NYLAS DATA PROCESSING ADDENDUM

This Data Processing Addendum (including its Exhibits) ("**Addendum**") forms part of and is subject to the terms and conditions of the Nylas Order Form (including the Terms governing such Order Form) (the "**Agreement**") between SHL Group Limited ("**Customer**") and Nylas, Inc. ("**Nylas**"). Defined terms used but not otherwise defined in this Addendum have the meanings given in the Agreement.

1. **Subject Matter and Duration.**

   a) **Subject Matter.** This Addendum reflects the parties' commitment to abide by Data Protection Laws concerning the Processing of Customer Personal Data in connection with Nylas' execution of the Agreement. If and to the extent language in this Addendum conflicts with the Agreement, this Addendum shall control.

   b) **Duration and Survival.** This Addendum will become legally binding upon the effective date of the Agreement or upon the date that the parties sign this Addendum if it is completed after the effective date of the Agreement. Nylas will Process Customer Personal Data until the relationship terminates as specified in the Agreement.

2. **Definitions.** For the purposes of this Addendum, the following terms and those defined within the body of this Addendum apply.

   a) "**Customer Personal Data**" means Customer End-User Data and Restricted Customer End-User Data as defined in the Nylas Privacy Policy (defined below).

   b) "**Data Protection Laws**" means the applicable data privacy, data protection, and cybersecurity laws, rules and regulations to which the Customer Personal Data are subject. "Data Protection Laws" may include, but are not limited to, the California Consumer Privacy Act of 2018 ("**CCPA**"); the EU General Data Protection Regulation 2016/679 ("**GDPR**") and its respective national implementing legislations; the Swiss Federal Act on Data Protection; the United Kingdom General Data Protection Regulation; and the United Kingdom Data Protection Act 2018 (in each case, as amended, adopted, or superseded from time to time).

   c) "**Process**" or "**Processing**" means any operation or set of operations which is performed on Customer Personal Data or sets of Customer Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

   d) "**Security Incident(s)**" means the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data attributable to Nylas.

   e) "**Services**" means the services that Nylas performs under the Agreement.

   f) "**Subprocessor(s)**" means Nylas' authorized vendors and third party service providers that Process Customer Personal Data.

3. **Data Use and Processing.**

   a) Documented Instructions. Nylas shall Process Customer Personal Data to provide the Services in accordance with the Agreement, this Addendum, Nylas' Privacy Policy (defined below), and any instructions agreed upon by the parties. Nylas will, unless legally prohibited from doing so, inform Customer in writing if it reasonably believes that there is a conflict between Customer's instructions and applicable law or otherwise seeks to Process Customer Personal Data in a manner that is inconsistent with Customer's instructions. The Nylas privacy policy available at https://www.nylas.com/privacy-policy/ may be updated by notice to Customer via legal@shl.com and the parties will work together in good faith to the extent any updates to the Nylas Privacy Policy require updates to this Addendum: https://www.nylas.com/privacy-policy/. Customer will sign up for notices to the privacy policy and maintain the legal notice email provided for privacy policy updates. Such privacy policy updated as of the Effective Date of the Agreement is defined as the "Privacy Policy", which may be updated or modified pursuant to this section.

   a) Authorization to Use Subprocessors. To the extent necessary to fulfill Nylas' contractual obligations under the Agreement, Customer hereby authorizes Nylas to engage Subprocessors as listed within this Addendum (updates to the Subprocessor list within the Nylas Privacy Policy apply to this Addendum except if in violation of Section 4 below). Nylas will communicate at least thirty days in advance via legal@shl.com, unless Customer provides a different email via the method described in the Nylas Privacy Policy, to the Customer the details of any new Sub-processors before any Sub-processors carries out any activity that involved data processing Customer Personal Data. The following subprocessors are approved by the Customer for the purposes of this Agreement, as may be updated pursuant to the changes to the Privacy Policy set forth above.

The following subprocessors are approved by the Customer for the purposes of this Agreement:

EEA

Sub-processor	Purpose	Country
Amazon Web Services	Cloud Services	EEA
Zendesk	Customer Support	EEA
Honeycomb.io	Platform Reliability Monitoring	EEA
Google Cloud Platform (Looker)	Business Intelligence	EEA
New Relic	Observability Platform	EEA

United States

Sub-processor	Purpose	Country
Amazon Web Services	Cloud Services	United States
Zendesk	Customer Support	United States
Honeycomb.io	Platform Reliability Monitoring	United States
Google Cloud Platform (Looker)	Business Intelligence	United States
New Relic	Observability Platform	United States

Canada

Sub-processor	Purpose	Country
Amazon Web Services	Cloud Services	Canada
Zendesk	Customer Support	Canada
Honeycomb.io	Platform Reliability Monitoring	Canada
Google Cloud Platform (Looker)	Business Intelligence	Canada
New Relic	Observability Platform	Canada

b) Nylas and Subprocessor Compliance. Nylas agrees to (i) enter into a written agreement with Subprocessors regarding such Subprocessors' Processing of Customer Personal Data that imposes on such Subprocessors data protection requirements for Customer Personal Data that are consistent with this Addendum; and (ii) remain responsible to Customer for Nylas' Subprocessors' failure to perform their obligations with respect to the Processing of Customer Personal Data pursuant to this Addendum and as required as a Processor under applicable Data Protection Laws pursuant to this Addendum. Nylas shall on an ongoing basis monitor and control its Subprocessors' compliance with the applicable Data Protection Law. Documentation of such monitoring and control shall be provided to the Customer if so requested in writing, Nylas is accountable to the Customer for any Sub-Processor in the same way as for its own actions and omissions and shall be responsible to the Customer for any non-compliance.

c) Right to Object to Subprocessors. Where required by Data Protection Laws, Nylas will notify Customer prior to engaging any new Subprocessors that Process Customer Personal Data by updating its subprocessor list at https://www.nylas.com/privacy-policy/ and allow Customer thirty (30) days to object. If Customer has objections to the appointment of any new Subprocessor the parties will work together in good faith to resolve the grounds for the objection. If Customer does not agree to the use of any new Subprocessor by Nylas, Customer may cease utilizing

the Services, which will not relieve Customer of its payment obligations under the Agreement. This substitution or addition of Subprocessors is subject to Section 4.

d) Confidentiality. Any person authorized to Process Customer Personal Data must contractually agree to maintain the confidentiality of such information or be under an appropriate statutory obligation of confidentiality.

e) Personal Data Inquiries and Requests. Where required by Data Protection Laws, Nylas agrees to provide reasonable assistance and comply with reasonable instructions from Customer related to any requests from individuals exercising their rights in Customer Personal Data granted to them under Data Protection Laws.

f) Data Protection Impact Assessment and Prior Consultation. Where required by Data Protection Laws, Nylas shall provide reasonable assistance to Customer if Customer requests a data protection impact assessment or prior consultation with the relevant data protection authorities where required by Data Protection Laws.

g) Demonstrable Compliance. Nylas agrees to provide information reasonably necessary to demonstrate compliance with this Addendum upon Customer's reasonable request.

4. Cross-Border Transfers of Customer Personal Data.

a) Data Residency; Cross-Border Transfers of Customer Personal Data. Customer may configure the Services to restrict where Customer Personal Data is stored and accessed. This is a material contract term for the Customer.

Customer Server Location	Nylas Server Location	Permitted Nylas Data Processing Locations by country	Permitted Nylas Data Processing Locations of Subprocessors by country
EU	**Europe (Ireland)**	EU only (Ireland – storage)	EU only
United States	**United States**	US (US -storage)	US only
AU	OFF	N/A	N/A
China	OFF	N/A	N/A

Nylas will not process or transfer Customer Personal Data on the European Nylas Server Location outside of the European Economic Area ("EEA"), except with the express prior written authorization of the Customer or as permitted within this Addendum, including if Customer has configured the Services to allow for cross-border transfers of Customer Personal Data pursuant to the documentation available https://docs.nylas.com/docs/data-residency. If Nylas appoints any new or substitute Subprocessor which results in the transfer or processing of Customer Personal Data outside of the EEA in violation of this Section 4(a), then Customer may immediately terminate the applicable Order Form and will be refunded for any pre paid fees on a pro rata basis based of the effective date of termination.

To the extent (i) Customer has configured the Services on the US server, support will be providing from the US.

b) If Customer has configured the Services to allow for cross-border transfers of Customer Personal Data pursuant to the documentation available https://docs.nylas.com/docs/data-residency, Customer authorizes Nylas to transfer Customer Personal Data across international borders, including from the European Economic Area, Switzerland, and/or the United Kingdom.

c) Data Transfer Impact Assessment Questionnaire. Nylas agrees that it has provided true, complete, and accurate responses to the Data Transfer Impact Assessment Questionnaire attached hereto as **Exhibit A**.

d) EEA, Swiss, and UK Standard Contractual Clauses. In the event that Customer authorised Nylas that Customer Personal Data can be transferred by Nylas to a third country that has not been found to provide an adequate level of protection by the European Commission, the parties agree that the transfer shall be governed by the Standard Contractual Clauses attached hereto as **Exhibit B**. Where the Standard Contractual Clauses are applicable and Customer acts as a controller of Customer Personal Data with Nylas acting as a processor of Customer Personal Data, each party shall comply with its obligations under Module Two of the Standard Contractual Clauses. Where the Standard Contractual Clauses are applicable and Customer acts as a processor of Customer Personal Data with Nylas also acting as a processor of Customer Personal Data, each party shall comply with its obligations under Module Three of the Standard Contractual Clauses. The parties agree that: (i) the certification of deletion required by Clause 8.5 and Clause 16(d) of the Standard Contractual Clauses will be provided upon Customer's written request; (ii) the measures Nylas is required to take under Clause 8.6(c) of the Standard Contractual Clauses will only cover Nylas's impacted systems; (iii) the audit described in Clause 8.9 of the Standard Contractual Clauses

shall be carried out in accordance with Section 7 of this Addendum; (iv) where permitted by Data Protection Laws, Nylas may engage existing Subprocessors authorised within this Addendum by the Customer using European Commission Decision C(2010)593 Standard Contractual Clauses for Controllers to Processors and such use of Subprocessors shall be deemed to comply with Clause 9 of the Standard Contractual Clauses provided such historical Standard Contractual Clauses are updated to the new template issued by the European Commission Decision before 01 December 2022; (v) the termination right contemplated by Clause 14(f) and Clause 16(c) of the Standard Contractual Clauses will be limited to the termination of the Standard Contractual Clauses, in which case, the corresponding Processing of Customer Personal Data affected by such termination shall be discontinued unless otherwise agreed by the parties; (vi) unless otherwise stated by Nylas, Customer will be responsible for communicating with data subjects pursuant to Clause 15.1(a) of the Standard Contractual Clauses; (vii) the information required under Clause 15.1(c) will be provided upon Customer's written request; and (viii) notwithstanding anything to the contrary, Nylas will provide reasonable support to fulfil its obligations, under Clause 15.1(b) and Clause 15.2 of the Standard Contractual Clauses, which for the avoidance of doubt and without regard for any limitation of liability set forth in the Agreement, the cost to Nylas for which will not exceed the fees paid to Nylas by Customer in the 12 months preceding request for such support or where the contract is less than 12 months old, the annual contract value paid to Nylas by the Customer, unless the request is caused by Nylas processing Customer Personal Data in breach of this Addendum. Each party's signature to this Addendum shall be considered a signature to the Standard Contractual Clauses to the extent that the Standard Contractual Clauses apply hereunder.

e) Data Transfer Impact Assessment Outcome. Taking into account the information and obligations set forth in this Addendum and, as may be the case for a party, such party's independent research, to the parties' knowledge, the Customer Personal Data originating in the European Economic Area, Switzerland, and/or the United Kingdom that is transferred pursuant to the attached Standard Contractual Clauses to a country that has not been found to provide an adequate level of protection under applicable Data Protection Laws is afforded a level of protection that is essentially equivalent to that guaranteed by applicable Data Protection Laws.

5. Information Security Program.

a) Security Measures. Nylas will implement and maintain commercially reasonable technical and organizational measures designed to protect Customer Personal Data consistent with the SOC 2 Type 2 framework. Any questions about Nylas' security practices can be sent to the Nylas Security Team at security-policies@nylas.com.

6. Security Incidents.

a) Notice. Upon becoming aware of a Security Incident, Nylas agrees to provide written notice to Customer via legal@shl.com without undue delay (within 48 hours). Where possible, such notice will include all available details required under Data Protection Laws for Customer to comply with its own notification obligations to regulatory authorities or individuals affected by the Security Incident.

7. Audits.

a) Customer Audit. The parties acknowledge and agree that Nylas uses independent, third-party auditors to verify the adequacy of its Processing of Customer Personal Data. This audit will: (i) be performed at least annually; (ii) be performed against the SOC 2 Type 2 framework; (iii) be performed by a qualified professional at Nylas' selection and expense; and (iv) result in the generation of an audit report affirming that Nylas' security controls are consistent with the SOC 2 Type 2 framework ("**Report**"). Upon Customer's written request, Nylas will provide Customer with an executive summary of its Report so that Customer can reasonably verify Nylas' compliance with the security obligations in this Addendum. Any provision of such Report shall be subject to reasonable confidentiality procedures. Nylas acknowledges and agrees that onsite audit rights form part of the Standard Contractual Clauses attached hereto as Exhibit B and therefore **clause 8.9 of the** Standard Contractual Clauses, Customer reserves the right to request, allow form and contribute to audits of the processing activities covered by the Standard Contractual Clauses at reasonable intervals or if there are indications of non- compliance.

8. Data Deletion.

a) Data Deletion. At the expiry or termination of the Agreement, Nylas will delete all Customer Personal Data, except where Nylas is required to retain copies under applicable laws, in which case Nylas will isolate and protect that Customer Personal Data from any further Processing except to the extent required by applicable laws.

9. Processing Details.

a) Subject Matter. The subject matter of the Processing is the Services pursuant to the Agreement.

b) Duration. The Processing will continue until the expiration or termination of the Agreement.

c) Categories of Data Subjects. Data subjects whose Customer Personal Data will be Processed pursuant to the

Agreement.

d) Nature and Purpose of the Processing. The purpose of the Processing of Customer Personal Data by Nylas is the performance of the Services.

e) Types of Customer Personal Data. Customer Personal Data that is Processed pursuant to the Agreement.

10. Contact Information.

a) Customer and Nylas agree to designate a point of contact for urgent privacy and security issues (a "**Designated POC**"). The Designated POC for both parties are:

- Customer Designated POC: Stephen Spick, Head of Information Security contacted via legal@shl.com
- Nylas Designated POC: [INSERT]

SHL Group Limited	**Nylas, Inc.**
Signature: DocuSigned by: Emmy Hackett F83AF10BA2144A1...	Signature:
Printed Name: Emmy Hackett	Printed Name:
Title: General Counsel	Title:
Date: 12 December 2022	Date:

Exhibit A – Data Transfer Impact Assessment Questionnaire

This Exhibit A forms part of the Addendum. Capitalized terms not defined in this Exhibit A have the meaning set forth in the Addendum.

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:** None outside the European Economic Area for the Nylas EU Server unless directed by Customer. Only for the Nylas US server, United States and Canada (if permitted pursuant to the Addendum only).

    a. **Purposes of such transfer? Agreed within this Addendum that no** Customer Personal Data will be transferred outside of the European Economic Area without Customer consent.

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:** Data subjects whose Customer Personal Data is Processed under the Agreement including, but not limited to, Customer's (and its affiliates', vendors', and suppliers') end users, customers, employees, and contractors.

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 Customer Personal Data that is Processed under the Agreement including, but not limited to, email address, IP address, name, telephone number, order details (including order tracking information), and calendar data (including event details and invitees).

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:** No

5. What business sector is Nylas involved in?

    a. **Answer:** Technology (Software as a Service)

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:** None required if Nylas Product configured by Customer to on the Nylas EU server. If Nylas' Product is configured by Customer to allow processing of data in the United States and/or Canada, then Customer Personal Data may be transferred to the United States or Canada for processing to provide the Products or for support purposes.

7. What is the frequency of the transfer of Customer Personal Data 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:** Only applicable for the US server - unless requested by Customer for processing or support to be received outside of the EU. The frequency will depend on Customer implementation and use of processing services.

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

    a. **Answer:** All Customer Personal Data is transferred to Nylas in an encrypted format using the following encryption standard TLS 1.2 or above.

9. 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:** Nylas will retain Customer Personal Data in accordance with the Agreement.

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:** A current list of Nylas' Subprocessors detailed within this Addendum.

11. Is Nylas 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 Nylas fulfilling its obligations under the attached 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 Addendum, no court has found Nylas 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 Nylas 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 Addendum, Nylas 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 Nylas aware of any such orders in progress.

13. Has Nylas 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 Nylas 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?

15. **Answer:** Those safeguards set forth in the Addendum (including Annex II to the Standard Contractual Clauses).

Exhibit B – Standard Contractual Clauses

This Exhibit B forms part of the Addendum.

STANDARD CONTRACTUAL CLAUSES

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.

(f) To the extent applicable hereunder, these Clauses, as supplemented by Annex III, also apply mutatis mutandis to the Parties' processing of personal data that is subject to UK Data Protection Laws (as defined in Annex III).

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 – Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d), and Clause 8.9(a), (c), (d), (e), (f) and (g);

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 – Modules Two and Three: 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 non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

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

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

MODULE THREE: Transfer processor to processor

8.1 Instructions

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

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

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter

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

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

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

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

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

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

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

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

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

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

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. 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.

MODULE THREE: Transfer processor to processor

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

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

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

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

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

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

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

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

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

MODULE THREE: Transfer processor to processor

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

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

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

Clause 11

Redress

(a) The data 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

MODULE THREE: Transfer processor 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

MODULE THREE: Transfer processor 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

MODULE THREE: Transfer processor 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

MODULE THREE: Transfer processor 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). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data 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

MODULE THREE: Transfer processor 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.

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

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

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

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

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

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data 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. [For Module Three: The data exporter shall make the assessment available to the controller.]

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data 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

MODULE THREE: Transfer processor 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 Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor 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 Ireland.

(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

MODULE THREE: Transfer processor to processor

Data exporter(s):

1. Name: Customer.

Address: As set forth in the Notices section of the Agreement.

Contact person's name, position and contact details: Customer's Designated POC.

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

Role (controller/processor): Controller (Module Two); Processor (Module Three).

Data importer(s):

1. Name: Nylas.

Address: As set forth in the Notices section of the Agreement.

Contact person's name, position and contact details: Nylas's Designated POC.

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

Role (controller/processor): Processor.

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor*Categories of data subjects whose personal data is transferred*

As set forth in Exhibit A.

Categories of personal data transferred

As set forth in Exhibit A.

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 A.

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

As set forth in Exhibit A.

Nature of the processing

As set forth in Exhibit A.

Purpose(s) of the data transfer and further processing

As set forth in Exhibit A.

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 A.

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

As set forth in Exhibit A.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

The supervisory authority mandated by Clause 13. If no supervisory authority is mandated by Clause 13, then the Irish Data Protection Commission (DPC), 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

MODULE THREE: Transfer processor 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.

Information Security Standards. These Information Security Standards apply to data importer's processing of personal data under the Clauses. Data importer shall implement and maintain an information security program ("**Information Security Program**") that: (i) is consistent with industry standard practices taking into consideration the sensitivity of the relevant personal data processed under the Clauses, and the nature and scope of the Services to be provided; and (ii) includes commercially reasonable technical and organizational measures designed to protect personal data processed under the Clauses. At a minimum, the Information Security Program shall include:

1. Information Security Policy. Data importer shall maintain a written information security policy applicable to all authorized personnel.

2. Training. Data importer shall provide information security awareness training to all employees annually.

3. Access Control. Data importer shall maintain access control procedures and controls consistent with industry standard practices. Data importer shall limit access to personal data to those employees and subprocessors with a need-to-know.

4. Logical Separation. Data importer shall ensure personal data is logically separated from other Data importer client data.

5. Encryption. Data importer shall encrypt personal data in-transit and at rest using industry standard encryption technologies.

6. Password Management. Data importer shall maintain a password management policy designed to ensure strong passwords consistent with industry standard practices.

7. Incident Response Plan. Data importer shall maintain an incident response plan that addresses security incident handling.

8. Malware Protection. Data importer shall maintain up-to-date malware prevention measures designed to protect against malicious code and viruses.

9. Backups of personal data. Data importer shall maintain an industry standard backup system and backup of personal data to facilitate timely recovery in the event of a service interruption.

10. Disaster Recovery and Business Continuity Plans. Data importer shall maintain disaster recovery and business continuity plans consistent with industry standard practices.

Assistance with Data Subject Requests. Pursuant to Clause 10(b), data importer will provide data exporter assistance with data subject requests in accordance with the Terms.

ANNEX III

Nylas approved Subprocessors listed within the Addendum.

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

UK Addendum to the EU Commission Standard Contractual Clauses

Date of this Addendum:

1. The Clauses are dated as of the same date as the Addendum.

Background:

2. The Information Commissioner considers this Addendum provides appropriate safeguards for the purposes of transfers of personal data to a third country or an international organisation in reliance on Articles 46 of the UK GDPR and, with respect to data transfers from controllers to processors and/or processors to processors. This Addendum forms part of and supplements the Clauses to which it is attached. If personal data originating in the United Kingdom is transferred by data exporter to data importer in a country that has not been found to provide an adequate level of protection under UK Data Protection Laws, the Parties agree that the transfer shall be governed by the Clauses as supplemented by this Addendum.

Interpretation of this Addendum

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

This Addendum	This Addendum to the Clauses
The Annex	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021
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	The United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.
UK	The United Kingdom of Great Britain and Northern Ireland

4. This Addendum shall be read and interpreted in the light of the provisions of UK Data Protection Laws, and so that if fulfils the intention for it to provide the appropriate safeguards as required by Article 46 UK GDPR.

5. This Addendum shall not be interpreted in a way that conflicts with rights and obligations provided for in UK Data Protection Laws.

6. 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

7. In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.

Incorporation of the Clauses

8. This Addendum incorporates the Clauses which are deemed to be amended to the extent necessary so they operate:

    a. for 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 transfer; and

    b. to provide appropriate safeguards for the transfers in accordance with Articles 46 of the UK GDPR Laws.

9. The amendments required by Section 8 above, include (without limitation):

    a. References to the "Clauses" means this Addendum as it incorporates the Clauses

    b. 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."

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

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

    e. References to the "Union", "EU" and "EU Member State" are all replaced with the "UK"

    f. Clause 13(a) and Part C of Annex II are not used; the "competent supervisory authority" is the Information Commissioner;

    g. Clause 17 is replaced to state "These Clauses are governed by the laws of England and Wales".

    h. Clause 18 is replaced to state:

    "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."