DIGITAL ON-DEMAND DATA PROCESSING ADDENDUM

This is the Data Processing Addendum of TD SYNNEX Belgium B.V. - Tragel 47, 9300 Aalst, Belgium hereinafter being referred to as "TD SYNNEX" or "Processor"

You, our Business Partner, are hereinafter referred to as "Controller" or "Business Partner" Together referred to as "the Parties"

By placing orders via Digital On-Demand and using the Digital On-Demand functionalities involving any processing on behalf by TD SYNNEX, you agree to this Data Processing Addendum ("DPA") and its referenced DPA Exhibit(s).

This DPA and DPA Exhibit(s) referenced herein apply to the Processing of Personal Data by TD SYNNEX on behalf of you, our Business Partners, in connection with the provisioning of Services by TD SYNNEX as further outlined in the DPA Exhibit and the Digital On-Demand Terms, which the Parties to this DPA have concluded an agreement or agreements on or otherwise are provided in connection with the Digital On-Demand offerings (hereinafter referred to as the "Digital On-Demand Agreements").

This DPA specifies the data protection obligations of the Parties, which arise from the data processing in connection with the Digital On-Demand Agreements. It applies to all activities performed by Processor in connection with the Digital On-Demand Agreements in which any personnel of the Processor or a third party acting on behalf of the Processor may come into contact with personal data of the Controller.

1. Definitions

1.1. **"Data Protection Laws"** means all laws and regulations applicable to the Processing of Personal Data, including without limitation the laws and regulations of the EU ("European Union"), the EEA ("European Economic Area") and their member states, Switzerland and the United Kingdom.

1.2. **"DPA Exhibit"** means the DPA Exhibit under the following link, which may be updated by TD SYNNEX from time to time: http://uk.tdsynnex.com/digitalondemand/termsandconditions

1.3. "**Data Subject**" means an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.4. "**GDPR**" means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation). References to Articles of GDPR in this DPA [Art.…GDPR] shall apply only to the extent that Personal Data from Data Subjects in the EEA (European Economic Area) and Switzerland is involved – for all other relevant jurisdictions the corresponding applicable Data Protection Laws apply.

1.5. "**Instruction**" means the instructions in written or documented electronic form (incl. email), issued by Controller to Processor and directing the Processor to perform a specific action with regard to Personal Data. Instructions are specified in the Service Agreement and this DPA and may, from time to time thereafter, be amended, supplemented or replaced by Controller by separate instructions (individual instructions). Oral Instruction will be confirmed in writing without undue delay.

1.6. **"International Data Transfer"** means any processing of Personal Data outside the country where Controller is located. If Controller is located in a member state of European Economic Area and Switzerland, International Data Transfer means any processing outside EEA and Switzerland.

1.7. "**Personal Data**" means any information relating to an identified or identifiable natural person which the Processor processes on behalf of the Controller.

1.8. "**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data that is governed by applicable Data Protection Laws, 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.

1.9. **"Represented TD SYNNEX Affiliate(s)"** means the TD SYNNEX Affiliate being a contract party to this DPA and SCCs and represented by TD SYNNEX signatory.

1.10. **"Standard Contractual Clauses" or "SCCs"** means the agreement executed by and between Controller and Processor attached hereto as Exhibit 2, or other similar documentation required by applicable Data Protection Laws, for the international transfer of Personal Data to ensure an adequate level of data protection, pursuant to the European Commission's decision (C (2010)593) of 5 February 2010 or other applicable Data Protection Laws.

1.11. **"TD SYNNEX Affiliate(s)"** means a legal entity including its legal successors directly or indirectly owned or controlled by TD SYNNEX Corporation for so long as such ownership lasts. Ownership or control shall exist through direct or indirect ownership entitling the holders to vote for the election of directors or persons performing similar functions.

1.12. **"Third Country"** means a country which is not a member state of the European Union, European Economic Area or is not the subject of a finding of adequacy by the European Commission pursuant to Art. 45 GDPR.

2. Scope

2.1 This DPA applies to the Processing of Personal Data by Processor on behalf of Business Partner being the Controller for the Personal Data. It applies as well if Business Partner in relation to Business Partner´s Customers or Customers´ End Users (hereinafter both further referred to as "Clients") is processing personal data in connection with TD SYNNEX´s services. Business Partner obtained all necessary authorizations of the relevant Client(s) to engage TD SYNNEX as Business Partners´ sub- processor to Process Client Personal Data as set out in this DPA. Business Partner will maintain at all times an uptodate record of each Client on whose behalf Business Partner is processing including name, contact details and data privacy officer. All notices, information and communication in connection with this DPA and the related Services will be solely provided by TD SYNNEX to Business Partner who is obliged to forward the information to the Clients, where legally required. Business Partner exercises all rights of their Clients with regard to the Services on their behalf and obtains all necessary permissions with regard to the processing and this DPA.

2.2. Nature, purpose and subject matter of Processing shall be specified in the Digital On-Demand Agreements, where applicable the scope of work, as further defined and described in the DPA **Exhibit** or in the relevant Service description where applicable. Categories of Data Subjects, types of Personal Data, Special Categories of Personal Data and the processing activities are further specified in the DPA **Exhibit** (Details of the Processing) to this DPA or otherwise are set out in the applicable DPA Exhibit for a Service. The duration of the Processing corresponds to the duration of the Service, unless otherwise stated in Exhibit 1.2 unless left intentionally blank, the DPA Exhibit or the respective DPA Exhibit for a Service.

2.3. Any changes in the Processing are subject to Controller's Instruction or the agreement of the Parties in writing or in a documented electronic form (incl. email) and shall be deemed an amendment to DPA Exhibit. Parties shall notify to each other the point of contact for any issues related to data protection arising out of or in connection with this DPA.

3. Obligations of Processor

3.1. Processor shall process Personal Data only in accordance with the Digital On-Demand Agreements, this DPA and within the scope of Controller's Instructions, unless required otherwise by applicable Data Protection Laws to which the Processor is subject. In such case the Processor shall inform the Controller prior to Processing of that legal requirement, unless that law prohibits such information on important grounds of public interest. Instructions not foreseen in or covered by the Service Agreement initially shall be treated as requests for changes to the Service Agreement.

3.2. Processor shall inform the Controller without undue delay if Processor is of the opinion that an Instruction received from the Controller is in violation of any Data Protection Law, and/or in violation of contractual duties under the Digital On-Demand Agreements or this DPA. Processor is entitled to suspend the implementation of such Instruction until it is examined by the Controller and confirmed or changed as a result.

3.3. Processor shall not use Personal Data received in connection with this DPA for any other purposes, in particular for own purposes. Personal Data shall not be transferred to or access be granted to any third party without Controller´s prior approval.

3.4. Processor shall forward to Controller without undue delay any requests where Processor is able to correlate the data subject to Controller, based on the information provided by the Data Subject, for exercising the Data Subject's rights laid down in applicable Data Protection Laws, including without limitation Articles 12-22 GDPR.

3.5. Processor shall assist Controller insofar as reasonably possible, in ensuring compliance with the obligations pursuant to Articles 32-36 GDPR taking into account the nature of processing and the information available to Processor. Processor´s assistance under 3.4 and 3.5 may be subject to reasonable charge unless Processor´s assistance is already addressed in the Service Agreement accordingly.

3.6. Processor shall inform Controller without undue delay of any inquiry, complaint, inspection or action ("action") of a relevant supervisory authority or other governmental body relating to either Processor's or Controller's compliance with applicable Data Protection Laws. Processor shall present upon request to the Controller such "action" and shall provide assistance as necessary to enable the Controller to respond accordingly. For the avoidance of doubt, Processor shall not respond to any such inquiry, complaint, notice or other communication without the prior written consent of Controller.

3.7. Processor will notify Controller as soon as possible and as far as permitted by law to do so, of any access request for disclosure of data which concerns the Personal Data (or any part thereof) by any governmental or other regulatory authority, or by a court or other authority of competent jurisdiction. If permitted to do so by law, Processor shall not disclose or release any Personal Data in response to such request served on Processor without first consulting with and obtaining the written consent of Controller. Where Controller's Personal Data becomes subject to search and seizure, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while being processed, Processor shall inform Controller without undue delay.

3.8. Controller shall retain title as to any carrier media provided to Processor as well as any copies or reproductions thereof. Processor shall store such media safely and protect it against unauthorized third-party access.

3.9. Processor shall ensure that Processor´s personnel is only entrusted with Processing Controller's Personal Data on a need-to-know basis, after being familiarized with and trained on the Data Protection Laws relevant for their work and having committed themselves to confidentiality or being under an appropriate statutory obligation of confidentiality. The confidentiality undertaking shall continue after the termination of this DPA and termination of any employment agreements.

3.10. Processor shall, at the choice of Controller, delete or return all Personal Data to Controller upon termination or expiry of the Digital On-Demand Agreements, and delete existing copies unless EU or member state law requires storage of the Personal Data.

4. Technical and Organizational Security Measures and Data Breach

4.1. Processor shall structure Processor's internal corporate organization to ensure compliance with the specific requirements of the protection of Personal Data. Processor shall implement and periodically review and verify to have implemented and maintained appropriate technical and organizational measures ("TOMs"), taking into account the state of the art, to ensure a level of security appropriate to 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.

4.2. TOMs are set forth in Exhibit 1.4 to this DPA and may be amended in the specific service descriptions.

4.3. TOMs are subject to technical progress and further development. Processor reserves the right to modify the measures and safeguards implemented, provided, however, that the level of security shall not be less protective than initially agreed upon. Any substantial security-related decisions on the organization of data processing and the applied procedures shall be agreed with Controller.

4.4. Processor maintains adequate state of the art security incident management and procedures. Processor will notify Controller in writing without undue delay after Processor becomes aware of any breach ("Data Breach") of this DPA (including the Standard Contractual Clauses (if any) and Controller´s Instructions) or of Data Protection Laws, leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data transmitted, stored or otherwise processed by

Processor or its Sub-processors. Processor shall make reasonable efforts to identify the cause of such Data Breach, take steps as necessary and appropriate in order to remediate the cause of such an incident in due time, to the extent the remediation is within Processor's or its Sub-processor's control. Processor shall reasonably assist Controller in ensuring compliance with its obligations relating to Data Breach notifications. Processor will not make any statement or notification to any Data Subject, supervisory authority or otherwise relating to such breach without the prior written approval of Controller.

Processor shall provide assistance with any obligation of Controller under applicable Data Protection Laws to document any Data Breach as reasonably requested by Controller.

5. Obligations of Controller

5.1. Controller remains the controller of the Personal Data within the meaning of applicable Data Protection Laws and has the sole right to give the Processor instruction with regard to the Processing of the Personal Data. The Processor recognizes that it is not allowed to use nor Process the Personal Data for its own account.

5.2. Controller shall be solely responsible for complying with the statutory requirements according to applicable Data Protection Laws relating to the lawfulness of Processing and the rights of Data Subjects. Based on such responsibility, Controller shall be entitled to demand the rectification, deletion, blocking and making available of Personal Data during and after the term of the Service Agreement.

5.3. Controller shall, upon termination or expiration of the Digital On-Demand Agreement and by way of issuing an Instruction, stipulate the measures to return Personal Data carrier media or to delete stored Personal Data.

5.4. Controller will notify Processor without undue delay of any errors or irregularities it gains knowledge of in connection with the Processing of Personal Data by the Processor.

6. International Data Transfer

6.1 Third country (ies) where Processor will Process Personal Data shall be set forth in the DPA Exhibit.

6.2 Any International Data Transfer is subject to an adequate Data Transfer Mechanism as to the extent this is required by applicable Data Protection Laws.

6.2.1 If Processor is located in a Third Country and Controller is established inside the EEA, or Switzerland and to the extent legally required, the SCCs shall be an integral part of this DPA amended in Exhibit 2: Processor agreeing to this DPA herewith is agreeing to the SCCs as Data Importer. Controller by agreeing to this DPA is also agreeing to the SCCs as Data Exporter on its own behalf and/or – where applicable - on behalf of and herewith duly representing its Clients.

6.2.2 If Processor and Controller are located in the EEA or Switzerland and Processor engages with a Sub-processor located in a Third Country, 8.5 shall apply.

6.3 If the Data Transfer Mechanism identified by Processor is no longer recognized as a valid transfer mechanism or in case of a change in any applicable Data Protection Laws relating to the country(ies) where an adequate level of data protection exists, the Parties will agree on an alternative solution permitting the Processor to continue to Process the Personal Data in said country/countries.

7. Documentation and Audit Obligations

7.1 Processor shall make available to Controller, or an authorized third party acting on Controller's behalf, on request all information necessary to demonstrate compliance with this DPA and applicable Data Protection Laws and in particular, the execution of the Technical and Organizational Measures and shall allow for and contribute to reviews and audits as stipulated below, including inspections (to the extent inspections are mandatorily required by applicable law or by the authorities) conducted by Controller or auditor mandated by Controller.

7.2. For the above purpose, Controller may

7.2.1. request information from Processor; and

7.2.2. request current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor) and/or

7.2.3. personally audit Processor where the information provided in line with 7.2.1. and 7.2.2. have not provided sufficient evidence of Processor´s compliance and to the extent an audit obligation mandated by applicable law cannot be satisfied otherwise.

7.3. Where personal audits and - on individual bases - inspections by Controller are a mandatory requirement, such audits and inspections will be conducted at Controller´s cost after consultation with the Processor, during regular business hours, without interfering with Processor's operations and upon reasonable prior notice. Processor may determine that such audits and inspections are subject to the execution of a confidentiality undertaking protecting the data of other customers and the confidentiality of the technical and organizational measures and safeguards implemented. Processor shall be entitled to rejecting auditors which are competitors of Processor.

7.4. Controller shall inform Processor without undue delay about any errors or irregularities detected during an audit.

7.5. Processor will provide assistance in connection with audits of any competent supervisory authority to the extent such audit relates to the processing of Personal Data by the Processor under this Agreement as reasonably requested by the Controller.

7.6. Processor shall have adequate audit provisions included in its agreements with sub-processors.

7.7. Processor shall be entitled to requesting a reasonable remuneration for Processor's support in conducting inspections and audits apart from 7.2.1. and 7.2.2. or as otherwise agreed. Processor's time and effort for inspections shall be limited to maximum one day per calendar year, unless agreed upon otherwise.

8. Subcontractors

8.1. Processor may only involve sub-processors with prior written authorization of Controller. Controller herewith authorizes Processor to a) retain other TD SYNNEX Affiliate(s) and b) either directly or via TD SYNNEX Affiliates engage other processors for carrying out specific processing activities on behalf of Controller ("Sub-processor").

8.2. Processor shall make available to Controller the current list of Sub-processors for the Services identified in the DPA Exhibit or otherwise the respective DPA Exhibit for a Service and shall inform Controller of any new assignments or replacements of Sub-processors in writing (incl. email or documented electronic form).

8.3 Controller shall be entitled to object to a subcontractor notified by Processor within 30 days of time and for materially important reasons. Otherwise Controller shall be deemed to have approved such new assignment or change. Where a materially important reason for such objection exists, and failing an amicable resolution of this matter by the parties, Controller shall be entitled to terminating the Service Agreement for the concerned service.

8.4. Processor shall select Sub-processors considering the suitability for fulfilling the required technical and organizational measures.

8.5. To the extent applicable to the nature of the areas of work provided by Sub-processor, Processor shall enter into written agreements with each Sub-processor containing data protection obligations in line with applicable Data Protection Laws, especially Art. 28 GDPR, being not less protective than those stipulated in this DPA. Such contract shall in particular provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of applicable Data Protection Laws and this DPA.

8.6. If Processing by a Sub-processor involves an international data transfer, Processor shall ensure that an adequate level of data protection exists or is created through an appropriate Data Transfer Mechanism. Where Processor enters into Standard Contractual Clauses with Sub-processors as a safeguard mechanism, Controller, by agreeing to this DPA, is also agreeing on its own behalf and/or on behalf of and duly representing its Clients as altogether "Data Exporters" to the SCCs being executed and to be executed (where applicable) by TD SYNNEX with Sub-processors and future Sub-processors.

8.7. Processor shall remain fully liable to Controller for the performance of Sub-processor's obligations to the same extent Processor would be liable if performing the services itself. Processor shall examine the Sub-processor's compliance with its data protection obligations and document the results of such examinations. The results shall be made available to Controller upon request.

8.8. All relevant documents, including sub-processing agreements and SCCs shall be made available to Controller upon request. Processor may remove or blacken all commercial information, or clauses unrelated to Data Protection Compliance beforehand.

8.9. Sub-sub processing shall be subject to the requirements of this Clause 8.

9. Liability

9.1. To the extent Personal Data processed hereunder falls under the scope of GDPR, Processor and Controller shall be liable to data subject in accordance with Article 82 of the GDPR.

9.2. The limitation of liability set out in the Digital On-Demand Agreements shall apply to the Parties' obligations to each other under this DPA unless statutory provisions explicitly request otherwise or as otherwise stipulated herein.

Parties shall be liable to each other only in case of intent or gross negligence of a Party, its legal representatives or vicarious agents. In countries where the liability for violation of material contractual obligations may not be excluded as such, compensation for damages resulting out of violation of material contractual obligations shall be limited to damages and loss typically foreseeable at the conclusion of the contract. The aforementioned limitations apply as well to consequential loss or indirect losses or loss of profit, but not to claims for damages arising from injury to life, body or health, or other mandatory provisions. Processor's aggregated liability to Controller under this DPA shall in any way not exceed the amount of fees paid for the relevant services in a 12 months period preceding an incident or violation.

10. Confidentiality

Each Party shall keep Confidential Information confidential and shall not disclose it, except (i) as required in this DPA or Parties' instruction, (ii) as required by law, (iii) in response to a competent authority or regulatory or government agency, and (iv) for disclosures to its employees, agents and contractors that are bound by confidentiality on a need-to-know basis.

Each Party may disclose the terms of this DPA to a data protection regulatory authority to the extent required by applicable law or regulatory authority, such as in course of notifications or approvals.

11. Place of jurisdiction and applicable law

This Agreement is subject to the laws of the country where the Processor is established. The Parties exclusively submit to the courts of the seat of the Processor.

12. Term

12.1. This DPA enters into force when Digital On-Demand Agreements are signed by the Parties and remains in force for the same term as the Digital On-Demand Agreements. If this DPA is covering more than one Digital On-Demand Agreement and/or service as to DPA **Exhibit**, the term of the DPA will follow the term of the respective Digital On-Demand Agreements and/or service.

12.2. Notwithstanding the term of this DPA, Processor will continue to protect Personal Data in accordance with the terms of this DPA until all Personal Data is deleted or otherwise not accessible anymore by Processor. Should provisioning of services proceed after the term of the Digital On-Demand Agreements or service has ended, the provisions of this DPA shall continue to apply to this further provisioning of services for the entire duration of the processing activity.

13. General

13.1. The invalidity of a provision of this DPA shall not affect the validity of the remaining provisions. If a provision proves to be invalid or unenforceable, the Parties shall replace it by a new provision which approximates the intentions of the Parties as closely as possible.

13.2. None of the Parties may assign or transfer any of the rights or obligations under this DPA without the prior written consent of each of the other Parties' authorized representative.

13.3. Any changes to this DPA and its attachments/Schedules, and any side agreements, must be made in writing. This also applies to the waiver of this written form clause itself.

13.4. Parties shall amend, modify or replace this DPA or any of its Exhibits if required by applicable law or jurisdiction in due time after being aware of such mandatory requirements.

13.5. In the event of any conflict between the terms of the Digital On-Demand Agreements and this DPA, the terms of this DPA shall prevail. Where Standard Contractual Clauses apply, the terms of this DPA are not intended to amend or modify the Standard Contractual Clauses but provide clarity in terms of processes and procedures for complying with the Standard Contractual Clauses. In the event of any

conflict between the terms of this DPA and the provisions of the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

14. This Agreement consists of this DPA and

Exhibit 1.1 – Exhibit 1.3 left intentionally blank
Exhibit 1.4 Technical and Organizational Measures
Exhibit 2 Standard Contractual Clauses - left intentionally blank (only applicable when processing TD entity is located outside EEA and Switzerland – non Eu data transfer on first level)

EXHIBIT 1 to DPA

Exhibit 1.1 to Exhibit 1.3 left intentionally blank

EXHIBIT 1.4 – Description of TD SYNNEX´s Technical and organizational measures

TD SYNNEX as a data processor ensures that the processing of Personal Data on behalf of the data controller is compliant with legal and regulatory requirements. To help the data controller understand the technical and organizational measures applied, TD SYNNEX is self-assessing systems and services involved in data processing and sharing the following security controls implemented to demonstrate compliance with data protection laws/regulations.

Organizational security controls

Personal Data protection is ensured through commitment and accountability:

1. Data Protection and Privacy related responsible individuals for ensuring information security, incident response and data privacy within the company are identified and roles & responsibilities clearly defined. An email address (or a generic email when applies) will be provided for contacting information security, incident response and data privacy.
2. Periodic technical and organizational security controls assessments/audits are conducted as part of the overall TD SYNNEX audit planning to ensure compliance with privacy and data protection laws and regulations.
3. TD SYNNEX as data processor extends the assessment to any sub-processor(s) in scope, ensuring they adhere to terms and conditions no less restrictive than those imposed to the data processor.
4. TD SYNNEX takes the following measures to ensure the confidentiality of data and information processed by its employees and contractors:
    a. NDA signed which includes explicit understanding of risks and responsibilities of Personal Data processing.
    b. Adherence and acceptance of the information security, data protection and other related corporate policies (accountability).

Physical security controls

5. TD SYNNEX takes appropriate measures to ensure the physical security of the systems and Personal Data processing environments, including but not limited to the following:
    a. High availability based on local threats including but not limited to natural disasters, flooding, landslip, etc.
    b. Fire prevention measures and climatic conditions assurance (temperature, humidity and static electricity)
    c. Access to systems by personnel is controlled and auditable
    d. Data Center (DC) environments are segregated from other business areas by specific physical access controls
    e. Visitor process in place and published, and visitor log maintained
    f. Visitors to the DC environment are escorted at all times

Access controls

6. TD SYNNEX maintains access controls appropriate to the environment and nature of the services supplied including but not limited to:
    a. All users, including administrator level users have a unique User ID
    b. Strong passwords are enforced (min. 8 characters, 1 capital, 1 numeric, 1 special character)
    c. Password recovery method is secure (password request link through corporate email or similar)
    d. Accounts are locked after several unsuccessful login attempts
    e. Unused accounts are disabled after a defined period of inactivity
    f. Access to information systems is restricted according to the role of the individual (need to know) g. Privileged access is reviewed regularly
    h. More stringent access controls for administrator access are implemented

7. Personal Data is secured from unauthorized viewing and access. Only authorized users with necessary business need to access to Personal Data will have related access rights.
    a. Access rights are formally requested and approved based on business need to know
    b. Access rights to Personal Data are revoked after contract termination or default time expiration

8. Access logs are stored and available upon request to be reviewed
    a. Access to Personal Data is formally audited and tracked, where supported by the applications
    b. Access logs are stored in a centralized platform

9. Only authorized users with necessary business need to access systems involved in Personal Data processing have privileged access rights.
    a. Privileged access rights to systems processing Personal Data are formally requested and approved based on business need to know
    b. Privileged access rights to systems processing Personal Data are revoked after contract termination or role change
    c. Users with privileged access rights to systems involved in Personal Data processing are formally reviewed regularly to ensure user´s access rights are aligned with business needs

10. Privileged access logs are stored and available upon request to be reviewed
    a. Privileged access to systems processing Personal Data is formally tracked
    b. Privileged access logs are stored in a centralized platform

System security controls

11. Computer systems where Personal Data processing takes place are protected following "defense in depth" principles. TD SYNNEX implements appropriate measures to ensure the security of the relevant Infrastructure including but not limited to:
    a. Use of firewalls and ACLs on routers and switches to isolate networks (VLANs, VRFs, VPNs) and secure zones
    b. Secure communications between devices and management systems (privileged access or administrator access)
    c. Operating system configuration is appropriately hardened: Services, applications and ports not used are disabled; guest accounts are removed or disabled; default and vendor supplied passwords are changed
    d. The most recent security patches are installed on the system as soon as feasible after following a test
    e. Anti-virus software is installed and regularly updated; scans are run at regular intervals
    f. Appropriate measures are in place to handle Denial of Service attacks
    g. Appropriate measures are in place for intrusion detection and/or protection

h. Systems and applications are monitored for relevant vulnerability alerts
i. Systems are configured to store security relevant logs
j. Systems clocks are synchronized using time synchronization technology
k. Systems and processes used for test and development activities are segregated from production systems
l. Changes to production systems are performed through a formal process with testing and approvals

12. TD SYNNEX ensures that the internal systems and infrastructure are contained within a dedicated logical network (such as VLAN, VRF or VPN). These networks consist of the systems dedicated to delivery of a secure data processing facility and segregated/isolated from the Internet and non-trusted networks.
    a. Externally-facing components are logically segregated from backend components which are not intended to be publicly accessible (e.g. databases and internal services)
    b. Externally-facing components are hardened and protected to resist malicious attack and monitored so that any anomaly can be detected

13. TD SYNNEX´s devices (involved in Personal Data processing) which can connect to the internet do so via a secure internet gateway or proxy service which is configured to perform anti-malware scanning, filtering and monitoring and act as a protective barrier for these devices.

14. For forensic purpose, TD SYNNEX ensures an automated audit trail is implemented for all system components involved in Personal Data processing to reconstruct the following:
    a. Individual accesses and actions taken on systems involved in Personal Data processing
    b. Invalid access attempts, access to audit trails and enabling/disabling of audit log capabilities

15. Relevant TD SYNNEX infrastructure is scanned regularly to identify the presence of security vulnerabilities, unpatched systems or misconfiguration issues. Security vulnerabilities are fixed in a timely manner: critical and high vulnerabilities are usually fixed within 1 month, moderate/medium within 3 months, low within 1 year.

16. TD SYNNEX ensures any project development and software development integrates 'privacy by default' and 'privacy by design' procedures and checks in order to be compliant with laws and regulations.

    a. Vulnerability scans are performed and fixed before going live
    b. Privacy checklist will be applied to identify non-compliance issues and gaps will be fixed before going live

17. Vulnerability scan results are stored to be able to provide proof that testing has been conducted and required fixes are applied, within the required timescales as documented.

Data at rest security controls

18. TD SYNNEX ensures that no equipment personally owned by its employees, (including contractors, temporary employees and agency workers) is used to store or process any Personal Data related to data controller, or when required that requires specific approval and data protection and access controls are enforced through MDM tool.

19. Personal Data is not stored on removable media without explicit approval, and when approved is to be encrypted and deleted from the removable media as soon as practically possible.

20. Personal Data is stored in an encrypted way on servers and clients such as PC, laptop, mobile, wherever technically feasible.

a. Full disk encryption applied to end-point devices handling Personal Data (PC, laptop, mobile, tablet)
b. Removable media containing Personal Data encryption is enforced by Cybersecurity and Acceptable Use Policy)
c. Media containing backups is encrypted before being transferred to secure off-site storage locations

21. TD SYNNEX ensures that any equipment containing Personal Data to be re-used will be cleaned (delete containing data) securely in such a way that the recovery of any information is impossible.

22. TD SYNNEX ensures that any equipment containing Personal Data that will not be re-used is physically destroyed in such a way that the recovery of any information is impossible. A proof of destruction process is kept and provided upon request.

Data in transit security controls

23. The discussion of Personal Data with unauthorized persons either inside or outside the company is not allowed. This includes (not limited to) social networking sites, blogs, forums, instant messaging, etc.
    a. Whether personal data is sent via email to external email accounts is encrypted using an approved mechanism
    b. Use of personal email involving TD SYNNEX or data controller Personal Data is not allowed

24. Connectivity between TD SYNNEX's systems and any third party (subcontractor) or the data controller which involves processing of personal data is implemented via secure links with Personal Data protected by secure encryption.

25. When remote access to corporate networks or Personal Data processing systems via public or non-trusted networks is utilized, the connections are encrypted, and the remote user is strongly authenticated.

Personal Data availability controls

26. TD SYNNEX implements appropriate security measures to ensure the availability of Personal Data processed on behalf data controller (and relevant systems involved in processing) and to ensure data subject rights are met. Such measures include but are not limited to availability of appropriate employees, data, services, software/applications, systems, networks and communications systems, and backup processes or backup data.

Incident response security controls

27. TD SYNNEX has an incident response plan and procedures in place to respond to security incidents in accordance with the data protection laws and regulations.

28. TD SYNNEX has a Personal Data breach notification procedure in place in accordance with the data protection laws and regulations.
    a. Personal Data breach is determined by accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed. It includes any event that is likely to result in a risk to the rights and freedoms of natural persons, including any lack of availability of Personal Data
    b. TD SYNNEX determines whether any security incident implies a Personal Data breach and if so, will notify data controller without unreasonable delay.

29. TD SYNNEX agrees to take necessary measures to carry out any recovery or other action necessary to remedy the security breach.
    a. IR team will take the required actions to contain, respond and restore the availability and access to Personal Data in a timely manner
    b. IR team will analyze circumstances/context to determine the cause

c. IR team will identify Personal Data involved and affected individuals

30. TD SYNNEX agrees to provide the following information (sent through a secure channel) when notifying a security incident: date and time, location, type of incident, impact, classification of Personal Data impacted, status, and outcome or action plan/taken. TD SYNNEX provides also with the information regarding to the incident and affected individuals, in order to define if the data subject notification is required.

TD SYNNEX will support data controller when a forensic analysis (more detailed investigation) is required after the security incident in compliance with data protection laws and regulations. TD SYNNEX will provide with information related to the incident, systems involved, and countermeasures applied to reduce impact

EXHIBIT 2 TO DPA - Standard Contractual Clauses

Left intentionally blank