Synqly Data Privacy Agreement

This Synqly Data Privacy Agreement, including its Annexes ("SDPA"), is entered into by Synqly, Inc., a Delaware corporation having its principal place of business at 1575 Newport Ave., San Jose, CA 95125 ("Company" or "Synqly"), and Counterparty (defined below). Synqly provides its proprietary, Software-as-a-Service solution for integrating security and infrastructure products ("Service(s)") to Customers and End Customer (each as defined below). The provision of the Service involves the Processing of Personal Data subject to the Data Protection Laws, and the purpose of this SDPA is to set forth the terms under which Synqly Processes the Personal Data. THIS SDPA APPLIES BETWEEN THE PARTIES WHERE A REPRESENTATIVE OF COUNTERPARTY CLICKS A BOX INDICATING ACCEPTANCE, TRANSFERS PERSONAL DATA TO SYNQLY FOR PROCESSING BY MEANS OF THE SERVICE, OR OTHERWISE AFFIRMATIVELY INDICATES ACCEPTANCE OF THIS SDPA. BY DOING SO, YOU: (A) AGREE TO THIS SDPA ON BEHALF OF THE ORGANIZATION, COMPANY, OR OTHER LEGAL ENTITY FOR WHICH YOU ACT ("COUNTERPARTY"); AND (B) REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND COUNTERPARTY AND ITS AFFILIATES TO THIS SDPA. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT AGREE WITH THIS SDPA, YOU MAY NOT DIRECTLY OR INDIRECTLY TRANSFER PERSONAL DATA TO SYNQLY. SYNQLY RESERVES THE RIGHT TO MODIFY OR UPDATE THE TERMS OF THIS SDPA IN ITS DISCRETION, THE EFFECTIVE DATE OF WHICH WILL BE THE EARLIER OF (I) 30 DAYS FROM THE DATE OF SUCH UPDATE OR MODIFICATION AND (II) COUNTERPARTY'S CONTINUED TRANSFER OF PERSONAL DATA.

If Customer and Synqly have executed a written data processing agreement governing the processing of personal data by means of the Service, then the terms of such signed data processing agreement between the parties will supersede this SDPA. In the provision of services by Synqly involving Counterparty, the following roles ("Roles") apply among the parties:

Counterparty	Description	Data Processing Function(s)
Customer	Party that purchases a Subscription to the Service	For Customer Personal Data Processed by Synqly, Customer is the Controller and Synqly is a Processor. For End Customer Personal Data Processed by Synqly, Customer is a Processor and Synqly is a Processor and/or subprocessor
End Customer	The Customer's customer that enables integration between the Service and Partner's platform in order for Synqly to Process the End Customer's Personal Data for the benefit of the Customer	For End Customer Personal Data Processed by Synqly, End Customer is the Controller; Customer is a Processor; and Synqly is a Processor and/or subprocessor
Partner	Provider of a SaaS solution used by End Customer (e.g., typically IT infrastructure or cyber security spaces)	End Customer is the Controller; Partner is the Processor; Synqly is the Processor to End Customer

1. Definitions. All capitalized terms used in this SDPA will have the meanings given to them herein, in applicable Data Protection Laws, or as set forth in the applicable Agreement between Synqly and the Counterparty.

   “Agreement” means the applicable terms between Synqly and Counterparty regarding use of or integration with the Service.

   “Controller” means the entity or Business which solely or jointly with other entities determines the purposes and means of the Processing of Personal Data, and for the purposes of this SDPA is as set forth in the Roles table above.

   “Data Breach” means a breach of security leading to accidental or unlawful destruction, loss, or alteration, unauthorized disclosure of, or access to, Personal Data Processed by Synqly on behalf of Counterparty.

   "Data Protection Laws” means all applicable data protection and privacy laws, their implementing regulations, regulatory guidance, and secondary legislation, each as updated or replaced from time to time, including, as they may apply: (i) the General Data Protection Regulation ((EU) 2016/679) (the “GDPR”) and any applicable national implementing laws; (ii) the UK General Data Protection Regulation (“UK GDPR”) and 8/3/23, 1:43 PM Data Processing Agreement https://Synqly.dev/legal/data-processing-agreement 4/22 the UK Data Protection Act 2018; (iii) U.S. legislation (e.g., the California Consumer Privacy Act and the California Privacy Rights Act); and (iv) any other laws that may be applicable.

   “Data Subject” means the identified or identifiable person to whom the Personal Data relates, as defined in the applicable Data Protection Laws.

   “EU Standard Contractual Clauses” or “SCCs” or “Clauses” means the terms available at https://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN and promulgated pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council 4 June.

   “Personal Data” means any information relating to a Data Subject that is subject to the Data Protection Laws and that Synqly Processes on behalf of Counterparty as described in Section 4 of this SDPA.

   “Processing” has the meaning given to it in the Data Protection Laws and “process”, “processes” and “processed” will be construed accordingly.

   “Processor” means the entity or Service Provider which Processes Personal Data on behalf of the Controller, as defined in the applicable Data Protection Laws and for the purposes of this SDPA is as set forth in the Roles table above.

2. Compliance With Laws. Each party will comply with the Data Protection Laws as applicable to it.

3. Personal Data Obligations. Counterparty undertakes that all instructions for the Processing of Personal Data under the Agreement or this SDPA or as otherwise agreed will comply with the Data Protection Laws, and such instructions will not cause Synqly to be in breach of any Data Protection Laws. Counterparty, to the extent that it provides its Personal Data to Synqly, is responsible for the means by which the Personal Data was acquired.

4. Data Processing. Synqly will Process the Personal Data solely for the purposes of providing the Service and in accordance with Counterparty's instructions as outlined in the Agreement and this SDPA, or as otherwise documented by Counterparty, in either event only as permitted by applicable Data Protection Laws. Unless prohibited by applicable law, Synqly will notify Counterparty if in its opinion, an instruction infringes any Data Protection Laws to which it is subject, in which case Synqly will be entitled to suspend performance of such instruction without liability to Synqly, until Counterparty confirms in writing that such instruction is valid under the Data Protection Laws. Any additional instructions regarding the manner in which Synqly Processes the Personal Data will require prior written agreement between Synqly and Counterparty. Synqly will not disclose Personal Data to any government, except as necessary to comply with applicable law or a valid and binding order of a law enforcement agency (such as a subpoena or court order). If Synqly receives a binding order from a law enforcement agency for Personal Data, Synqly will notify Counterparty of the request it has received so long as Synqly is not legally prohibited from doing so. Synqly will ensure that individuals with access to or involved in the Processing of Personal Data are subject to appropriate confidentiality obligations and/or are bound by related obligations under Data Protection Laws or other applicable laws. Where Synqly acts as Counterparty's Service Provider, Synqly shall not: (i) sell or share Personal Data; (ii) collect, retain, use, or disclose Personal Data (a) for any purpose other than providing the Service specified in the Agreement and this Addendum or (b) outside of the direct business relationship between Synqly and Counterparty; or (iii) combine this Personal Data with Personal Data that Synqly obtains from other sources except as permitted by applicable Data Protection Laws. Synqly certifies that it understands the prohibitions outlined in this Section and will comply with them. The duration of the Processing, the nature and specific purposes of the Processing, the types of Personal Data Processed, and categories of Data Subjects under this Addendum are further specified in the Annexes to this Addendum and, on a more general level, in the Agreement.

5. Transfers of Personal Data. Synqly shall transfer Personal Data between jurisdictions as a Data Processor in accordance with applicable Data Protection Laws.

- i. Transfers of Personal Data Outside the EEA.
    1. Transfers to countries that offer adequate level of data protection. Personal Data may be transferred from EEA to other jurisdictions where such jurisdictions are deemed to provide an adequate level of data protection under applicable Data Protection Laws.

2. Transfers to other third countries. If the Processing of Personal Data includes transfers from EEA/EU Member States to countries outside the EEA/EU which have not been deemed adequate under applicable Data Protection Laws, the parties' EU Standard Contractual Clauses are hereby incorporated into and form part of this Addendum. The Parties agree to include the optional Clause 7 (Docking clause) to the EU SCCs incorporated into this Addendum. With regards to clauses 8 to 18 of the EU SCCs, the different modules and options will apply as follows:

a. Module Two or Three shall apply, in accordance with the Roles.

b. The Option within Clause 11(a) of the EU SCCs, providing for the optional use of an independent dispute resolution body, is not selected.

c. The Options and information required for Clauses 17 and 18 of the EU SCCs, covering governing law and jurisdiction, are outlined in Section 12 of this Addendum.

d. Option 2 within Clause 9(a) of the EU SCCs, covering authorization for sub-processors, is selected, as discussed within Section 11 of this Addendum.

ii. Transfers of Personal Data Outside Switzerland. If Personal Data is transferred from Switzerland in a manner that would trigger obligations under the Federal Act on Data Protection of Switzerland ("FADP"), the EU SCCs shall apply to such transfers and shall be deemed to be modified in a manner to that incorporates relevant references and definitions that would render such EU SCCs an adequate tool for such transfers under the FADP.

iii. Transfers of Personal Data Outside the UK. If Personal Data is transferred in a manner that would trigger obligations under UK GDPR, the parties agree (i) that Annex IV shall apply.

iv. Annexes. This Addendum and its Annexes, together with the Agreement, including as relevant applicable Clauses, serve as a binding contract that sets out the subject matter, duration, nature, and purpose of the Processing, the type of Personal Data and categories of data subjects as well as the obligations and rights of the Controller. Synqly may execute relevant contractual addenda, including as relevant the EU SCCs (Module 3) with any relevant Subprocessor (as hereinafter defined, including Affiliates). Unless Synqly notifies Customer to the contrary, if the European Commission subsequently amends the EU SCCs at a later date, such amended terms will supersede and replace any EU SCCs executed between the parties.

v. Alternative Data Export Solution. The parties agree that the data export solutions identified in this Section 5 will not apply if and to the extent that Customer adopts an alternative data export solution for the lawful transfer of Personal Data (as recognized under applicable Data Protection Laws), in which event, Customer shall reasonably cooperate with Synqly to implement such solution and such alternative data export solution will apply instead (but solely to the extent such alternative data export solution extends to the territories to which Personal Data is transferred under this Addendum).

6. Technical and Organizational Measures. Synqly will implement appropriate technical and organizational measures to ensure a level of security of the Personal Data appropriate to the risk, as further described in Annex II hereto. In assessing the appropriate level of security, Synqly will take into account the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

7. Data Subject Rights. Synqly will assist Counterparty in responding to Data Subjects' requests exercising their rights under the Data Protection Laws. To that effect, Synqly will (a) to the extent permitted by applicable law, promptly notify Counterparty of any request received directly from Data Subjects to access, correct or delete its Personal Data without responding to that request, and (b) upon written request from Counterparty, provide Counterparty with information that Synqly has available to reasonably assist Counterparty in fulfilling its obligations to respond to Data Subjects exercising their rights under the Data Protection Laws.

8. Data Protection Impact Assessments. If Counterparty is required under the Data Protection Laws to conduct a Data Protection Impact Assessment, then upon written request from Counterparty, Synqly will assist where reasonably possible in the fulfilment of the Counterparty's obligation as related to its use of the Service, to the extent Counterparty does not otherwise have access to the relevant information. If required under Data Protection Laws Synqly will provide reasonable assistance to Counterparty in the cooperation or prior consultation with Data Protection Authorities in relation to any applicable Data Protection Impact Assessment.

9. Audit of Technical and Organizational Measures. Synqly agrees to make available all information necessary to demonstrate its compliance with data protection policies and procedures implemented as part of the Service. To this end, upon written request (not more than once annually) Counterparty may, at its sole cost and expense, verify Synqly's compliance with its data protection obligations as specified in this SDPA by: (i) submitting a security assessment questionnaire to Synqly; and (ii) if Counterparty is not satisfied with Synqly's responses to the questionnaire, then Counterparty may conduct an audit in the form of meetings with Synqly's information security experts upon a mutually agreeable date. Such interviews will be conducted with a minimum of disruption to Synqly's normal business operations and subject always to Synqly's agreement on scope and timings. The Counterparty may perform the audit described above either by itself or through a mutually agreed upon third party auditor, provided that Counterparty or its authorized auditor executes a mutually agreed upon non-disclosure agreement. Counterparty will be responsible for any actions taken by its authorized auditor. All information disclosed by Synqly under this Section 9 will be deemed Synqly Confidential Information, and Counterparty will not disclose any audit report to any third party except as obligated by law, court order or administrative order by a government agency. Synqly will remediate any mutually agreed, material deficiencies in its technical and organizational measures identified by the audit procedures described in this Section 9 within a mutually agreeable timeframe.

10. Breach notification If Synqly becomes aware of a Data Breach that results in unlawful or unauthorized access to, or loss, disclosure, or alteration of the Personal Data, then Synqly will notify the Counterparty without undue delay and in any event, within seventy-two hours after becoming aware of such Data Breach and will co-operate with the Counterparty and take such reasonable commercial steps as agreed with the Counterparty to assist in the investigation, mitigation and alternative data export solution extends to the territories to which Personal Data is transferred under this Addendum).

11. Sub-processing. Counterparty agrees that Synqly may engage either Synqly affiliated companies or third parties providers as "Subprocessors" and hereby authorizes Synqly to engage such Subprocessors in the provision of the Service. Synqly will restrict the Processing activities performed by Subprocessors to only what is necessary to accomplish the purposes of the Agreement and this SDPA. Synqly will impose appropriate contractual obligations in writing upon the Subprocessors that are no less protective than this SDPA, and Synqly will remain responsible for the Subprocessors' compliance with the obligations under this SDPA. Synqly maintains a list of all Subprocessors at www.Synqly.com/data-subprocessors (Annex III). Synqly may amend the list of Subprocessors by adding or replacing Subprocessors at any time and will use commercially reasonable efforts to provide Counterparty with fifteen (15) days' advance notice of any updates so long as Counterparty subscribes to Synqly's notification list. Controller will be entitled to object to a new Subprocessor by notifying Synqly in writing the reasons of its objection. Synqly will work in good faith to address Controller's objections. If Synqly is unable or unwilling to adequately address Controller's objections to its reasonable satisfaction, then Controller may terminate this SDPA and the Agreement, as specified in the Agreement.

12. Governing Law. This Addendum shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws. For the purposes of Clauses 17 and 18 of the EU SCCs, where applicable, to the extent that the governing law and jurisdiction provisions in the Agreement do not meet the requirements of the EU SCCs, the parties select Option 2 of Clause 17, and agree that the EU SCCs shall be governed by the law of the EU Member State in which the data exporter is established; where such law does not allow for third-party beneficiary rights, the EU SCCs shall be governed by the laws of the country of Ireland. Pursuant to Clause 18, any dispute between the Parties arising from the EU SCCs shall be resolved by the courts of Ireland, and the Parties submit themselves to such jurisdiction. For the purposes of Clause 13 of the EU SCCs, the Supervisory Authority shall be the data exporter's applicable Supervisory Authority. Data exporter shall notify data importer of the applicable Supervisory Authority by email at legal@Synqly.com and shall provide any necessary updates without undue delay.

13. Return or Deletion of Personal Data. Unless otherwise required by applicable Data Protection Laws, Synqly will delete or return, in Counterparty's discretion and upon Counterparty's written request, Personal Data within a reasonable period of time following the termination or expiration of the Agreement.

14. Termination. This Addendum shall automatically terminate upon the termination or expiration of the Agreement. This Addendum cannot, in principle, be terminated separately to the Agreement, except where the Processing ends before the termination of the Agreement, in which case, this Addendum shall automatically terminate.

15. Entire Agreement; Conflict. Except as amended by this SDPA, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this SDPA, the terms of this SDPA will control.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporters(s):
The Customer as defined above
Role (controller/processor): Controller and/or Processor as specified in the SDPA

Data importer(s):
Synqly, Inc. Address: 1575 Newport Ave, San Jose CA 95125
Contact person's name, position and contact details: legal@Synqly.com, Joel Bauman, Chief Executive Officer
Role: Processor (or Subprocessor as the case may be)
Activities relevant to the data transferred under these Clauses: Processing of personal data for the Services pursuant to the Agreement.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
Customer and its end users (e.g., account holders, end-customers, prospective customers, employees, contractors, suppliers and end-users of the data exporter and the data exporter's customers, vendors and partners).

Categories of personal data transferred
Categories of personal data chosen by a controller and issued to processor or subprocessor as the case may be, via the Service (e.g., log files, identify information, vulnerability information, IP addresses, and other identifying characteristics)

Note: Data Importer does not process sensitive data except to the extent transferred via the Service by Data Exporter's end users.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
On a continuous basis as determined by a controller or on its behalf as permitted under the Agreement

Nature of the processing Integration services between joint systems that a controller chooses and made available by processor or subprocessor as the case may be

Purpose(s) of the data transfer and further processing
For processor/subprocessor to provide the specific Services to a controller (or on their behalf) as required under the Agreement. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For the term of the Agreement and until notified by a controller, or controller deletion (via Service API)

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

For the term of the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY
Identify the competent supervisory authority/ies in accordance with Clause 13 The competent supervisory authority/ies applicable to Data Exporter as notified to Data Importer in accordance with Section 12 of the Addendum.

ANNEX II

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

Synqly processes all personal data received from Controller, or on its behalf under this SDPA in conformity with the following technical and organizational measures:

Information Security Organization

- Synqly's Information Security Policy outlines roles and responsibilities for personnel with responsibility for the security, availability, and confidentiality of the Product and Service.
- The Chief Product Officer is responsible for the design, implementation, and management of the organization's security policies, which are reviewed at least annually.
- Annual review includes assessment of internal controls used in the achievement of Synqly's Service commitments and system requirements. Following review, any deficiencies are resolved in accordance with the Risk Assessment and Management Program.
- The Chief Product Officer performs an annual formal risk assessment, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.
- The Chief Product Officer maintains a risk register, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.
- The Security team is responsible for identifying and tracking incidents and creating a 'lessons learned' document and sharing it with the engineering team. The Engineering team is responsible for Software development and deployment.

Personnel Security

Synqly has established a Code of Conduct outlining ethical expectations, behavior standards, and ramifications of noncompliance, as well as Acceptable Use, Data Protection, and Information Security Policies. Internal personnel acknowledge all codes and procedures within 30 days of hire. Background checks are performed on full-time employees within 30 days of the employee's start date as permitted by local laws. Reference checks are performed on contractors who have access to production data. Internal personnel complete annual training programs for information security to help them understand their obligations and responsibilities related to security.

Access Controls and Asset Management

Internal users are provisioned access to systems based on role as defined in the access matrix, which is reviewed and approved annually by the Chief Product Officer. The Chief Product Officer approves any additional access required outside the access matrix. The Chief Product Officer conducts quarterly user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities. Identified access changes are tracked to remediation. Access to production machines, network devices, and support tools

requires a unique ID. Internal user access to systems and applications with service data requires two-factor authentication in the form of user ID / password, and one-time passcode. Synqly has formal policies for password strength and use of authentication mechanisms. Production infrastructure is restricted to users with a valid SSH key; administrative access to production servers and databases is restricted to the Back-end Engineering team. Upon termination or when internal users no longer require access, infrastructure and application access is removed within one business day. Internal use of the internal admin tool is logged. These logs are reviewed monthly for appropriateness. Firewall configurations help ensure available networking ports and protocols are restricted to approved business rules. The Engineering team maintains a list of the company's system components, owners, and their business function, and the Chief Product Officer reviews this list annually.

Incident Management and Business Continuity

Synqly's Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning, and tracking incidents through to resolution. The Security team tracks identified incidents according to the Incident Response Plan and creates a 'lessons learned' document after each high or critical incident. This document is shared with the Engineering team to make any required changes. The Chief Product Officer maintains a disaster recovery plan, which is tested at least annually. The Engineering team reviews test results and makes changes to the plan accordingly.

Change Controls

Synqly's Change Management Process and Standard governs the system development life cycle, including documented policies for tracking, testing, approving, and validating changes. System changes are tested via automated test scripts prior to being deployed into production.

Code

Synqly requests are independently peer reviewed prior to integrating the code change into the master branch. System users who make changes to the development system are unable to deploy their changes to production without independent approval. The Engineering team uses a tool to enforce standard production images for production servers. Configuration changes are tested (if applicable) and approved prior to being deployed into production. The production and testing environments are segregated; production data is not used in the development and testing environments.

Data and Availability

Controls Synqly's Data Protection Policy details the security and handling protocols for service data. Full backups are performed daily and retained in accordance with the Backup Policy. The Engineering team restores backed-up data to a non-production environment at least annually to validate the integrity of backups. Access to erase or destroy customer data is limited to the Chief Product Officer and back-end engineers. The Chief Product Officer and the Engineering team manually delete data that is no longer needed from databases and other file stores in accordance with agreed-upon customer requirements. Synqly's Encryption and Key Management Policy supports the secure encryption and decryption of app secrets, and governs

the use of cryptographic controls. Encryption is used to protect the transmission of data over the internet; service data is encrypted at rest. The Engineering team encrypts hard drives for portable devices with full disk encryption. System tools monitor company load balancers and notify appropriate personnel of any events or outages based on predetermined criteria. Any identified issues are tracked through resolution in accordance with the Incident Response Plan. The Platform is configured to operate across availability zones to support continuous availability.

Vendor and Vulnerability Management

Synqly's Vendor Risk Management Policy defines a framework for the onboarding and management of the vendor relationship lifecycle. The Chief Product Officer assesses new vendors according to the Vendor Risk Management Policy prior to engaging with the vendor. Synqly's Vulnerability Management and Patch Program outlines the procedures to identify, assess, and remediate identified vulnerabilities. Vulnerability scans are executed monthly on production systems. The Chief Product Officer and the Engineering team track critical or high-risk vulnerabilities through resolution. Management has implemented intrusion prevention and detection tools to provide monitoring of network traffic to the production environment. The Engineering team uses logging and monitoring software to collect data from servers and endpoints, and detect potential security threats and unusual system activity. Malware detection software is installed on susceptible endpoints that can access the production environment. The Engineering team uses alerting software to notify impacted teams of potential security and availability events.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorized the use of the Subprocessors listed at the following website: Synqly.com/data-subprocessors

ANNEX IV

UK ADDENDUM TO EU STANDARD CONTRACTUAL CLAUSES PART 1:

TABLES

Table 1:Parties

Start Date	Effective the date of the execution of the Addendum	
Parties	The Parties Exporter (who sends the Restricted Transfer) As listed in Annex I	Importer (who receives the Restricted Transfer)As listed in Annex I
Party Details	As Listed in Annex 1	As Listed in Annex 1
Key Contacts	As Listed in Annex 1	As Listed in Annex 1

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the approved EU SCCs agreed to in the Addendum to which this UK Addendum is appended to, including the Appendix Information.

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 SCCs (other than the Parties), and which for this UK Addendum is set out in Annex 1

A: List of Parties: See Annex I Annex 1
B: Description of Transfer: Annex I
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Annex II
Annex III: List of Sub processors: Annex III

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum: ☒ Importer ☒ Exporter ☐ neither Party

PART 2: MANDATORY CLAUSES "Mandatory Clauses"

“Mandatory Clauses”	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 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 of those Mandatory Clauses.
