobalSign shall ensure that each Subprocessor performs the obligations under clauses 2.2, 6.1, and 7.2, as they apply to Processing of Customer Personal Data carried out by that Subprocessor, as if it were party to this DPA in place of GlobalSign.

4. GlobalSign's personnel

4.1 GlobalSign shall ensure that its personnel engaged in the Processing of Customer Personal Data are informed of the confidential nature of the Customer Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements.

4.2 GlobalSign shall ensure that access to Customer Personal Data is limited to those personnel who require such access to perform the Services.

5. Security

5.1 GlobalSign will implement appropriate technical and organisational measures against unauthorised or unlawful Processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Customer Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Customer Personal Data as set out in Exhibit A.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, GlobalSign shall assist each Customer Group Member by implementing the technical and organisational measures set forth in Exhibit A,

insofar as this is possible, for the fulfilment of the Customer Group Members' obligations to respond to requests to exercise Data Subject rights under the Data Protection Laws. GlobalSign and Customer acknowledge that they consider these measures to be appropriate, taking into account the nature of the Processing.

6.2 GlobalSign shall:

6.2.1 promptly notify Customer if any GlobalSign Group Member receives a request from a Data Subject under any Data Protection Laws in respect of Customer Personal Data; and

6.2.2 ensure that the GlobalSign Group Member does not respond to that request except on the instructions of Customer or the relevant Customer Affiliate or as required by applicable laws to which the GlobalSign Group Member is subject, in which case GlobalSign shall to the extent permitted by applicable laws inform Customer of that legal requirement before the GlobalSign Group Member responds to the request.

7. Personal Data Breach

7.1 GlobalSign shall notify Customer without undue delay upon any GlobalSign Group Member becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow Customer to meet any obligations to report or inform Data Subjects or the relevant Supervisory Authority of the Personal Data Breach under the Data Protection Laws.

7.2 GlobalSign shall co-operate with Customer and take such reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Cross-border transfers of Customer Personal Data

8.1 Subject to the terms of this clause 8, Customer Personal Data may be transferred to any country in which GlobalSign and/or its Subprocessors operate.

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

8.2.1 it is transferred to an Adequate Country;

8.2.2 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.

8.2.3 a derogation under the applicable Data Protection Laws applies;

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

8.2.5 the transfer is otherwise permitted under applicable Data Protection Laws;

8.2.6 a Data Transfer Agreement applies in accordance with Clause 8.3 of this DPA.

8.3 Where there is a Restricted Transfer of Customer Personal Data (which is not otherwise permitted under clauses 8.2.1 to 8.2.5 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:

8.3.1 Where the Restricted Transfer is from the European Economic Area and/or Switzerland, then the EEA and Swiss (Controller to Processor) SCCs will apply (subject to Clause 8.4 of this DPA);

8.3.2 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 8.3.1 above; and

8.3.3 where applicable and, as required by applicable Data Protection Laws, GlobalSign agrees that it will comply with the supplementary measures set forth in Exhibit C.

Each party's execution of this DPA shall be considered a signature to the applicable Data Transfer Agreement to the extent that such Data Transfer Agreement applies.

8.4 *EEA and Swiss Standard Contractual Clauses*

Where the EEA and Swiss (Controller to Processor) SCCs apply, the parties agree that:

8.4.1 the certification of deletion required by clause 8.5 and clause 16(d) of the EEA and Swiss (Controller to Processor) SCCs will be provided upon Customer's written request; (ii) the measures GlobalSign is required to take under clause 8.6(c) of the EEA and Swiss (Controller to Processor) SCCs will only cover GlobalSign's impacted systems; (iii) the audit described in clause 8.9 of the EEA and Swiss (Controller to Processor) SCCs shall be carried out in accordance with clause 10 of this DPA; (iv) GlobalSign may engage Subprocessors in accordance with clause 3.5.2 and 8.5 of this DPA and that use of European Commission Decision C(2010)593 Standard Contractual Clauses for Controllers to Processors or any other adequacy mechanism provided that such adequacy mechanism complies with applicable Data Protection Laws and such use of Subprocessors shall not be considered a breach of clause 9 of the EEA and Swiss (Controller to Processor) SCCs; (v) the termination right contemplated by clause 14(f) and clause 16(c) of the EEA and Swiss (Controller to Processor) SCCs will be limited to the termination of the relevant Data Transfer Agreement and, in which case, clause 8.7.2(ii) of this DPA will apply; (vi) unless otherwise stated by GlobalSign, Customer will be responsible for communicating with Data Subjects pursuant to clause 15.1(a) of the EEA and Swiss (Controller to Processor) SCCs; (vii) the information required under clause 15.1(c) of the EEA and Swiss (Controller to Processor) SCCs will be provided upon Customer's written request; and (viii) notwithstanding anything to the contrary, Customer will reimburse GlobalSign for all costs and expenses incurred by GlobalSign in connection with the performance of GlobalSign's obligations under clause 15.1(b) and clause 15.2 of the EEA and Swiss

(Controller to Processor) SCCs without regard for any limitation of liability set forth in the Original Agreement.

8.5 Where there is an onward Restricted Transfer of Customer Personal Data by GlobalSign to a Subprocessor (which is not otherwise permitted under clauses 8.2.1 to 8.2.5 of this DPA), GlobalSign will provide an appropriate safeguard in accordance with Data Protection Laws including:

8.5.1 by implementing an appropriate Data Transfer Agreement with such Subprocessor and/or such other adequacy mechanism in compliance with applicable Data Protection Laws; and

8.5.2 where the Subprocessor is a GlobalSign Group Member, GlobalSign will enter into EU and Swiss (Processor to Processor) SCCs for transfers to any GlobalSign Group Member.

8.6 Where Customer Personal Data is transferred on the basis of a Data Transfer Agreement and this Data Transfer Agreement is updated or amended by applicable Data Protection Laws, then the parties agree that GlobalSign may at any time, by giving Customer 10 days' written notice:

8.6.1 unilaterally replace the Data Transfer Agreement with any amended or updated Data Transfer Agreement and/or by such other data transfer mechanism applicable under the appropriate Data Protection Laws; or

8.6.2 terminate the relevant Data Transfer Agreement in accordance with the terms of that Data Transfer Agreement. Clause 8.7 of this DPA will then apply.

8.7 If a transfer of Customer Personal Data is lawful but subsequently becomes unlawful (and which does not become lawful following the operation of Clause 8.7), then:

8.7.1 the parties shall use their reasonable endeavours to agree an alternative basis for the transfer so as to ensure the transfer is lawful in accordance with applicable Data Protection Laws; and/or

8.7.2 GlobalSign shall, at its option:

(i) provide any modifications to the Services and/or the location of the processing so that any transfer is considered lawful; or

(ii) discontinue the corresponding Processing of Customer Personal Data affected by such termination and the Customer agrees this will fulfil the right to termination under clause 14(f) and clause 16(c) of the EEA and Swiss (Controller to Processor) SCCs.

8.8 Customer acknowledges that in respect of any Restricted Transfers:

8.8.1 GlobalSign has (at the date of this DPA) provided reasonable assistance to assist the Customer in carrying out a data transfer risk assessment in the Data Transfer Impact Assessment Questionnaire (provided to the Customer on written request); and

8.8.2 taking into account the information and obligations set forth in this DPA and the Customer's independent research, the Customer is satisfied that, to its knowledge, the measures provided in this DPA provide an adequate level of protection under applicable Data Protection Laws.

9. Deletion or return of Customer Personal Data

9.1 Subject to clause 9.2 GlobalSign shall promptly and in any event within thirty (30) days of the date of cessation of any Services involving the Processing of Customer Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of the Customer Personal Data, unless applicable law or regulation requires its storage.

9.2 Subject to clause 9.1, Customer may by written notice to GlobalSign within ten (10) days of the Cessation Date require GlobalSign to (a) return a copy of all Customer Personal Data to Customer in a mutually agreeable format; and (b) delete and procure the deletion of all other copies of Customer Personal Data Processed by any GlobalSign Group Member. GlobalSign shall comply with any such written request within thirty (30) days of the Cessation Date.

9.3 GlobalSign shall provide written certification to Customer that it and each GlobalSign Affiliate has fully complied with this clause 9 upon Customer's written request.

10. Audit Rights, Assistance and Privacy Impact Assessments

10.1 The parties agree that the audits described in clause 8.9 of the EEA and Swiss (Controller to Processor) SCCs shall be carried out in accordance with the following specifications:

10.1.1 GlobalSign shall, in accordance with the Data Protection Laws, make available to the Customer such information in GlobalSign's possession or control as the Customer may reasonably request with a view to demonstrating GlobalSign's compliance with the obligations of a Processor under the Data Protection Laws in relation to its Processing of Customer Personal Data.

10.1.2 The Customer may exercise its right of audit under the Data Protection Laws in relation to Customer Personal Data, through GlobalSign providing:

(i) an audit report not older than eighteen (18) months, prepared by an independent external auditor demonstrating that GlobalSign's technical and organizational measures are sufficient and in accordance with an accepted industry audit standard; and

(ii) additional information in GlobalSign's possession or control to an EU Supervisory Authority when it requests or requires additional information in relation to the Processing of Customer Personal Data carried out by GlobalSign under this DPA.

10.1.3 GlobalSign will provide reasonable assistance to respond to Customer's questions concerning the Services (provided Customer will pay GlobalSign's reasonable costs) to enable Customer to assess and consider reasonable mitigation measures when carrying out a data protection impact assessment.

10.1.4 If Customer requires additional information, assistance or audit to demonstrate GlobalSign's compliance with its obligations under this DPA, then GlobalSign will provide reasonable information and assistance on at least thirty (30) days' notice (unless Customer can demonstrate that the request is urgent), provided the Customer pays GlobalSign's reasonable costs.

11. Personal Data disclosure requests

11.1 To the extent permitted by law, GlobalSign agrees to notify Customer without undue delay of any legally binding requests for disclosure of Customer Personal Data. GlobalSign must not disclose the Customer Personal Data to any Data Subject or to a third party other than at the Customer's request or instruction, as provided for in this DPA or as required by law.

11.2 GlobalSign shall reject any requests for Customer Personal Data disclosures that are not legally binding, and, if permitted by law, agrees to consult the Customer prior to making any Customer Personal Data disclosures.

12. Term

12.1 This DPA shall remain in full force and effect so long as the Original Agreement remains in effect or a GlobalSign Group Member retains any Personal Data relating to the Original Agreement in its possession or control.

13. Notice

13.1 Any required notice to be given under or in connection with this DPA shall be in writing and sent by first class post or by email to:

13.1.1 in the case of GlobalSign: DPO@globalsign.com;

13.1.2 in the case of Customer: the contact details detailed in the Original Agreement.

14. General Terms

Entire Agreement

14.1 This DPA including its Exhibits and referenced documents together with the Original Agreement constitutes the entire agreement between the parties as it relates to the Processing of Customer Personal Data and supersedes any previous agreements, arrangements, undertakings or proposals, written or oral, between the parties in relation to its subject matter.

Further assistance

14.2 If required by applicable Data Protection Laws, each party agrees to execute any Data Transfer Agreement and/or (subject to Customer paying GlobalSign's reasonable costs) to take any other necessary steps to seek approval from an applicable Supervisory Authority for any transfer of Customer Data, where required.

Governing law and jurisdiction

14.3 Without prejudice to clauses 17 and 18 of the EEA and Swiss (Controller to Processor) SCCs and clauses 15(m) and 15(n) of the UK Addendum SCCs:

14.3.1 the parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Original Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

14.3.2 this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Original Agreement.

Order of precedence

14.4 Nothing in this DPA reduces GlobalSign's obligations under the Original Agreement in relation to the protection of Customer Personal Data or permits GlobalSign to Process (or permit the Processing of) Customer Personal Data in a manner which is prohibited by the Original Agreement. In the event of any conflict or inconsistency between this DPA and the Data Transfer Agreement, the relevant Data Transfer Agreement shall prevail. Where the UK Addendum SCCs apply, clauses 9 to 11 provide the hierarchy between the UK Addendum SCC and any applicable EU and Swiss SCCs.

14.5 Subject to clause 14.4, 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.

Severability

14.6 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

No variation

14.7 No modification or variation of this DPA (or any document entered into pursuant to or in connection with the DPA) shall be valid unless it is in writing and signed by or on behalf of each of the parties to this DPA.

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Original Agreement with effect from the effective Date.

Customer

Signature: _____

Name: _____

Title: _____

Date Signed: _____

GMO GlobalSign

Signature: _____

Name: Ichiro Chujo

Title: CEO

Date Signed: 2022/08/09

Exhibit A to the DPA

GlobalSign Security Standards

This Exhibit A forms part of the DPA. GlobalSign currently abides by the security standards in this Exhibit A. 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

Data Processing Particulars

[Transfer Impact Assessment Questionnaire]

This Exhibit B forms part of the DPA.

1. What countries will Customer Personal Data that is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom be stored in or accessed from? If this varies by region, please specify each country for each region.

a. Answer: As set forth on https://www.globalsign.com/en/repository/GlobalSign-Subprocessors.pdf

2. What are the categories of data subjects whose Customer Personal Data will be transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?

a. Answer: The personal data transferred concern the following categories of data subjects:

- Prospects, customers, business partners and vendors of data exporter (who are natural persons)
- Employees or contact persons of data exporter's prospects, customers, business partners and vendors
- Employees, agents, advisors, consultants, or contractors of data exporter
- Data exporter's users authorized to use the Services

3. What are the categories of Customer Personal Data transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?

a. Answer: Customer Personal Data that is Processed in connection with the Original Agreement includes:

Personal Identification Data such as name, title, address (private, work), former addresses, telephone number (private, work).

Identification details issued by the government such as ID number, passport number, driver license number.

Electronic identification data such as accounts, mail address, IP addresses.

Financial identification data such as bank account numbers, credit or debit card numbers.

Photographs, video or other digital media.

4. Will any Customer 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 be transferred outside of the

European Economic Area, Switzerland, and/or the United Kingdom? If so, are there any 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?

a. Answer: GlobalSign may require ID to be supplied by Customer for certain services. This is an industry requirement and the ID will only accessible by GlobalSign's vetting team who are based in the United Kingdom, United States, India, Philippines, Russia and Japan. Any details GlobalSign does not require are redacted from the ID prior to storage.

5. What is the frequency of the transfer of Customer Personal Data outside of outside of the European Economic Area, Switzerland, and/or the United Kingdom? E.g., is Customer Personal Data transferred on a one-off or continuous basis?

a. Answer: Customer Personal Data is transferred on a continuous basis by virtue of Customer's use of the Services.

6. Broadly speaking, what are the services to be provided and the corresponding purposes for which Customer Personal Data is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?

a. Answer: So GlobalSign can provide PKI management solutions to Customer.

7. What is the period for which the Customer Personal Data will be retained, or, if that is not possible, the criteria used to determine that period?

a. Answer: GlobalSign will retain Customer Personal Data in accordance with the DPA.

8. What business sector is GlobalSign involved in?

a. Answer: Trusted identity and security solutions.

9. When Customer Personal Data is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom to GlobalSign, how is it transmitted to GlobalSign? Is the Customer Personal Data in plain text, pseudonymized, and/or encrypted?

a. Answer: GlobalSign encrypts Customer Personal Data as appropriate.

10. Please list the Subprocessors that will have access to Customer Personal Data that is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom:

a. Answer: As set forth on https://www.globalsign.com/en/repository/GlobalSign-Subprocessors.pdf

11. Is GlobalSign subject to any laws in a country outside of the European Economic Area, Switzerland, and/or the United Kingdom where Customer Personal Data is stored or accessed from that would interfere with GlobalSign fulfilling its obligations under either of the attached set(s) of Standard Contractual Clauses? For example, FISA 702 or U.S. Executive Order 12333. If yes, please list these laws.

a. Answer: As of the effective date of the DPA, no court has found GlobalSign to be eligible to receive process issued under the laws contemplated by Question 11, including FISA Section 702 and no such court action is pending.

12. Has GlobalSign ever received a request from public authorities for information pursuant to the laws contemplated by Question 11 above (if any)? If yes, please explain.

a. Answer: As of the effective date of the DPA, GlobalSign has not received any national security orders of the type described in Paragraphs 150-202 of the judgment in the CJEU Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, nor is GlobalSign aware of any such orders in progress.

13. Has GlobalSign ever received a request from public authorities for Personal Data of individuals located in European Economic Area, Switzerland, and/or the United Kingdom? If yes, please explain.

a. Answer: No.

14. What safeguards will GlobalSign apply during transmission and to the processing of Customer Personal Data in countries outside of the European Economic Area, Switzerland, and/or the United Kingdom that have not been found to provide an adequate level of protection under applicable Data Protection Laws?

a. Answer: As set forth in Exhibit A and Exhibit C.

Exhibit C to the DPA

Supplemental Measures

GlobalSign is committed to providing users with control over their own data, to securing customer data against unauthorized access, and to protecting users' privacy. In accordance with this commitment GlobalSign complies with the following principles in responding to third party requests, including requests by governmental entities, for Customer Personal Data:

1. GlobalSign will retain and, as appropriate, consult with expert legal counsel regarding all third-party requests for Customer Personal Data.

2. GlobalSign seeks to refer each government request promptly to the relevant customer so that the customer can respond directly.

3. If the government declines to redirect its request to the relevant customer, GlobalSign will provide the customer with prompt notice of the request unless it is legally prohibited from doing so.

4. If GlobalSign is prohibited from providing prompt notice of a request to a customer, GlobalSign provides such notice as soon as the prohibition expires or is no longer in effect.

5. GlobalSign assesses the legality of all such requests and complies with requests only if and to the extent it assesses that they are valid, lawful and compulsory.

6. GlobalSign will decline to comply with and undertake reasonable efforts to contest any request it determines is not absolutely required by applicable law, including any non-valid request under FISA 702 or U.S. Executive Order 12333.

Furthermore, GlobalSign represents that:

1. Applicability of FISA Section 702: As of the effective date of the DPA, no court has found GlobalSign to be eligible to receive process issued under FISA Section 702 and no such court action is pending.

2. No National Security Orders Received: As of the effective date of the DPA, GlobalSign has not received any national security orders of the type described in Paragraphs 150-202 of the judgment in the CJEU Case C311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, nor is GlobalSign aware of any such orders in progress.

Exhibit D to the DPA

This Exhibit D forms part of the DPA.

EUROPEAN ECONOMIC AREA AND SWITZERLAND STANDARD CONTRACTUAL CLAUSES

(Module 2 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) 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.

(e) To the extent applicable hereunder, these Clauses also apply mutatis mutandis to the Parties processing of personal data that is subject to the Swiss Federal Act on Data Protection. Where applicable, references to EU Member State law or EU supervisory authorities shall be modified to include the appropriate reference under Swiss law as it relates to transfers of personal data that are subject to the Swiss Federal Act on Data Protection.

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 – 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.

MODULE TWO: Transfer controller to processor

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

MODULE TWO: Transfer controller to processor

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten (10) 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. 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

MODULE TWO: Transfer controller to processor

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

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

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

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.

MODULE TWO: Transfer controller to processor

(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

MODULE TWO: Transfer controller to processor

(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

MODULE TWO: Transfer controller to processor

(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

MODULE TWO: Transfer controller to processor

(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

MODULE TWO: Transfer controller to processor

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

MODULE TWO: Transfer controller to processor

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

MODULE TWO: Transfer controller to processor

(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

MODULE TWO: Transfer controller to processor

Data exporter(s):

Name: Customer.

Address: As set forth in the Original Agreement.

Contact person's name, position and contact details: As set forth in clause 13 of the DPA.

Activities relevant to the data transferred under these Clauses: As set forth in Exhibit B.

Role (controller/processor): Controller.

Data importer(s):

Name: GMO GlobalSign, K.K**.**.

Address: As set forth in the DPA.

Contact person's name, position and contact details: As set forth clause 13 of the DPA.

Activities relevant to the data transferred under these Clauses: As set forth in Exhibit B.

Role (controller/processor): Processor.

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

As set forth in Exhibit B.

Categories of personal data transferred

As set forth in Exhibit B.

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.

As set forth in Exhibit B.

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

As set forth in Exhibit B.

Nature of the processing

As set forth in Exhibit B.

Purpose(s) of the data transfer and further processing

As set forth in Exhibit B.

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

As set forth in Exhibit B.

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

As set forth in Exhibit B.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

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

MODULE TWO: Transfer controller to processor

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

Data importer shall implement and maintain appropriate technical and organisational measures designed to protect personal data in accordance with the DPA.

Pursuant to Clause 10(b), data importer will provide data exporter assistance with data subject requests in accordance with the DPA.

Exhibit E 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	Customer	GlobalSign
Key Contact	For Customer, the contact details are detailed in the Original Agreement.	DPO@globalsign.com
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 2, as set out in Exhibit D 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 D.
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 D.
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 D.
Annex III: List of Sub processors (Modules 2 and 3 only): As set out in https://www.globalsign.com/en/repository/GlobalSign-Subprocessors.pdf.

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: ☒ 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.