Additional Protections for European Personal Data Addendum

The contractual protections set out in this Addendum will apply only to Transfers of European Personal Data subject to either the GDPR and/or UK GDPR.

1. **Definitions**. For the purposes of this Addendum (Additional Protections for European Personal Data), the following capitalized terms have the meanings provided below. Capitalized terms not defined below have the meaning set forth in the Agreement.

    1.3 "**Public Body**" means any local, regional, state, national or federal law enforcement authority, regulator, government department, agency or court in any Third Country.

    2.3 "**Third Country**" means a country which is not a Member State of the EEA or the UK, and which does not benefit from an adequacy decision under Article 45 of the GDPR or UK GDPR (with respect to Transfers subject to the GDPR or UK GDPR respectively).

    3.3 "**Third-Party Request**" means any criminal, civil, or administrative subpoena, mandatory request, order, demand, warrant, or any other document requesting or purporting to compel the production of European Personal Data, including but not limited to subpoenas, warrants and orders authorized under local, regional, state, national or and federal laws or regulations or any other laws applicable to the Supplier or its Affiliates in any Third Country.

2. The commitments given in this Addendum are in each case without prejudice to the commitments given by Supplier in the Agreement and in the EEA and UK Standard Contractual Clauses, as well as those under applicable Privacy Laws.

3. Supplier warrants that neither it nor its Affiliates have taken any steps to facilitate access to European Personal Data (including systems on which European Personal Data is Processed) by any Public Body, including, without limitation, by creating back-doors or similar programming that provide a mechanism for a Public Body to access European Personal Data or changing its business processes with the express intention of facilitating access to European Personal Data. Supplier certifies that neither it nor its Affiliates are subject to laws that would require it or its Affiliates to take any of the steps referred to this Section 3.

4. If Supplier or its Affiliates receive a Third-Party Request, Supplier will attempt to redirect the Public Body issuing such Third-Party Request to request that European Personal Data directly from Visa. If this is not possible, Supplier will permit Visa to respond to the Third-Party Request directly, unless Supplier is legally prohibited from doing so. Any disclosure made by Supplier or its Affiliates in response to a Third-Party Request will be made in compliance with Privacy Laws (including the GDPR and/or UK GDPR, as applicable) and the EEA and/or UK Standard Contractual Clauses (as applicable) to the greatest extent possible.

5. Supplier will implement and maintain appropriate procedures for the assessment and handling of Third-Party Requests, which will be aligned to the requirements of Privacy Laws and this DPA, and provide training on those procedures to its Personnel.

6. Supplier will maintain accurate and up-to-date written records of all Third-Party Requests. Upon request, Supplier agrees to provide Visa with a "transparency report" regarding all requests for access to Personal Information (whether European Personal Data or otherwise) received from Public Bodies over a specified period. The report should not disclose the identity of any other client or customer of Supplier, but must detail the type of information requested and the legal power under which the request was made.

7. Supplier will ensure that its Data Protection Officer has oversight of Supplier's approach to Transfers and is involved in determining the response to any Third-Party Request for European Personal Data.

8. Upon request, Supplier agrees to cooperate with and assist data subjects seeking to exercise their rights or obtain effective redress in a Third Country in relation to a Transfer.