

CLAUSE XX: DATA PRIVACY

1. The following definitions are applicable to this data privacy clause ("this Clause"):
 - a) **"Data Privacy Laws"** means any national, federal, state, and provincial laws applicable to the processing of Personal Information by Supplier in the course of the performance of the Agreement. Data Privacy Laws include the GDPR (General Data Protection Regulation), as well as any similar legislation in the world such as, without limitation, (i) the Australian Privacy Principles and the Australian Privacy Act (1998), (ii) the Personal Information Protection Law (PIPL) in the People's Republic of China, (iii) the Act on the Protection of Personal Information (APPI) in Japan, (iv) the Personal Data Protection Act 2012 in Singapore, (v) the Lei Geral de Proteção de Dados (LGPD) in Brazil, (vi) the Federal or State laws in the United States of America that govern the protection of personal data such as the California Consumer Privacy Act (CCPA), (vii) the Federal Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, (viii) the Swiss Federal Act on Data Protection in Switzerland. **(As applicable)**
 - b) **"Personal Information"** means any information relating to an identified or identifiable natural person ('Data Subject') 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. For the sake of clarity, Personal Information includes, without limitation, any information qualifying as personal data under Data Privacy Laws.
 - c) **"Data Breach"** means any actual or reasonably suspected incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Information transmitted, stored or otherwise processed.
 - d) **(EU & UK Only) "SCCs"** means the **"EEA Standard Contractual Clauses"** being the standard contractual clauses approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 and the **"UK Standard Contractual Clauses"** being the International Data Transfer Addendum to the EEA Standard Contractual Clauses issued by the Information Commissioner ("ICO") under section 119A of the Data Protection Act 2018.
2. Supplier shall:
 - a) comply with all applicable Data Privacy Laws;
 - b) neither sell, nor exchange for anything of value, Personal Information processed hereunder in the course of the performance of the Agreement and thereafter;
 - c) in the performance of the Agreement, not process Personal Information for any purposes other than to provide the products and or services, and shall not disclose such Personal Information to any third party, unless requested to do so by Carrier or where mandated by law, e.g., through regulatory request for, subpoena, search warrant, or other legal, regulatory, administrative, or governmental process seeking disclosure of Personal Information. Supplier shall use commercially and legally reasonable efforts to limit the nature and scope of the required disclosure to the minimum amount of Personal Information required to comply with applicable law. Unless prevented by applicable law, Supplier shall provide Carrier with advance written notice of any such disclosure request sufficient to allow Carrier to contest legal, regulatory, administrative, or other governmental processes, and shall co-operate with Carrier to limit the scope of the disclosure to what is strictly required by law;
 - d) immediately inform Carrier if, in the Supplier's opinion, the collecting or processing Carrier Personal Information pursuant to this Clause infringes Data Privacy Laws;
 - e) notify Carrier promptly in writing of any (new) Data Privacy Laws that (i) potentially impact Supplier's ability to deliver the goods or provide the services, (ii) mandate any specific contractual terms to be added herein, or otherwise require any amendment to this Clause, or (iii) which impose any obligations on Carrier or Supplier that deviate from this Clause;

- f) where Supplier engages a sub-processor for carrying out specific processing activities (on behalf of Carrier), only do so by way of an agreement which imposes on the sub-processor, in substance, the same or equivalent data protection obligations as the ones imposed on Supplier in accordance with this Clause. Supplier shall ensure that the sub-processor complies with the obligations to which the Supplier is subject pursuant to this Clause and applicable Data Privacy Laws. Supplier shall remain fully responsible and liable for the acts and omissions of any sub-processor or other such third-party subcontractor, that processes Carrier Personal Information on Supplier's behalf in the same manner and to the same extent as it is responsible for its own acts and omissions with respect to such Carrier Personal Information. Supplier shall notify Carrier of any failure by the sub-processor to fulfil its contractual obligations;
- g) take reasonable steps to ensure the reliability of Supplier's employees, agents, representatives, subcontractors, subcontractor employees, or any other person used by the Supplier ("Supplier's Personnel") who have access to Personal Information provided by Carrier, including by (i) ensuring that all Supplier's Personnel are obligated to maintain the confidentiality of Personal Information by contractual or legal obligations of confidentiality in favour of Carrier equivalent to those in the Agreement, (ii) ensuring that Supplier's Personnel comply with the terms of this Clause, and (iii) ensuring that each member of Supplier's Personnel has undergone appropriate training in data protection, and has received the necessary instructions to process Personal Information in accordance with this Clause. In any event, the Supplier shall limit access to the Personal Information to Supplier's Personnel on a strict need-to-know basis. Supplier shall regularly review the list of Supplier's Personnel who have access to the Personal Information and immediately withdraw access, if no longer necessary;
- h) assist Carrier in ensuring compliance with the following obligations, taking into account the nature of the Personal Information processing and the information available to the Supplier. The obligation to: i) conduct a 'Data Protection Impact Assessment' – (D)PIA); ii) conduct a Transfer Impact Assessment ("TIA"); iii) consult the competent authorities prior to processing where a (D)PIA indicates that the processing would result in a high risk in the absence of measures taken by Carrier to mitigate the risk; iv) ensure that Personal Information is accurate and up to date, by informing Carrier without delay if the Supplier becomes aware that the Personal Information it is processing is inaccurate or has become outdated; v) the obligations in Article 32 GDPR and Articles 33, 36 to 38 GDPR; vi) provide a privacy notice to data subjects with whom the Supplier has direct contact unless Supplier and Carrier agree in writing that the privacy notice obligation is solely Carrier's responsibility; vii) notify Carrier immediately if Supplier receives any request from any competent authority relating to Personal Information or any complaint from an individual about the processing of Personal Information in relation to the providing of goods and/or services. Supplier shall co-operate with Carrier and, where applicable, with any competent authority to permit Carrier to respond to the correspondence or complaint; viii) the obligation (a) to notify Carrier immediately if Supplier receives any legally binding request for disclosure of the Personal Information by a law enforcement authority unless otherwise prohibited, (b) to examine such request for data and appropriately narrow and challenge requests which are not necessary and proportionate and (c) to provide assistance such as reasonable requested by Carrier;
- i) permit Carrier to take reasonable steps to monitor compliance with its obligations under this Clause, including by inspecting Supplier's data processing facilities, procedures, documentation, and by allowing and contributing to audits. Provisions of the Agreement that apply to audits of any kind, shall equally apply to any audits related to the compliance with the Data Privacy Laws or Supplier's obligations stipulated under this Clause. Without prejudice to the foregoing, Supplier shall allow for, collaborate with Carrier and contribute to audits and inspections conducted by Carrier or by an auditor mandated by Carrier, in a manner commensurate to (i) the nature and intensity of the risks associated with the processing of Personal Information under the Agreement, and (ii) the degree of urgency and the severity of the actual or suspected potential breach to the Parties' obligations under Data Privacy Laws. In general, Carrier shall give Supplier a prior notice of no less than 30 days prior to conducting such audits, unless an earlier audit/inspection is required by the applicable Data Privacy Laws or mandated by the competent authorities;

- j) provide Carrier - upon its first request - with any audit reports issued under ISO 27001, ISO 29100, SSAE 16 (or SAS 70), SSAE 18, SOC 2, OR ISAE 3402 that covers Carrier Personal Information;
 - k) implement and maintain appropriate technical, physical, organizational, administrative and contractual measures (including the use of encryption, restrictions of physical access to any locations containing Personal Information provided by Carrier, such as the storage of such records in locked facilities, storage areas, or containers, back-up and disaster recovery systems, and any such other measures as necessary or mandated pursuant to applicable Data Privacy Laws, as well as, without limitation, any security measures) to ensure a level of security appropriate to the risk, to avoid unauthorised or unlawful processing of Personal Information, as well as accidental or unlawful loss, destruction, alteration, disclosure, access, storage or any damage to Personal Information. Supplier must periodically test and re-evaluate such technical, physical, organizational and administrative security measures adopted to ensure that they remain appropriate and effective.
3. If Supplier becomes aware of any actual or suspected incident, event, risk or intrusion that, alone or in combination with other circumstances, can subsequently result in, entail or otherwise bring about a Data Breach, as defined above (hereinafter referred to as an "Incident"), Supplier shall:
- (i) take all reasonable actions and measures needed to contain and remedy the Incident, wherever possible;
 - (ii) assist Carrier and provide Carrier with any available information regarding the investigation, remediation and analysis of the Incident, unless specifically restricted to do so under applicable laws;
 - (iii) as soon as becoming aware of such Incident, notify Carrier of all available details relating to such Incident, investigate further and provide Carrier with all additional details, information or conclusions as they become available to Supplier in the course of investigating the Incident;
 - (iv) if required, provide a detailed explanation alongside the initial notification of why a comprehensive notification of the Data Breach could not be done earlier, so as to enable Carrier to engage with the supervisory authority in accordance with Data Privacy Laws, if need be through an iterative process;
 - (v) ensure that Carrier has all the information necessary to notify such Incident to the competent authorities in accordance with the Data Privacy Laws, including, without limitation, the categories and approximate number of data subjects concerned, the categories and approximate number of records concerned, the name and contact details of the contact point where more information concerning the Incident can be obtained, the likely consequences of such Incident and the measures taken or proposed by the Supplier to mitigate the potential adverse effects thereof;
 - (vi) promptly initiate, at its own costs, a full investigation into the circumstances surrounding the Incident, and make any reports or notes of the investigation available to Carrier as soon as possible;
 - (vii) fully co-operate, at Supplier's cost, with Carrier's investigation and provide any assistance requested by Carrier in order for Carrier to investigate the Incident, and possibly notify the Data Breach to the competent authority in accordance with the Data Privacy Laws;
 - (viii) not make any notification, announcement or publication or authorize any such notification, announcement or publication about an Incident (a "Breach Notice") - unless required by law or court order - without the prior written consent of and approval by Carrier of the content, media and timing of the Breach Notice. Where required to provide a Breach Notice by law or court order, Supplier shall make all reasonable efforts to coordinate with Carrier prior to providing any such Breach Notice.
4. Following termination of the Agreement, Supplier shall, at the choice of Carrier, delete all Personal Information processed on behalf of Carrier and certify that it has done so, or, return all the Personal Information to Carrier and delete existing copies unless Data Privacy Laws requires storage of the Personal Information. Until the data is deleted or returned, the Supplier shall continue to ensure

compliance with this Clause. Absent instructions and except as prohibited by law, the Supplier shall immediately destroy all Personal Information after termination or completion of the Agreement, after waiting 30 days to allow Carrier to request the return of Personal Information.

5. Pursuant to Carrier's written instructions, Supplier shall provide Carrier with the ability to purge Carrier Personal Information older than one year, or such other time period agreed upon in writing by the Parties, unless otherwise required to retain the data by applicable law.
6. **(EU & UK only)** Parties agree that the SCCs are incorporated by reference as if set forth herein. The SCCs will apply to Personal Information that is transferred from the European Economic Area or the UK, either directly or via onward transfer, to any country or recipient outside the European Economic Area or the UK that is (a) not recognized as providing an adequate level of protection for Personal Information, and (b) not covered by any other appropriate data transfer tool. If the Supplier will act as a controller, the Parties agree that Module One applies; if the Supplier will act as a processor, the Parties agree that Module Two applies. For Module Two, Option 2 for Clause 9(a) applies, and notice shall be provided no less than 30 days in advance. For both Modules, Option 2 for Clause 17 applies and the data exporter at issue shall be the relevant one. The law of Belgium shall be the governing law if the applicable EU Member State does not allow for third-party beneficiary rights. For clause 18 for both Modules, disputes shall be resolved in the courts of the EU Member State for the relevant data exporter. If there are multiple relevant data exporters, the Parties agree to jurisdiction and forum of the courts of Belgium. If there is any conflict between the SCCs and the Agreement, the SCCs shall prevail.
7. This Clause will survive the termination of the Agreement.