Data Processing Addendum (DPA)

BETWEEN:

Company

and

tyntec
tyntec Ltd.
13th floor, One Angel Court
London EC2R 7HJ
United Kingdom

together the "**Parties**" and each a "**Party**",

as supplemental to the Integration Partner Agreement dated _____ entered into between the Parties (hereinafter referred to as "**the Agreement**"), the Parties wish to execute this Data Processing Addendum which shall be an integral part of the Agreement (the "**Addendum**");

1. Definitions

For the Purposes of this Addendum:

(a) "**Personal Data**", "**special categories of data**", "**process/processing**", "**controller**", "**processor**", "**data subject**" and "**supervisory authority**" shall have the same meanings given to them in the Regulation (or where the same or similar terms are used under another applicable Data Protection Law, the meanings given to such terms under such Data Protection Law).

(b) For transfers of EU Personal Data for processing in a jurisdiction other than a jurisdiction in the EU, the EEA, or the European Commission-approved countries providing 'adequate' data protection, each party agrees it will use Module Two of the Standard Contractual Clauses (SCCs) for Controller to Processor (C-to-P) transfers, which are incorporated herein by reference:

https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en

Schedule 1 to this DPA shall apply as Annex I of SCCs and Appendix 2 of Schedule 2 shall apply as Annex II of the SCCs.

1. The Clauses shall be governed by the law which is set out in the Agreement (Clause 17 and 18 (b).
2. In Clause 9, Option (b) applies.

(c) "**Data Protection Laws**" means the Regulation, any successor thereto, and any other applicable law relating to the data protection or privacy of individuals.

(d) "**Regulation**" means Regulation (EU) 2016/679 of the European Parliament and the Council (General Data Protection Regulation).

2. Role of the Parties

The Parties agree that Company is the controller and **tyntec** is the processor of all Personal Data processed by **tyntec** on Company's behalf under the Agreement ("**Company Personal Data**"). [The details of the processing activities to be carried out by **tyntec** on behalf of Company are specified in Schedule 1]

3. Obligations of tyntec

tyntec warrants and undertakes that:

(a) it will have in place and will maintain appropriate technical and organisational security measures to protect Company Personal Data, which is transferred for the purpose of performing the works and services provided under the Agreement, against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and in particular, where the processing involves the transmission of data over a network, against all other lawful forms of processing. Having regard to the state of the art and cost of their implementation, tyntec agrees that such measures shall provide a level of security appropriate to the risk represented by the processing and the nature of Company Personal Data to be protected.

(b) it will have in place procedures so that any third party it authorises, to the extent permitted by this Addendum, to have access to Company Personal Data, including its sub-contractors, will respect and maintain the confidentiality and security of Company Personal Data;

(c) it will only collect and process the Company Personal Data specified in Schedule 1 hereto and only on behalf of Company in connection with the Agreement. The collection and the processing of the Company Personal Data by tyntec shall be in accordance with Company's documented instructions and this Addendum and within the scope and for the purposes of the works and services provided under the Agreement, unless otherwise required by European Union or European Member State law to which tyntec is subject;

(d) it will identify to Company a contact point within its organisation authorised to respond to enquiries concerning processing of Company Personal Data and will keep a record of all processing activities carried out on behalf of Company;

(e) it will cooperate in good faith with Company concerning all enquiries regarding the processing of Company Personal Data within a reasonable time.

(f) Processor shall make available to Controller all information necessary to demonstrate compliance with Article 28 GDPR and this Addendum. Processor shall allow for and contribute to audits, including inspections, conducted by Controller or an auditor mandated by Controller. Audits may be conducted upon reasonable prior notice, during normal business hours, and shall not unreasonably interfere with Processor's operations. The audit costs shall be borne by the Controller.

(g) Processor shall assist Controller in fulfilling its obligations relating to data protection impact assessments and prior consultations with supervisory authorities, taking into account the nature of processing and information available to Processor.

(h) Processor shall immediately inform Controller if, in its opinion, an instruction infringes the GDPR or other applicable data protection laws. Processor shall not be obliged to follow such instruction until it has been confirmed or modified by Controller.

(i) it will within 48 hours notify Company if it becomes aware of:

  (i) any legally binding request for disclosure of Company Personal Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

  (ii) any actual or suspected security breach, accidental or unauthorised access or unlawful processing, misappropriation loss of, damage to or destruction of or other compromise of the security, confidentiality, or integrity of Company Personal Data processed by tyntec or a sub-contractor (**"Security Breach"**); or

  (iii) any complaint, communication or request received directly by tyntec or a sub-contractor from a data subject relating specifically to data under the Agreement without responding to that request, unless it has been otherwise authorised to do so by Company, in which case, it shall provide Company with full co-operation and assistance in relation to any such complaint or request and will not respond directly to the data subject without receiving Company's prior written approval to conduct any such direct communication;

(j) upon discovery of any Security Breach, it shall:

  (i) immediately take action to prevent any further Security Breach; and

  (ii) provide Company with full and prompt cooperation and assistance in relation to any notifications that Company is required to make as a result of the Security Breach;

Notice of any Security Breach shall be made to: _____.

(k) it shall ensure its employees are informed of the confidential nature of Company Personal Data and are obliged to keep such Company Personal Data confidential; have undertaken training relating to handling personal data; and are aware both of tyntec's duties and their personal duties and obligations under this Addendum;

(l) it shall not disclose Company Personal Data whether directly or indirectly to any data subject, person, firm, or other entities without the written consent of Company except to those of its employees who are engaged in the processing of the data and are subject to the binding obligations referred in clause (i) above, to other Company entities at Company's request or as otherwise provided for in this Addendum;

(m) Processor shall not act on data subject requests directly. Processor shall forward any request received from a data subject to Controller without undue delay. Processor shall only delete or modify personal data upon documented instruction from Controller, unless it is otherwise required or allowed under law to keep such data.

4. International Data Transfers

1. No Company Personal Data processed within the European Economic Area (the **"EEA"**) by tyntec pursuant to the Agreement shall be exported outside the EEA without adequate safeguards applied by tyntec in accordance with laws.
2. tyntec agrees to comply with the C-to-P Transfer Clauses in its capacity as the processor whereby Company will be regarded as the Data Exporter and tyntec will be regarded as the Data Importer.
3. The C-to-P Transfer Clauses may be varied or terminated only as specifically set out in the C-to-P Transfer Clauses.
4. In the event of inconsistencies between the provisions of the C-to-P Transfer Clauses and this Addendum, the Agreement or other agreements between the Parties, the C-to-P Transfer Clauses shall take precedence. The terms of this Addendum shall not vary the C-to-P Transfer Clauses in any way.
5. In the event that the C-to-P Transfer Clauses are amended, replaced or repealed by the European Commission or under Data Protection Laws, the Parties shall work together in good faith to enter into any updated version of the C-to-P Transfer Clauses or negotiate in good faith a solution to enable a transfer of Company Personal Data to be conducted in compliance with Data Protection Laws.

5. Liability

The limitation of liability in the Agreement applies to this Addendum except where such limitation is prohibited under applicable data protection laws.

6. Subcontracting

tyntec shall not subcontract any of its processing operations performed on behalf of Company under the Agreement without the prior written consent of Company. Where tyntec subcontracts its obligations under this Addendum, with the consent of Company, it shall do so only by way of a written agreement with the sub-contractor which imposes the same obligations on the sub-contractor as are imposed on tyntec under this Addendum. Where the sub-contractor fails to fulfil its data protection obligations under such written agreement tyntec shall remain fully liable to Company for the performance of the sub-contractor's obligations under such agreement and upon request it shall promptly send a copy of any agreement it concludes with a sub-contractor under clause 7 below relating to Company Personal Data to Company.

7. Allocation of costs

Notwithstanding anything in contrary in this Addendum, each Party shall perform its obligations under this Addendum at its own cost.

8. Termination

1. In the event that tyntec is in breach of its obligations under this Addendum, or the Agreement, then Company may temporarily suspend the transfer of Company Personal Data to tyntec until the breach is repaired.

2. In the event that:

   (a) the transfer of Company Personal Data to tyntec has been temporarily suspended for longer than one month;

   (b) compliance by tyntec with this Addendum would put it in breach of its legal or regulatory obligations in the country where tyntec exists;

   (c) Tyntec is in substantial or persistent breach of any warranties or undertakings given by it under this Addendum; or

   (d) a petition is presented for the administration or winding up of tyntec, which petition is not dismissed within the applicable period for such dismissal under applicable laws; a winding up order is made; a receiver is appointed over any of its assets; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs;

   then Company, without prejudice to any other rights which it may have against tyntec, shall be entitled to terminate the Agreement and this Addendum.

3. In the event that the Agreement terminates for any reason, this Addendum shall be immediately terminated.

9. Post-Termination Data Handling

Upon termination, Processor shall, at Controller's choice, return all personal data and delete all copies, or securely delete all personal data and certify deletion. Processor may retain only such data as required by law. Processor may retain anonymized data only if anonymization is irreversible and the data no longer constitutes personal data under GDPR.

IN WITNESS WHEREOF, each Party has caused this Addendum to be executed by its duly authorized representative as of the date first written above.

Company
Authorized signature:

_____
Date:
Name:
Title:

tyntec Limited
Authorized signature:

_____
Date:
Name:
Title:

SCHEDULE 1

DETAILS OF THE PROCESSING

1. **The subject-matter of the processing:**

   Services provided by tyntec as defined in the Agreement

2. **The duration of the processing:**

   Until the Agreement is terminated

3. **The nature and purpose of the processing:**

   Processing steps necessary to provide the services defined in the Agreement

4. **The types of personal data:**

   Phone numbers

5. **The categories of data subjects:**

   Natural persons whose personal data is processed under the Agreement

APPENDIX 1 OF SCHEDULE 2

DESCRIPTION OF THE TRANSFERS (CONTROLLER TO PROCESSOR)

This Appendix forms part of the Transfer Clauses and must be completed and signed by the Parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data Exporter

The Data exporter is Company.

Data Importer

The Data Importer is tyntec.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Natural persons and companies

Categories of data

The personal data transferred concern the following categories of data (please specify):

Data necessary to provide the services defined in the Agreement.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

N/A

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Processing of data provided by the Controller in order to provide the services defined in the Agreement.

APPENDIX 2 OF SCHEDULE 2

Technical and organisational security measures

This Appendix 2 forms part of the Transfer Clauses and summarizes the technical, organisational and physical security measures implemented by the parties in accordance with Clause 4 - OBLIGATIONS OF THE DATA EXPORTER and Clause 5 - OBLIGATIONS OF THE DATA IMPORTER of Schedule 2:

In addition to any data security requirements set forth in the Agreement, the Data Importer shall comply with the following:

Data Importer undertakes to implement, maintain, and continuously control and update, appropriate technical and organizational security measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

This includes:

1. *Preventing unauthorised persons from gaining access to data processing systems with which personal data are processed or used (physical access control); in particular, by taking the following measures:*
    - Controlled access for critical or sensitive areas
    - Video monitoring in critical areas
    - Incident logs
    - Implementation of single entry access control systems,
    - Automated systems of access control,
    - Permanent door and windows locking mechanisms,
    - Key management
    - Permanently manned reception
    - Code locks on doors
    - Monitoring facilities (e.g. alarm device, video surveillance)
    - Logging of visitors
    - Security awareness training

2. *Preventing data processing systems from being used without authorisation (logical access control); in particular, by taking the following measures:*
    - Network devices such as intrusion detection systems, routers and firewalls
    - Secure log-in with unique user-ID/password
    - Policy mandates locking of unattended workstations. Screensaver password is implemented such that if user forgets to lock the workstation, automatic locking is ensured.
    - Logging and analysis of system usage
    - Role-based access for critical systems containing personal data
    - Process for routine system updates for known vulnerabilities
    - Encryption of laptop hard drives
    - Monitoring for security vulnerabilities on critical systems
    - Deployment and updating of antivirus software
    - individual allocation of user rights, authentication by password and username and 2FA, minimum requirements for passwords, password management, password request after inactivity, password protection for BIOS, blocking of external ports (such as USB ports), encryption of data, virus protection and use of firewalls, intrusion detection systems.

3. *Ensuring that persons entitled to use a data processing system can gain access only to the data to which they have a right of access, and that, in the course of processing or use and after storage, personal data cannot be read, copied, modified or deleted without authorisation (access control to data); in particular, by taking the following measures:*
    - Network devices such as intrusion detection systems, routers and firewalls
    - Secure log-in with unique user-ID/password
    - Logging and analysis of system usage
    - Role based access for critical systems containing personal data
    - Encryption of laptop hard drives
    - Deployment and updating of antivirus software
    - Definition and management of role based authorization concept, access to personal data only on a need-to-know basis, general access rights only for a limited number of admins, access logging and controls, encryption of data, intrusion detection systems, secured storage of data carriers, secure data lines, distribution boxes and sockets.

4. *Ensuring that personal data cannot be read, copied, modified or deleted without authorisation during electronic transmission, transport or storage and that it is possible to verify and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged (data transfer control); in particular, by taking the following measures:*
    - Encryption of communication, tunnelling (VPN = Virtual Private Network), firewall, secure transport containers in case of physical transport, encryption of laptops

5. *Ensuring that it is possible retrospectively to examine and establish whether and by whom personal data have been inserted into data processing systems, modified or removed (entry control); in particular, by taking the following measures:*
    - Logging and analysis of system usage
    - Role based access for critical systems containing personal data
    - Logging and reporting systems, individual allocation of user rights to enter, modify or remove based on role based authorization concept.

6. *Ensuring that personal data processed on the basis of a commissioned processing of personal data are processed solely in accordance with the directions of the data exporter (job control); in particular, by taking the following measures:*
    - Mandatory security and privacy awareness training for all employees
    - Employee hiring procedures which require the completion of a detailed application form for key employees with access to significant personal data and, where allowed by local law
    - Periodic audits are conducted
    - Implementation of processes that ensure that Company personal data is only processed as instructed by the data exporter, covering any sub-processors, including diligently selecting appropriate personnel and service providers and monitoring of contract performance, entering into appropriate data processing agreements with sub-processors, which include appropriate technical and organizational security measures.

7. *Ensuring that personal data are protected against accidental destruction or loss (availability control); in particular, by taking the following measures:*
    - Backup procedures and recovery systems, redundant servers in separate location, mirroring of hard disks, uninterruptible power supply and auxiliary power unit, remote storage, climate monitoring and control for servers, fire resistant doors, fire and smoke detection, fire extinguishing system, anti-virus/firewall systems, malware protection, disaster recovery and emergency plan.

8. *Ensuring that data collected for different purposes or different principals can be processed separately (separation control); in particular, by taking the following measures:*
    - Internal client concept and technical logical client data segregation, development of a role based authorization concept, separation of test data and live data.