S&P Global Market Intelligence – Event Sponsorship Data Protection Addendum

This Event Sponsorship Data Protection Addendum ("DPA") forms part of the online terms and conditions governing event sponsorships, as referenced in the applicable Sales Order Form pursuant to which S&P Global Market Intelligence, including its applicable affiliates ("S&P"), sells an event sponsorship package to the Client (the "Agreement"), in connection with one or more events (each, an "Event").

For purposes of this DPA:

i) Capitalized terms used but not otherwise defined in this DPA have the meaning given to them in the applicable Agreement.

ii) In the event of a conflict, this DPA takes priority over the provisions of the Agreement.

1. Definitions: In this DPA, the following terms shall have the following meanings:

1.1. "**Agreement**" shall mean the online terms and conditions governing event sponsorships, as incorporated by reference into the applicable Sales Order Form.

1.2. "**CCPA**" shall mean the California Consumer Privacy Act of 2018, Cal. Civ. Code §1798.100, et seq., and its implementing regulations, as each may be amended from time to time;

1.3. "**Client**" shall have the meaning set forth in the Agreement.

1.4. "**Client Data** " shall mean personal data of data subjects who are employees and/or agents of Client including: name; job title, name of employer, office e-mail address, office physical address, office telephone number, mobile telephone number, dietary preferences and other accommodations, and support and training interactions processed by and/or for S&P for the Permitted Purpose;

1.5. "**controller**" shall mean the person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data, "**data subject**" shall mean an identified or identifiable natural person (or an identified or identifiable entity where information about an entity is protected similarly to the protection afforded to information about an individual under Data Protection Laws) and shall include corollary terms under Data Protection Law, "**personal data**" shall mean any information relating to a data subject and shall include corollary terms under Data Protection Law, and "**process**" (and its derivatives) shall mean any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means;

1.6. "**Controller-to-Controller Standard Contractual Clauses"** shall mean the standard contractual clauses (as adopted by European Commission Decision 2021/914 on June 4, 2021);

1.7. "**Event(s)**": shall mean any conference, meeting, or event in respect of which a sponsorship package is sold by S&P under the Agreement;

1.8. "**Event Media**" means photographs, audio recordings, and video recordings captured at or in connection with an Event;

1.9. "**Data Protection Law**" shall mean all applicable data protection and privacy laws, regulations, binding guidance and mandatory codes of practices issued by any authority of competent jurisdiction as may be amended, superseded or replaced from time to time;

1.10. "**Destination Jurisdiction**" shall have the meaning set forth in Section 8.2(a) below;

1.11. "**Permitted Purpose**" shall mean processing: (A) of Client Data by or for S&P or its agents (i) for managing and executing contracts with Client and in connection with the provision and/or management of the Services and/or the Event(s); (ii) to improve and develop S&P's Services, and develop new Services and offerings; (iii) as otherwise set out in S&P's Corporate Privacy Policy available at: https://www.spglobal.com/en/privacy/privacy-policy-english; (iv) as otherwise set forth in the applicable Agreement; and (v) for any other purpose as permitted under Data Protection Laws; (B) of the Registration List, by the Client in connection with the Events: (i) to contact attendees with details about programs, meetings, receptions and/or other events occurring at the Event; (ii) to contact attendees in connection with the Client's participation in the Event and, where permitted by applicable law, to send marketing communications consistent with the Event context and the Agreement; and/or (iii) for purposes S&P has explicitly approved in writing; (C) of S&P Data other than the Registration List by the Client for managing and executing contracts with S&P or its Affiliates and in connection with the applicable Agreement;

Event Sponsorship Data Protection Addendum © S&P Global Market Intelligence LLC 2026
All rights reserved

1.12. "**Personal Data Breach**" shall mean the accidental or unlawful destruction, loss, alteration or unauthorized disclosure of or access to S&P Data (as applicable);

1.13. "**Registration List**" shall mean the list containing limited business contact and attendance related personal data belonging to individuals who are registered to attend the Event, excluding personal email addresses unless the individual has expressly opted in, and shared in accordance with the Agreement;

1.14. "**Restricted Transfer**" shall mean a transfer of Client Data or S&P Data (including making personal data available by remote access or otherwise) to a jurisdiction in respect of which additional safeguards are required under Data Protection Law in order to lawfully transfer that personal data;

1.15. "**S&P Data**" shall mean (i) personal data of data subjects who are employees and/or agents of S&P including business contact information such as name; job title, name of employer, office e-mail address, office physical address; telephone number, and mobile telephone number; and (ii) the Registration List processed by and/or for Client for the applicable Permitted Purpose;

1.16. "**Security Safeguard(s)**" shall have the meaning set forth in Section 5 below;

1.17. "**Service(s)**" shall mean S&P's proprietary products and services as specified in the Agreement, as applicable;

1.18. "**Sales Order Form**" shall mean the sponsorship event statement, or any written statement of work, executed by both parties and referring to applicable event terms and conditions, detailing inter alia the Event, the fees and the sponsorship package details;

1.19. "**Standard Contractual Clauses**" shall mean the applicable standard contractual clauses as set forth herein and as may be amended from time to time, in particular to amend or replace standard contractual clauses when a regulatory authority has issued a new version or to add standard contractual clauses for an additional jurisdiction; and,

1.20. "**UK Addendum**" shall mean the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the United Kingdom Information Commissioner's Office under S199A(1) Data Protection Act of 2018, effective March 21, 2022, completed in the form available in the UK Addendum as applicable pursuant to section 8.2 of this DPA.

2. **Disclosure.** Each party acknowledges that the other party is only disclosing Client Data or S&P Data (as applicable) to the other party to process strictly for the Permitted Purpose. Client confirms that all Client Data is accurate and up to date and warrants that it has provided all information to, and obtained all consents from, the relevant data subjects as required by Data Protection Law in order to provide the Client Data to S&P.

3. **Relationship of the parties.** The parties acknowledge that (i) Client is a controller of the Client Data it discloses to S&P and S&P is a controller of the S&P Data it discloses to Client, and (ii) S&P and Client will each process such data as separate and independent controllers for the applicable Permitted Purpose. In no event will the parties process Client Data or S&P Data as joint controllers. Each party shall be individually and separately responsible for complying with the obligations that apply to it as a controller under Data Protection Law. Each party shall comply with, and not cause the other to breach, Data Protection Law in its performance or receipt of the Services. By way of clarification S&P is not a "data processor", "service provider" or "entrusted party" for or to the Client Data.

4. **Cooperation.** Client shall: (i) use all reasonable efforts to assist S&P to comply with all obligations imposed on S&P by Data Protection Law, including by providing S&P with reasonable assistance with regard to request from Data Subjects to exercise their rights under Data Protection Law or inquiries from supervisory authorities; and (ii) promptly inform S&P (and in any event within two (2) business days of receipt) at privacy@spglobal.com about the receipt of: (a) any complaints from Data Subjects, (b) any inquiries from any governmental, regulatory or supervisory authority received by Client relating to S&P, or (c) any other person or entity, alleging unlawful or unauthorized processing.

5. **Security**: Each party shall implement appropriate technical and organisational measures ("**Security Safeguards**") to protect the Client Data or S&P Data (as applicable) from: (i) accidental, unauthorized or unlawful destruction; and (ii) loss, alteration, unauthorized disclosure of, or access to the Client Data or S&P Data (as applicable). Client shall ensure that the Security Safeguards applicable to the Registration List (i) include all measures required by Data Protection Law, and (ii) are at least as protective as current practice and standards in Client's industry.

All rights reserved

6. **Event Media.** Event Media are processed by S&P and do not form part of the Registration List or Client Data shared under this DPA.

7. **Personal Data Breach.** If there is a Personal Data Breach impacting the Registration List, the Client shall notify S&P by calling US +1-866-810-0436 or + 44 207 176 7999 or emailing security@spglobal.com. Client's notification will provide S&P with (i) a detailed description of the Personal Data Breach, including the personal data and approximate number of Data Subjects concerned and the likely consequences of the Personal Data Breach; and (ii) timely information as S&P may require in order for S&P to fulfill its notice and reporting obligations under Data Protection Law.

8. **Cross-Border Transfers.**

8.1. Client will not transfer the Registration List (nor permit the transfer of the Registration List) across jurisdictional borders unless: (i) the transfer is necessary for Client to perform the Permitted Purpose; (ii) Client transfers only that S&P Data for which transfer is necessary to perform the Permitted Purposes; and (iii) Client takes the measures necessary to ensure that the transfer of S&P Data complies with Data Protection Law.

8.2. Without limiting the generality of the foregoing, Client agrees that it will:

(a) provide S&P with prior written notice of each jurisdiction to which Client will transfer (or have transferred) the Registration List (each, a "Destination Jurisdiction");

(b) for a Restricted Transfer, ensure that the Registration List receives at least equivalent protection in the Destination Jurisdiction; and

(c) if the Standard Contractual Clauses are not recognized as a lawful transfer tool for a Restricted Transfer of the Registration List:

8.2(c)(1). cooperate with S&P to identify and implement, or otherwise seek to adhere to, an alternative or additional adequate transfer tool to the extent that one is required by, and available under, Data Protection Law; and

8.2(c)(2). notify S&P of any alternative adequate transfer tool for the transfer of the Registration List upon which it intends to rely.

(d) as and when required by competent government authorities or Data Protection Law: (i) participate in periodic assessments of the adequacy of personal data protection in each Destination Jurisdiction where the Registration List is located or Processed; (ii) take all commercially-reasonable steps to supplement data protection measures (including Security Safeguards) for a Restricted Transfer as a result of a periodic assessment; and (iii) suspend cross-border transfers of the Registration List if S&P, Client or a competent government authority determines in good faith that Client's personal data protection measures or the laws of a Destination Jurisdiction can no longer ensure an essentially equivalent level of protection for the Registration List as the protection provided for in the Data Protection Law of the jurisdiction from which the personal data is transferred.

8.3. S&P may process (or permit to be processed) any Client Data in any jurisdiction where S&P has an office as set out here: https://www.spglobal.com/en/contact-us/office-locations or receive and make Restricted Transfers in relation to any Client Data, provided that it does so in accordance with Data Protection Laws, and Client may process (or permit to be processed) any S&P Data with the exception of the Registration List, in any jurisdiction where Client Data has an office or receive and make Restricted Transfers in relation to any S&P Data, provided it does so in accordance with Data Protection Law, in particular in accordance with data minimization principles.

8.4. To the extent required under Data Protection Law, the relevant Standard Contractual Clauses, completed in the form available in the UK Addendum as amended or updated by S&P (in its sole discretion) from time to time, shall apply in respect of any Restricted Transfer by either party made under the Agreement or this DPA and:

(a) shall be deemed to be populated with the details of the Client as set out in the Agreement;

(b) shall be incorporated into and made a part of this DPA; and

(c) unless other execution arrangements are agreed between the relevant parties, the execution of the Agreement shall be a deemed execution of the relevant Standard Contractual Clauses by S&P and the Client. In the event that deemed execution of the Standard Contractual Clauses is not legally sufficient under the applicable governing law of the Standard Contractual Clauses, the parties hereby agree promptly to cooperate and execute the applicable Standard Contractual Clauses.

8.5. With respect to the Controller-to-Controller Standard Contractual Clauses:

(a) Client acknowledges that all employees and/or agents of Client, customers of Client, and/or Authorized Users may be provided with the information required pursuant to clause 8.2(a) of the Controller-to-Controller Standard Contractual Clauses through S&P's Corporate Privacy Policy, which is available online at: https://www.spglobal.com/en/privacy/privacy-policy-english;

All rights reserved

(b) The Client agrees and acknowledges that S&P has provided it with relevant information for the purposes of clause 14(c) of the Controller-to-Controller Standard Contractual Clauses;

(c) The Client shall provide S&P with a copy of any assessment under clause 14(b) of the Controller-to-Controller Standard Contractual Clauses within one week after being so requested in writing by S&P;

(d) In making any assessment as to whether S&P can comply with the Controller-to-Controller Standard Contractual Clauses, the Client shall act reasonably and in good faith, based on objectively verifiable information.

8.6 Any requirement in the Standard Contractual Clauses for either party to make a notification to the other party shall be satisfied by providing notice in accordance with the service of notices provision of the Agreement.

8.7 To the extent permissible by law, the terms of the Agreement, including without limitation in relation to the parties' liability to each other, shall also apply in relation to the Standard Contractual Clauses.

8.8 If (i) S&P notifies the Client of any concern in relation to S&P's ability to comply with the Standard Contractual Clauses; (ii) Client notifies S&P of any concern in relation to Client's ability to comply with the Standard Contractual Clauses; (iii) the Client notifies S&P of its wish to exercise its right to terminate under the applicable Controller-to-Controller Standard Contractual Clauses, or (iv) S&P notifies Client of its wish to exercise its right to terminate under the applicable Controller-to-Controller Standard Contractual Clauses, the parties shall work together in good faith to resolve any issues and to use best endeavours to put in place such additional safeguards or steps that are reasonably required in order to allow Restricted Transfers to continue between them.

8.9 Each party shall perform its obligations under the Standard Contractual Clauses at its own cost, unless otherwise agreed in writing.

8.10 If the Standard Contractual Clauses are amended or replaced, the parties shall take steps to put in place any amended or replacement version between them, as required by Data Protection Law.

8.11 In the event of a conflict between the Standard Contractual Clauses and the terms of this DPA, the Standard Contractual Clauses shall prevail.

9. Registration List Obligations.

9.1. With regard to Client's Processing of the Registration List, Client warrants that it will:

(a) process the Registration List only for the Permitted Purpose and in accordance with Data Protection Law;

(b) regularly assess the Registration List for opt outs and delete the personal data of those individuals who opt out;

(c) maintain all registrations and notifications which are required under the Data Protection Law to Process the Registration List personal data;

(d) respond to any rights request from data subjects, or enquires from governmental, regulatory or supervisory authorities, received by it (subject to Clause 4 herein);

(e) ensure that any person authorized to gain access to and/ or use the Registration List is permitted to do so solely for the Permitted Purpose and is under a statutory or contractual obligation to keep such data secure and confidential;

(f) if Client becomes aware of any breach of the terms of its use of the Registration List as set out in the Agreement or this DPA, or if Client determines it can no longer meet its obligations under Data Protection Law, (i) immediately notify S&P and (ii) take such prompt action as is reasonably necessary to remedy such a breach in consultation with S&P;

(g) only retain the Registration List for as long as necessary to fulfill its obligations related to the Permitted Purposes; and

(h) indemnify, and keep indemnified, S&P and its affiliates from and against all liabilities, costs, expenses, damages, demands and losses which S&P or its affiliates may suffer or incur arising directly or indirectly from Client's failure to comply with Data Protection Law or any of its obligations under this Clause.

9.2. Client shall not disclose the Registration List to any third party, or permit any third party to access the Registration List, without the prior written consent of S&P, except to Client's employees, agents or professional advisors who need access to the Registration List, or as otherwise needed for the Permitted Purpose, and are bound by obligations of confidentiality and data protection at least as protective as those set out in the Agreement.

10. California. This Section 10 applies to S&P Data subject to CCPA.

10.1. The Parties acknowledge and agree that S&P is disclosing the S&P Data to Client only for the limited and specified Permitted Purpose.

10.2. Client shall not:

(a) retain, use, or disclose S&P Data for any purpose other than the Permitted Purpose, which for the avoidance of doubt prohibits Client from retaining, using, or disclosing S&P Data outside of the conditions of the Agreement and direct

All rights reserved

business relationship with S&P or for any other purpose;

(b) share, sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, S&P Data to another person or entity for: (i) monetary or other valuable consideration; or (ii) cross-context behavioral advertising for the benefit of a business in which no money is exchanged; or

(c) combine or update S&P Data with personal data Client receives from or on behalf of another person or entity or collects from its own interactions with a Data Subject.

10.3. Client shall (a) comply with all applicable sections of CCPA and provide the same level of privacy protection for S&P Data as required of a "business" under CCPA; (b) enable S&P to comply with consumer requests made pursuant to CCPA; and (c) notify S&P if it determines it can no longer meet obligations under Data Protection Law. Client acknowledges that S&P has the right to take reasonable and appropriate steps to help ensure that Client uses S&P Data in a manner consistent with S&P's obligations under Data Protection Law, including the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of S&P Data.

11. Survival. This DPA shall survive termination or expiry of the Agreement. Upon termination or expiry of the Agreement, S&P may continue to process the Client Data provided that such processing complies with the requirements of this DPA and Data Protection Law.

12. Updates. Notwithstanding the provisions of the Agreement, S&P may amend this DPA at any time by updating the webpage at: Privacy Policy- With Intelligence.

Event Sponsorship Data Protection Addendum © S&P Global Market Intelligence LLC 2026
All rights reserved

Standard Contractual Clauses

Definitions

(a) "**Brazil Controller-to-Controller Standard Contractual Clauses**" means the standard contractual clauses between Controllers and Controllers published by the Brazilian Data Protection Authority (ANPD) in Resolution CD/ ANPD No. 19 on August 23, 2024 and completed in the form set forth below.

(b) "**Controller-to-Cont1roller Standard Contractual Clauses**" means the standard contractual clauses between Controllers and Controllers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (module 1) and completed in the form set forth below.

(c) "**Saudi Arabia Standard Contractual Clauses**" means the standard contractual clauses published by the Saudi Data and AI Authority (SDAIA) on September 2024 based on the Personal Data Protection Law, issued by Royal Decree No. (M/19) dated 9/2/1443 AH (the "Law") and amended by Royal Decree No. (M/148) dated 5/9/1444 AH and completed in the form set forth below.

(d) "**UK Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the United Kingdom Information Commissioner's Office under S119A(1) Data Protection Act of 2018, effective March 21, 2022 and completed in the form set forth below.

Relevant Standard Contractual Clauses

For the purposes of section 8 of the DPA, the relevant Standard Contractual Clauses are as follows:

Restricted Transfer	
Criteria	**Relevant Standard Contractual Clauses**
EEA: Restricted Transfer where the origin jurisdiction of the Restricted Transfer is within the European Economic Area.	The Controller-to-Controller Standard Contractual Clauses.
United Kingdom: Restricted Transfer that is subject to Data Protection Law of the United Kingdom.	The Controller-to-Controller Standard Contractual Clauses as modified by the UK Addendum.
Switzerland: Restricted Transfer that is subject to the Swiss Federal Act on Data Protection ("FADP").	The Controller-to-Controller Standard Contractual Clauses interpreted as follows: a) The competent supervisory authority in Annex I shall refer to the Swiss Federal Data Protection and Information Commissioner (FDPIC); b) Clause 18 c shall be interpreted to permit data subjects in Switzerland to bring legal proceedings in Switzerland; and c) References to the General Data Protection Regulation should be understood as references to the FADP.
Brazil: Restricted Transfer that is subject to the Data Protection Law of Brazil.	Brazil Controller-to-Controller Standard Contractual Clauses.
Saudi Arabia: Restricted Transfer that is subject to the Personal Data Protection Law of Saudi Arabia	Saudi Arabia Standard Contractual Clauses.
Other: Restricted Transfer that is subject to the Data Protection Law of any jurisdiction not otherwise listed in this table.	The Controller-to-Controller Standard Contractual Clauses construed in light of the equivalent provisions of relevant Data Protection Law of the origin jurisdiction insofar as Data Protection Law requires, and in particular references: a) to provisions of the GDPR shall be read as being references to any equivalent provisions in the Data Protection Law of the origin jurisdiction; b) to Member States and the Union shall be read as being references to the relevant origin jurisdiction; and c) to third countries shall be read as being references to the relevant destination jurisdiction, in each case as the context requires.

Event Sponsorship Data Protection Addendum © S&P Global Market Intelligence LLC 2026
All rights reserved

Brazil Controller-to-Controller Standard Contractual Clauses

STANDARD CONTRACTUAL CLAUSES
(Resolution CD/ANPD No. 19/2024)

Section I – General Information

Clause 1. Identification of the Parties

1.1. Through this contractual instrument, the Exporter and the Importer (hereinafter referred to as "the Parties"), identified below, agree to adopt the Standard Contractual Clauses (hereinafter referred to as "Clauses") approved by the Brazilian Data Protection Authority (ANPD) to govern the International Data Transfer described in Clause 2, in accordance with the provisions of the Brazilian Legislation.

Name: S&P and its affiliates (as set forth in the Agreement or Sales Order Form) Primary address: As set forth in the Agreement or Sales Order Form Email address: privacy@spglobal.com Contact for the Data Subject: Data Privacy Officer Other information: N/A

(x) Exporter/Controller
(x) Importer/ Controller

Name: Client name as set forth in the Agreement or Sales Order Form Primary address: As set forth in the Agreement or Sales Order Form Email address: As set forth in the Agreement or Sales Order Form Contact for the Data Subject: Client contact as set forth in the Agreement or Sales Order Form Other information: N/A

(x) Exporter/Controller
(x) Importer/ Controller

Clause 2. Subject Matter

2.1. These Clauses apply to the International Data Transfers from the Exporter to the Importer, as described below.
Description of the international data transfer:

Main purposes of the transfer: The Permitted Purpose Categories of personal data transferred: Client Data and/or S&P Data (as both terms are defined in the DPA) Data retention period: As required to provide the Services Other information: as set forth in the DPA and the Sales Order Form

Clause 3. Further Transfers

3.1. The Importer may carry out further transfers of the Personal Data subject to the International Data Transfer governed by these Clauses under the conditions described below and provided that the provisions of Clause 18 are complied with.

Main purposes of the transfer: The Permitted Purpose Categories of personal data transferred: Client Data and/or S&P Data (as both terms are defined in the DPA) Data retention period: As required to provide the Services Other information: as set forth in the DPA and the Sales Order Form

Clause 4. Responsibilities of the Parties

4.1. Without prejudice to the duty of mutual assistance and the general obligations of the Parties, the Party designated below as the Controller shall be responsible for complying with the following obligations under these Clauses:

a) Responsible for publishing the document referred to in Clause 14:
(x) Exporter (x) Importer
b) Responsible for responding to data subject requests as provided in Clause 15:
(x) Exporter (x) Importer

All rights reserved

c) Responsible for reporting security incidents as provided in Clause 16:
(x) Exporter (x) Importer

4.2. For the purposes of these Clauses, if it is later verified that the designated Party under item 4.1 is acting as a Processor, the Controller shall remain responsible:

a) for complying with the obligations set forth in Clauses 14, 15, and 16 and other provisions established in Brazilian Legislation, especially in the event of omission or non-compliance by the designated Party;

b) for complying with the determinations of the ANPD; and

c) for guaranteeing the rights of the Data Subjects and for compensating for any damages caused, as provided in Clause 17.

Section II – Mandatory Clauses

Clause 5. Purpose

5.1. These Clauses serve as a mechanism to facilitate the secure international flow of personal data, establish minimum guarantees and valid conditions for carrying out International Data Transfers, and aim to ensure the adoption of appropriate safeguards for compliance with the principles of data subject rights and the data protection regime outlined in Brazilian Legislation.

Clause 6. Definitions

6.1. For the purposes of these Clauses, the definitions set forth in Article 5 of Law No. 13,709 of August 14, 2018, and Article 3 of the International Personal Data Transfer Regulation shall apply, without prejudice to other normative acts issued by the ANPD. The Parties also agree to consider the following terms and their respective meanings as outlined below:

a) Data Processing Agents: the Controller and the Processor;

b) ANPD: Brazilian Data Protection Authority;

c) Clauses: the standard contractual clauses approved by the ANPD, which are integrated into Sections I, II, and III;

d) Associated Contract: contractual instrument signed between the Parties or at least one of them and a third party, including a Third-Party Controller, which has a common purpose, connection, or dependency with the contract governing the International Data Transfer;

e) Controller: Party or third party ("Third-Party Controller") responsible for decisions regarding the processing of Personal Data;

f) Personal Data: information related to an identified or identifiable natural person;

g) Sensitive Personal Data: personal data regarding racial or ethnic origin, religious beliefs, political opinions, membership in a trade union or organization of a religious, philosophical, or political nature, data concerning health or sexual life, genetic or biometric data when linked to a natural person;

h) Deletion: removal of data or a set of data stored in a database, regardless of the method employed;

i) Exporter: processing agent located within a national territory or a foreign country that transfers personal data to an Importer;

j) Importer: processing agent located in a foreign country or an international organization that receives personal data transferred by the Exporter;

k) Brazilian Legislation: set of Brazilian constitutional, legal, and regulatory provisions regarding the protection of Personal Data, including Law No. 13,709 of August 14, 2018, the International Data Transfer Regulation, and other normative acts issued by the ANPD;

l) Arbitration Law: Law No. 9,307 of September 23, 1996;

m) Security Measures: technical and administrative measures adopted to protect personal data from unauthorized access and from accidental or unlawful situations of destruction, loss, alteration, communication, or dissemination;

n) Research Organization: public or private legal entity under Brazilian law that is nonprofit and legally constituted under Brazilian laws with headquarters and jurisdiction in the country, whose institutional mission or social or statutory objective includes historical, scientific, technological, or statistical research;

o) Processor: Party or third party, including a subcontractor, that processes personal data on behalf of the Controller;

p) Designated Party: Party to the contract designated in accordance with Clause 4 ("Option A") to fulfill, as Controller, specific obligations related to transparency, data subjects' rights, and communication of security incidents;

q) Parties: Exporter and Importer;

r) Access Request: mandatory request by law, regulation, or public authority determination to grant access to the Personal Data subject to the International Data Transfer governed by these Clauses;

s) Subcontractor: processing agent hired by the Importer without a direct link to the Exporter to process Personal Data after an International Data Transfer;

t) Third-Party Controller: Controller of Personal Data who provides written instructions for carrying out the International Data Transfer between Processors governed by these Clauses as described in Clause 4 ("Option B");

All rights reserved

u) Data Subject: natural person to whom the Personal Data subject to the International Data Transfer governed by these Clauses refers;

v) Transfer: processing modality whereby one processing agent transmits, shares, or grants access to Personal Data to another processing agent;

w) International Data Transfer: transfer of Personal Data to a foreign country or an international organization of which the country is a member; and

x) Further Transfer: International Data Transfer originating from an Importer and destined for a third party, including a subcontractor, provided it does not constitute an Access Request.

Clause 7. Applicable Legislation and ANPD Supervision

7.1. The International Data Transfer subject to these Clauses is governed by Brazilian Legislation and subject to supervision by the ANPD, including the authority to apply preventive measures and administrative sanctions to both Parties, as appropriate, as well as the power to limit, suspend, or prohibit international transfers resulting from these Clauses or an Associated Contract.

Clause 8. Interpretation

8.1. Any application of these Clauses must occur in accordance with the following terms:

a) These Clauses must always be interpreted in a manner most favorable to the Data Subject and in line with the provisions of Brazilian Legislation;

b) In case of doubt regarding the meaning of the terms in these Clauses, the meaning most aligned with Brazilian Legislation shall apply;

c) No part of these Clauses, including an Associated Contract and the provisions set out in Section IV, may be interpreted with the objective of limiting or excluding the responsibility of any of the Parties in relation to obligations provided for in Brazilian Legislation; and

d) The provisions of Sections I and II shall prevail in the event of a conflict in interpretation with additional Clauses and other provisions set out in Sections III and IV of this instrument or in Associated Contracts.

Clause 9. Possibility of Third-Party Adherence

9.1. By mutual agreement between the Parties, a processing agent may adhere to these Clauses as an Exporter or Importer by completing and signing a written document that will become part of this instrument.

9.2. The adhering party will have the same rights and obligations as the original Parties, depending on its position as Exporter or Importer, and in accordance with the corresponding category of processing agent.

Clause 10. General Obligations of the Parties

10.1. The Parties undertake to adopt and, when necessary, demonstrate the adoption of effective measures capable of proving compliance with the provisions of these Clauses and Brazilian Legislation, including the effectiveness of these measures, and in particular:

a) To use the Personal Data only for the specific purposes described in Clause 2, without the possibility of further processing that is incompatible with these purposes, always observing the limitations, guarantees, and safeguards provided for in these Clauses;

b) To ensure that the processing is compatible with the purposes informed to the Data Subject, according to the context of the processing;

c) To limit the processing to the minimum necessary for the fulfillment of its purposes, ensuring that the data is relevant, proportional, and not excessive in relation to the purposes of Personal Data processing;

d) To guarantee the Data Subjects, as provided in Clause 4:

(d.1.) Clear, precise, and easily accessible information regarding the processing and the respective processing agents, while respecting commercial and industrial secrets;

(d.2.) Facilitated and free consultation on the form and duration of the processing, as well as the completeness of their Personal Data; and

(d.3.) Accuracy, clarity, relevance, and updating of the Personal Data, according to necessity and for the purpose of fulfilling the objective of its processing;

e) To adopt appropriate security measures compatible with the risks involved in the International Data Transfer governed by these Clauses;

f) To avoid processing Personal Data for discriminatory, unlawful, or abusive purposes;

g) To ensure that any person acting under their authority, including subcontractors or any agent collaborating with them free of charge or for a fee, processes the data only in accordance with their instructions and with the provisions of these Clauses; and

All rights reserved

h) To maintain a record of operations involving the processing of Personal Data subject to the International Data Transfer governed by these Clauses and present the relevant documentation to the ANPD when requested.

Clause 11. Sensitive Personal Data

11.1. If the International Data Transfer involves Sensitive Personal Data, the Parties will apply additional safeguards, including specific security measures proportionate to the risks of the processing activity, the specific nature of the data, and the rights, interests, and guarantees to be protected as described in Section III.

Clause 12. Personal Data of Children and Adolescents

12.1. If the International Data Transfer involves the Personal Data of children and adolescents, the Parties will apply additional safeguards, including measures to ensure that the processing is carried out in the best interests of the child, in accordance with Brazilian Legislation and relevant international legal instruments.

Clause 13. Legal Use of Data

13.1. The Exporter guarantees that the Personal Data has been collected, processed, and transferred to the Importer in accordance with Brazilian Legislation.

Clause 14. Transparency

14.1. The Designated Party shall publish on its website a document containing easily accessible information, written in simple, clear, and precise language, regarding the International Data Transfer, including at least the following:

a) The form, duration, and specific purpose of the international transfer;
b) The destination country of the transferred data;
c) The identification and contact details of the Designated Party;
d) The data sharing practices of the Parties and the purpose of such sharing;
e) The responsibilities of the agents conducting the processing;
f) The rights of the Data Subject and the means for exercising them, including a readily accessible channel for handling their requests and the right to petition against the Controller to the ANPD; and
g) Any further transfers, including the recipients and the purpose of the transfer.

14.2. The document referred to in item 14.1 may be made available on a specific page or integrated prominently and accessibly into the Privacy Policy or an equivalent document.

14.3. Upon request, the Parties shall provide the Data Subject with a free copy of these Clauses, while respecting commercial and industrial secrets.

14.4. All information made available to Data Subjects in accordance with these Clauses must be written in Portuguese.

Clause 15. Data Subject Rights

15.1. The Data Subject has the right to obtain from the Designated Party, in relation to the Personal Data subject to the International Data Transfer governed by these Clauses, at any time and upon request, as provided for in Brazilian Legislation:

a) confirmation of the existence of processing;
b) access to the data;
c) correction of incomplete, inaccurate, or outdated data;
d) anonymization, blocking, or deletion of unnecessary, excessive, or unlawfully processed data in accordance with these Clauses and Brazilian Legislation;
e) data portability to another service or product provider upon express request, in accordance with ANPD regulations, while respecting commercial and industrial secrets;
f) deletion of Personal Data processed with the Data Subject's consent, except in cases provided for in Clause 20;
g) information about the public and private entities with which the Parties have shared the data;
h) information about the possibility of not providing consent and the consequences of refusal;
i) revocation of consent through a free and easy procedure, with processing carried out before the revocation being ratified;
j) review of decisions made solely based on the automated processing of Personal Data that affect their interests, including decisions intended to define their personal, professional, consumer, and credit profile, or aspects of their personality; and
k) information on the criteria and procedures used for automated decision-making, while respecting commercial and industrial secrets.

15.2. The Data Subject may object to processing carried out on the basis of one of the exceptions to consent if there is non-compliance with these Clauses or Brazilian Legislation.

15.3. The time limit for responding to requests provided for in this Clause and in item 14.3 is 15 (fifteen) days from the date of

All rights reserved

the Data Subject's request, except in cases where a different time limit is established by specific ANPD regulations.

15.4. If the Data Subject's request is directed to the Party not designated as responsible for the obligations set out in this Clause or item 14.3, the Party shall:

a) inform the Data Subject of the service channel provided by the Designated Party; or

b) forward the request to the Designated Party as soon as possible to ensure a response within the time limit provided in item

15.5. The Parties shall immediately inform the Processing Agents with whom they have shared data of any correction, deletion, anonymization, or blocking of data so that the same procedure can be followed, except in cases where such communication is proven to be impossible or would involve disproportionate effort.

15.6. The Parties shall promote mutual assistance to ensure that Data Subjects' requests are addressed.

Clause16. Security Incident Communication

16.1. The Designated Party must notify the ANPD and the Data Subjects within 3 (three) business days of any security incident that may pose a risk or significant harm to the Data Subjects, in accordance with Brazilian Legislation.

16.2. The Importer must keep a record of security incidents, as required by Brazilian Legislation.

Clause 17. Liability and Compensation for Damages

17.1. A Party that causes material or moral damages to an individual or collective entity, in violation of these Clauses and Brazilian Legislation, through the processing of Personal Data is obligated to repair such damages.

17.2. The Data Subject may seek compensation for damages caused by any of the Parties as a result of a violation of these Clauses.

17.3. The defense of the Data Subjects' rights and interests may be pursued individually or collectively in court, in accordance with applicable legislation regarding instruments of individual and collective protection.

17.4. A Party acting as a Processor is jointly liable for damages caused by the processing if it fails to comply with these Clauses or does not follow the lawful instructions of the Controller, except as provided in item 17.6.

17.5. Controllers directly involved in the processing that resulted in damages to the Data Subject are jointly liable for such damages, except as provided in item 17.6.

17.6. The Parties are not liable if it is proven that:

a) they did not perform the Personal Data processing attributed to them;

b) although they performed the attributed Personal Data processing, there was no violation of these Clauses or Brazilian Legislation; or

c) the damage resulted exclusively from the fault of the Data Subject or a third party not involved in the Further Transfer or subcontracted by the Parties.

17.7. In accordance with Brazilian Legislation, the court may reverse the burden of proof in favor of the Data Subject when the allegation is credible, there is an imbalance of power in terms of evidence production, or when producing evidence is excessively burdensome for the Data Subject.

17.8. Actions for the compensation of collective damages resulting from liability under this Clause may be exercised collectively in court, as provided for in the relevant legislation.

17.9. The Party that compensates the Data Subject has the right to seek reimbursement from the other responsible parties to the extent of their participation in the harmful event.

Clause18. Safeguards for Further Transfers

18.1. The Importer may only carry out Further Transfers of Personal Data subject to the International Data Transfer governed by these Clauses if expressly authorized under the conditions described in Clause 3.

18.2. In any case, the Importer must:

a) ensure that the purpose of the Further Transfer is compatible with the specific purposes described in Clause 2;

b) guarantee through a written contractual instrument that the safeguards provided in these Clauses are observed by the third-party recipient of the Further Transfer; and

c) for the purposes of these Clauses, and in relation to the transferred Personal Data, be considered responsible for any irregularities committed by the third-party recipient of the Further Transfer.

18.3. The Further Transfer may also be carried out based on another valid mechanism for International Data Transfer provided for in Brazilian Legislation, regardless of the authorization provided in Clause 3.

Clause 19. Notification of Access Request

19.1. The Importer shall notify the Exporter and the Data Subject about an Access Request related to the Personal Data subject to the International Data Transfer governed by these Clauses, except when notification is prohibited by the law of the country where

All rights reserved

the data is processed.

19.2. The Importer shall take appropriate legal measures, including judicial actions, to protect the Data Subject's rights whenever there is a legal basis to question the legality of the Access Request, and if necessary, to prevent the notification prohibition mentioned in item 19.1.

19.3. To comply with requests from the ANPD and the Exporter, the Importer must maintain a record of Access Requests, including the date, requester, purpose of the request, type of data requested, number of requests received, and the legal measures taken.

Clause 20. Termination of Processing and Data Deletion

20.1. The Parties shall delete the Personal Data subject to the International Data Transfer governed by these Clauses upon termination of processing, within the technical limits of the authorized activities, with retention only for the following purposes:

a) compliance with legal or regulatory obligations by the Controller;
b) research purposes by a Research Organization, ensuring Personal Data anonymization whenever possible;
c) transfer to a third party, provided the requirements of these Clauses and Brazilian Legislation are met; and
d) exclusive use by the Controller, with the prohibition of access by third parties and provided the data is anonymized.

20.2. For the purposes of this Clause, the processing is considered terminated when:

a) the purpose outlined in these Clauses is achieved;
b) the Personal Data is no longer necessary or relevant to the specific purpose outlined in these Clauses;
c) the processing period has expired;
d) the Data Subject's request is fulfilled; and
e) it is determined by the ANPD that there has been a violation of these Clauses or Brazilian Legislation.

Clause 21. Data Security Measures

21.1. The Parties shall adopt security measures that ensure the protection of the Personal Data subject to the International Data Transfer governed by these Clauses, even after processing has terminated.

21.2. The Parties shall specify in Section III the Security Measures adopted, taking into account the nature of the information processed, the specific characteristics and purpose of the processing, the current state of technology, and the risks to the Data Subject's rights, especially in the case of sensitive personal data and data of children and adolescents.

21.3. The Parties shall take necessary steps to periodically assess and review the measures to maintain an adequate level of security for the characteristics of the data processing.

Clause 22. Legislation of the Data Recipient’s Country

22.1. The Importer declares that no laws or administrative practices in the data recipient country have been identified that prevent compliance with the obligations assumed in these Clauses.

22.2. If there is a change in legislation that alters this situation, the Importer shall immediately notify the Exporter for an evaluation of whether to continue the contract.

Clause 23. Non-Compliance by the Importer

23.1. In the event of a violation of the safeguards and guarantees provided for in these Clauses or the inability of the Importer to comply with them, the Exporter shall be notified immediately, except as provided in item 19.1.

23.2. Upon receiving the notification mentioned in item 23.1, or if the Exporter detects non-compliance with these Clauses by the Importer, the Exporter shall take appropriate measures to ensure the protection of the Data Subject's rights and the compliance of the International Data Transfer with Brazilian Legislation and these Clauses, which may include:

a) suspending the International Data Transfer;
b) requesting the return, transfer to a third party, or deletion of the Personal Data; and
c) terminating the contract.

Clause 24. Choice of Forum and Jurisdiction

24.1. These Clauses are governed by Brazilian law, and any dispute between the Parties arising from these Clauses shall be resolved in the competent courts of Brazil, subject to the forum elected by the Parties in Section IV, if applicable.

24.2. The Data Subjects may bring legal action against the Exporter or the Importer, at their discretion, in the competent courts in Brazil, including those located in their place of residence.

24.3. The Parties may mutually agree to use arbitration to resolve disputes arising from these Clauses, provided the arbitration takes place in Brazil and in accordance with the provisions of the Arbitration Law.

All rights reserved

SECTION III – Security Measures
As set forth in Security Safeguards Attachment.

Event Sponsorship Data Protection Addendum © S&P Global Market Intelligence LLC 2026
All rights reserved

Module 1: Controller to Controller

Controller-to-Controller Standard Contractual Clauses

SECTION I

Clause 1. Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) ([1]) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2. Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3. Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.5 (e) and Clause 8.9(b);

(iii) N/A

(iv) Clause 12(a) and (d);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

All rights reserved

(vii) Clause 16(e);
(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4. Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5. Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6. Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7. Docking clause - Optional

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8. Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;
(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;
(ii) of the categories of personal data processed;

All rights reserved

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation ([2]) of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

[2] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

All rights reserved

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union ([3]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation

[3] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

All rights reserved

(EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9. Use of sub-processors

N/A

Clause 10. Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. ([4]) The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

[4] That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

All rights reserved

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

Clause 11. Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body ([5]) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

[5] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

All rights reserved

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12. Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13. Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in

All rights reserved

Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14. Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([6]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate

[6] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Event Sponsorship Data Protection Addendum © S&P Global Market Intelligence LLC 2026
All rights reserved

with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15. Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

Event Sponsorship Data Protection Addendum © S&P Global Market Intelligence LLC 2026
All rights reserved

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16. Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

Event Sponsorship Data Protection Addendum © S&P Global Market Intelligence LLC 2026
All rights reserved

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17. Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

Clause 18. Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Republic of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Event Sponsorship Data Protection Addendum © S&P Global Market Intelligence LLC 2026
All rights reserved

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

Event Sponsorship Data Protection Addendum © S&P Global Market Intelligence LLC 2026
All rights reserved

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name: S&P Global and/or its affiliates as set forth in the Agreement or the applicable Sales Order Form
Address: 55 Water Street, New York, NY 10041 USA (or as set forth in the Agreement or Sales Order Form).
Contact person's name, position and contact details:
Data Protection Officer
55 Water Street, New York, NY 10041, USA 1-855-529-1761
privacy@spglobal.com

Activities relevant to the data transferred under these Clauses:
The Client is a customer of S&P. S&P will be disclosing S&P Data (as defined in the DPA) to Client in connection with the Event.
Signature and date: As set forth in the Agreement or Sales Order Form.
Role (controller/processor): Controller

2. Name: Client (as defined in the Agreement or Sales Order Form).
Address: As set forth in the Agreement or Sales Order Form.
Contact person's name, position and contact details: As set forth in the Agreement or Sales Order Form
Activities relevant to the data transferred under these Clauses: Client is a customer of S&P. Client will be disclosing Client Data (as defined in the DPA) to S&P in connection with the Event.
Signature and date: As set forth in the Agreement or the Sales Order Form.
Role (controller/processor): Controller

Data importer(s):

1. Name: Client (as defined in the Agreement or Sales Order Form).
Address: As set forth in the in the Agreement or Sales Order Form.
Contact person's name, position and contact details: As set forth in the Agreement or Sales Order Form.
Activities relevant to the data transferred under these Clauses: Client is a customer of S&P. Client will be receiving S&P Data (as defined in the DPA) from S&P in connection with the Event.
Signature and date: As set forth in the Agreement or Sales Order Form
Role (controller/processor): Controller

2. Name: S&P Global and/or its affiliates as set forth in the Agreement or Sales Order Form.
Address: 55 Water Street, New York, NY 10041 USA (or as set forth in the Agreement or Sales Order Form).
Contact person's name, position and contact details:
Data Protection Officer
55 Water Street, New York, NY 10041, USA 1-855-529-1761
privacy@spglobal.com
Activities relevant to the data transferred under these Clauses:
Client is a customer of S&P. S&P will be receiving Client Data (as defined in the DPA) from the Client in connection with the Event.
Signature and date: As set forth in the Agreement or Sales Order Form.
Role (controller/processor): Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

For transfers of Client Data (As defined in the DPA): (1) data subjects who are employees and/or agents of Client; and (2) other individuals who are registered to attend the Event.

Event Sponsorship Data Protection Addendum © S&P Global Market Intelligence LLC 2026
All rights reserved

For transfers of S&P Data (As defined in the DPA): (i) data subjects who are employees and/or agents of S&P; and (2) other individuals who are registered to attend the Event.

Categories of personal data transferred: Client Data and S&P Data (as both terms are defined in the DPA).
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures. N/A
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis). One-off.
Nature of the processing: For the Permitted Purpose (as defined in the DPA).
Purpose(s) of the data transfer and further processing: For the Permitted Purpose (as defined in the DPA).
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: As required to provide the Services.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: N/A.

COMPETENT SUPERVISORY AUTHORITY
Identify the competent supervisory authority/ies in accordance with Clause 13: To be determined in accordance with Clause 13 in relation to the particular data exporter.

 © S&P Global Market Intelligence LLC 2026
All rights reserved

ANNEX II

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

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Security Safeguards Attachment, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Event Sponsorship Data Protection Addendum © S&P Global Market Intelligence LLC 2026
All rights reserved

Saudi Arabia Standard Contractual Clauses

Clause (1) Purpose and Scope

A. The purpose of these Clauses is to ensure that an appropriate level of Personal Data protection equivalent to the level of protection applicable under the Personal Data Protection Law and its Implementing Regulations is applied in the absence of an appropriate level of Personal Data protection outside the Kingdom by specifying the obligations of the parties involved in the transfer of Personal Data to a country or international organization that does not have an appropriate level of Personal Data protection.

Appendix (1) shows the data for both Data Exporters and Data Importers.

B. These Clauses apply to the transfer of Personal Data as specified in Appendix (2) ("Personal Data to be Transferred or Disclosed").

Clause (2) Impact and Modification

A. These Clauses set out appropriate safeguards, including rights of complaint by Personal Data Subjects, and cannot be amended except to select the appropriate template or to add or update information in the appendix.

B. The parties may incorporate these Clauses into a comprehensive agreement or add other clauses or additional guarantees, provided they do not directly or indirectly conflict with these Clauses or infringe on the fundamental rights of Personal Data Subjects.

C. These Clauses do not relieve any party from its obligations under the Law and Regulations, nor do they prejudice the provisions of the Laws and Regulations in force in the Kingdom or agreements to which the Kingdom is a party.

Clause (3) Rights of Personal Data Subjects

A. These Standard Contractual Clauses are without prejudice to the rights of Personal Data Subjects under the Law and Regulations.

B. Personal Data Subjects whose Personal Data is transferred from the parties based on these Standard Contractual Clauses may notify the Competent Authority ("Saudi Data & AI Authority") if they become aware of any violation of these Standard Contractual Clauses.

Clause (4) Interpretation

A. Unless the context requires otherwise, the words and phrases used in these Clauses shall have the meanings assigned to them in Article (1) of the Personal Data Protection Law issued by Royal Decree No. (M/19) dated 9/2/1443 AH and amended by Royal Decree No. (M/148) dated 5/9/1444 AH, Article (1) of the Implementing Regulation of the PDPL and Article (1) of the Regulation on the Transfer of Personal Data Outside the Kingdom.

B. These Clauses must be read and interpreted in light of and in accordance with the provisions of the Law and Regulations referred to in paragraph (a) of this Article, and may not be interpreted in any other way that is inconsistent with the provisions of the Law and Regulations.

Conflict (5) Clause

In the event of a conflict between these Clauses and any provision in any other agreement between the parties, these Clauses shall prevail.

Clause (6) Details of Transfers

The transfer(s), as well as the categories of Personal Data and the purposes of the transfers, are described in the Appendix.

Clause (7) Addition of New Parties

A. Any Personal Data Importer or Personal Data Exporter who is not a party to these Standard Clauses may join these Standard Contractual Clauses by completing and signing Appendix (1), with the consent of the existing parties. The Joining Entity shall be either the Personal Data Importer or the Personal Data Exporter.

All rights reserved

B. Once Appendix (1) has been completed and signed, the Joining Entity shall be a party to these Clauses, and the newly Joined Entity shall, as of the date of joining, and assume the responsibilities depending on the nature of the Personal Data processing and transfer operations that occurred on or after the date of joining, and shall be entitled to exercise the rights and obligations corresponding to its role as defined in these Clauses.

Clause (8) Governing Law and Jurisdiction

These Standard Contractual Clauses shall be governed by the applicable laws of the Kingdom of Saudi Arabia. Any dispute arising from the application of the provisions of these Clauses shall fall under the jurisdiction of the Kingdom and be vested in its courts. The Personal Data Importer, under these Standard Contractual Clauses, agrees to submit to the jurisdiction of the Kingdom of Saudi Arabia.

Clause (9) Compliance with the Requests of the Competent Authority

A. Each party agrees to comply with any requests from the Competent Authority in relation to these Standard Contractual Clauses or the processing of transferred Personal Data.

B. The Personal Data Importer agrees and commits to cooperate with the Competent Authority and comply with all its requests and inquiries and provide the necessary documents and information to ensure compliance with the Standard Contractual Clauses.

C. The Personal Data Importer agrees to abide by the measures adopted by the Competent Authority, including corrective measures and compensation.

Clause (10) Compensation

A. If any dispute arises between the Personal Data Subject and a party regarding compliance with the Standard Contractual Clauses, that party shall use all necessary means to settle the dispute amicably with the Personal Data Subject, and all parties shall inform each other of the existence of such dispute to ensure that it is resolved in cooperation with each other.

B. The Personal Data Subject may submit to the Competent Authority any complaint arising from the application of the provisions of these Standard Contractual Clauses, in accordance with the procedures for submitting complaints specified by the Law and Regulations.

C. The Personal Data Subject has the right to claim before the competent court for compensation for material or moral damage in proportion to the magnitude of the damage arising from the application of these Standard Contractual Clauses.

Clause (11) Personal Data Security

A. All parties shall take the necessary organizational, administrative, and technical measures that ensure to maintain the privacy of personal Data against any breach at all stages of processing, including personal data security during the transfer process. In assessing the appropriate level of security, the Parties shall take into account the current state of technology, implementation costs, and the nature of the Personal Data transferred, as well as the nature, scope, context, purposes, the risks involved in the processing of the Personal Data, and specifically consider the application of encryption or de-identification, including during Personal Data transfer, where the purpose of the data processing can be achieved in this way.

B. The Personal Data Exporter shall assist the Personal Data Importer in fulfilling the necessary data security requirements, and in the event of any Personal Data breach in relation to the transferred Personal Data processed by The Personal Data Exporter under these Standard Contractual Clauses, The Personal Data Exporter shall notify the Personal Data Importer without delay after becoming aware of such breach and shall assist the Personal Data Importer in containing such breach.

C. The Data Exporter ensures that persons authorized to process the transferred Personal Data are bound by confidentiality and nondisclosure under an appropriate legal obligation of confidentiality and non-disclosure.

Clause (12) Duration and Termination

A. If, for any reason, the personal Data Importer is unable to fulfill its obligations under these Standard Contractual Clauses, it must inform the Personal Data Exporter within (24) hours from the time it becomes aware of this.

Event Sponsorship Data Protection Addendum © S&P Global Market Intelligence LLC 2026
All rights reserved

B. In the event that the personal Data Importer violates these Standard Contractual Clauses or is unable to comply with them, the personal Data Exporter shall immediately cease the transfer of Personal Data to the Personal Data Importer until the Personal Data Importer ensures its return to compliance again, provided that the Personal Data Importer shall be given a period of (30) days, extendable for a similar maximum period, to prove its ability to comply with these Clauses, and if the period expires without achieving this, the two parties shall agree to terminate the contract, without any liability for the Personal Data Exporter or Controller, as the case may be.
C. The Personal Data Exporter or Controller, as the case may be, shall ensure that all Personal Data previously transferred to the Personal Data Importer is fully destroyed before terminating the Standard Contractual Clauses under paragraph (b) above. It shall also ensure that any copies it has of such personal data are destroyed.
D. The Personal Data Importer must document the destruction of the data, and this documentation must be provided to the Personal Data Exporter or controller upon request.
E. The Personal Data Importer must continue to ensure - until the data is destroyed - that it complies with these Standard Contractual Clauses.

Clause (13) Protection of Transferred Personal Data
The Personal Data Exporter and the Personal Data Importer shall process the transferred Personal Data according to the nature and purposes of the transfer and the appropriate template as follows:
r
1. Processing Restrictions
The personal Data Importer is obliged to process the transferred Personal Data in accordance with the purposes set out in Appendix (2).

2. Compliance with the Requests of the Competent Authority
A. The parties shall provide a copy of these Clauses to the Competent Authority upon request and without undue delay in order for the Competent Authority to exercise its powers under the Law and Regulations. The Competent Authority may request any additional information regarding the transfers of Personal Data.
B. Each party agrees to comply with any requests made by the Competent Authority in relation to these Clauses or the processing of the transferred data.
C. Upon request, the Personal Data Importer (either directly or through the Personal Data Exporter) shall disclose its identity and contact details and the categories of Personal Data being processed to the Personal Data Subject and provide a copy of these items.

3. The Minimum Amount of Personal Data Needed to Fulfill the Purpose
All parties shall ensure that the Personal Data transferred is sufficient and limited to the minimum amount necessary to fulfill the purposes set out in Appendix (2).
If any party becomes aware of any transfer of unnecessary Personal Data, that party shall inform the other party(ies) as soon as it becomes aware of it.

4. Personal Data Retention
The Personal Data Importer shall retain the transferred Personal Data if it is necessary to fulfill the purposes set out in Appendix (2), provided that the Personal Data Importer shall, without undue delay, delete or anonymize the transferred Personal Data except in the following cases:
A. If it is in accordance with a legal justification under the Kingdom's laws and the Personal Data Protection Law and its Regulations; in this case, the data shall be destroyed after expiration of the period or once the purpose for collecting it has been fulfilled, whichever is longer.
B. If retaining the transferred personal data for an additional period is directly related to a case pending before a judicial authority, and such retention is required for this purpose, the data shall be destroyed after completion of the judicial procedures related to the case.
C. If retaining the transferred personal data for an additional period is necessary to protect the life of the data subject or their vital interests.

5. Personal Data Security and Personal Data Breach Incident Notifications

All rights reserved

The Parties shall ensure that the organizational, administrative, and technical measures specified in Appendix (3) provide a sufficient level of protection for the transferred Personal Data to comply with the requirements of Article (19) of the Law and Article (23) of the Implementing Regulations.
A. The Personal Data Importer shall implement the security measures specified in Appendix (3) and apply those measures to all Personal Data transferred to ensure the security and protection of Personal Data against any violation that may result in damage to the Personal Data Subject, unlawful action, loss, alteration, disclosure of Personal Data or unauthorized access.
B. The Personal Data Importer must periodically review the security measures stipulated in Appendix (3) to ensure that they are being implemented as required, and update them as needed to ensure compliance with Article (19) of the Law and Article (23) of the Implementing Regulations.
If the Personal Data Importer becomes aware of a data breach incident that could harm the transferred personal data or the data subjects, or conflict with their rights or interests, the Personal Data Importer must notify the competent authority within (72) hours of becoming aware of the incident, in accordance with the requirements stated in Article (24) of the Implementing Regulations of the Law.

6. Sensitive Data
Without prejudice to any restrictions relating to sensitive data stipulated in the Law and the Implementing Regulations of the Law, the Personal Data Exporter shall ensure that the Personal Data Importer adopts additional safeguards appropriate to the nature of the sensitive data and ensures that it is protected from any risks when processing it while ensuring that the restrictions and additional safeguards described in Attachment B Appendix (2) are applied.

7. Subsequent Transfer
A. The Personal Data Importer shall not transfer or disclose the transferred Personal Data to a third party outside the Kingdom unless that party has acceded to these Clauses and in accordance with the appropriate template and the provisions of Clause (7) above.
B. Without prejudice to the provisions of Articles (8) and (15) of the Law and (17) of the Implementing Regulation of the Law, the provisions of the Law and Regulations shall apply to subsequent transfer of Personal Data that has been previously transferred or disclosed to an entity outside the Kingdom.

8. Assigning Processors
The Personal Data Importer shall be obliged to select a Processor that provides sufficient guarantees for the protection of the transferred Personal Data, and the agreement with the Processor shall include all the requirements set out in Article (17) of the Implementing Regulation, and the processing shall be based solely on the instructions of the Data Importer, provided that these instructions are consistent with the requirements set out in these Clauses.

9. Compliance with these Clauses
A. All parties shall demonstrate full compliance with these Clauses to the Competent Authority upon request, and the Personal Data Importer shall maintain documents related to the Personal Data processing activities conducted under its supervision, in addition to the records of Personal Data processing activities as stipulated in Article (33) of the Regulation.
B. The Personal Data Importer shall provide these documents to the Competent Authority upon request.

10.Accountability
A. Each party shall be accountable to the other party for any damages caused to the other party as a result of a breach of any of these Standard Contractual Clauses.
B. Each party shall be accountable to the Personal Data Subject, without prejudice to the accountability of the Personal Data Exporter under the Law and Regulations, and the Personal Data Subject shall be entitled to compensation for any material and moral damages caused by the negligent party that harms the Personal Data Subject. If more than one party is responsible for causing damage to the Personal Data Subject as a result of the violation of these Standard Contractual Clauses, the responsible parties shall be held jointly or individually

All rights reserved

accountable, and the Personal Data Subject shall have the right to take legal action before a court against any of these parties.
C. The parties agree that if any party assumes accountability (b), it shall be entitled to claim from the other party(ies) that portion of the compensation corresponding to his/her/their accountability for the damage.
D. The Personal Data Importer may not rely on the behavior of the data Processor or Sub- Processor to avoid accountability.

11.Right of Personal Data Subjects

A. The Personal Data Importer (with the support of the Personal Data Exporter) shall deal, as appropriate, with any queries or requests received from the Data Subject regarding the processing of Personal Data and the exercise of the rights provided for in accordance with the Law and applicable regulations without any delay within a period of no more than thirty (30) days from the date of receipt of such request. This period may be extended for a similar period up to a maximum of thirty (30) days if the execution of the request requires extraordinary effort or if the Personal Data Importer receives many requests from the Personal Data Subject. The Data Subject is notified in advance of this extension and its reasons.
B. All statements made to the Personal Data Subject must be presented in a clear, legible, and accessible format.

Event Sponsorship Data Protection Addendum © S&P Global Market Intelligence LLC 2026
All rights reserved

Appendix 1- List of Parties

Information of Personal Data Exporter (s) / Importer(s)	**Information of Personal Data Importer (s) / Exporter (s)**
Name: S&P Global and/or its affiliates (as defined in the Agreement or Sales Order Form	Name: Client (as defined in the Agreement or Sales Order Form).
Address: 55 Water Street, New York, NY 10041, USA (or as set forth in the Agreement or Sales Order Form)	Address: As set forth in the Agreement or Sales Order Form.
Contact Information: attn to Data Privacy Officer privacy@spglobal.com	Contact Information: As set forth in the Agreement or Sales Order Form
Signature: As set forth in the Sales Order Form.	Signature: As set forth in the Agreement or Sales Order Form.
Date: As set forth in the Agreement or Sales Order Form.	Date: As set forth in the Agreement or Sales Order Form.
Role: Controller/Processor	Role: Controller/Processor

Appendix 2- Description of Transferred Personal Data

S&P Data and/or Client Data (as those terms are defined in DPA) for the Permitted Purpose.

Appendix 3 - Security Measures

As set forth in Security Safeguards Attachment.

Event Sponsorship Data Protection Addendum © S&P Global Market Intelligence LLC 2026
All rights reserved

UK Addendum

This UK Addendum forms part of the DPA between S&P and Client, as applicable.

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This UK Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	As set forth in the Sales Order Form.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: S&P (as defined in the Agreement or the Sales Order Form) Trading name (if different): N/A Main address (if a company registered address): 55 Water Street, New York, NY 10041 Official registration number (if any) (company number or similar identifier): N/A	Full legal name: Client name as set forth in the Agreement or Sales Order Form Trading name (if different): As set forth in the Agreement or Sales Order Form. Main address (if a company registered address): As set forth in the Agreement or Sales Order Form Official registration number (if any) (company number or similar identifier): As set forth in the Agreement or Sales Order Form

Event Sponsorship Data Protection Addendum © S&P Global Market Intelligence LLC 2026
All rights reserved

Key Contact	Full Name (optional): N/A Job Title: Data Protection Officer Contact details including email: 55 Water Street, New York, NY 10041, USA (or as set forth in the Agreement or Sales Order Form) 1-855-529-1761 privacy@spglobal.com	Full Name (optional): As set forth in the Agreement or Sales Order Form. Job Title: As set forth in the Agreement or Sales Order Form Contact details including email: As set forth in the Agreement or Sales Order Form
Signature (if required for the purposes of Section 2)	N/A	N/A

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this UK Addendum is appended to, detailed below, including the Appendix Information: Date: As set forth in signature block of the Sales Order Form or the Agreement incorporating this UK Addendum. Reference (if any): N/A					
	Other identifier (if any): N/A Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this UK Addendum:					
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
3						
4						

Event Sponsorship Data Protection Addendum © S&P Global Market Intelligence LLC 2026
All rights reserved

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

Annex IA: List of Parties: As set forth in Annex IA of the Approved EU SCCs which this UK Addendum is appended to.

Annex IB: Description of Transfer: As set forth in Annex IB of the Approved EU SCCs which this UK Addendum is appended to.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set forth in Annex II of the Approved EU SCCs which this UK Addendum is appended to.

Annex III: List of Sub processors (Modules 2 and 3 only): As set forth in Annex III of the Approved EU SCCs which this UK Addendum is appended to.

Table 4: Ending this UK Addendum when the Approved Addendum Changes

Ending this UK Addendum when the Approved Addendum changes	Which Parties may end this UK Addendum as set out in Section 19: ☐ Importer ☐ Exporter ☒ Neither Party

Part 2: Mandatory Clauses

Entering into this UK Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this UK Addendum, in exchange for the other Party also agreeing to be bound by this UK Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this UK Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this UK Addendum. Entering into this UK Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this UK Addendum

3. Where this UK Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

UK Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this UK Addendum is appended to, as set out in Table 2, including the Appendix Information.

Event Sponsorship Data Protection Addendum © S&P Global Market Intelligence LLC 2026
All rights reserved

Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 28 January 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This UK Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this UK Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this UK Addendum, UK Data Protection Laws applies.
7. If the meaning of this UK Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re- enacted and/or replaced after this UK Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy

Event Sponsorship Data Protection Addendum © S&P Global Market Intelligence LLC 2026
All rights reserved

in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this UK Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this UK Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This UK Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
    c. this UK Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
    a. References to the "Clauses" means this UK Addendum, incorporating the Addendum EU SCCs;
    b. In Clause 2, delete the words:
       "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";
    c. Clause 6 (Description of the transfer(s)) is replaced with:
       "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";
    d. Clause 8.7(i) of Module 1 is replaced with:
       "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";
    e. Clause 8.8(i) of Modules 2 and 3 is replaced with:
       "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"
    f. References to "Regulation (EU) 2016/679", "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 (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;
    g. References to Regulation (EU) 2018/1725 are removed;
    h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";
    i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

 © S&P Global Market Intelligence LLC 2026
All rights reserved

j. Clause 13(a) and Part C of Annex I are not used;
k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";
l. In Clause 16(e), subsection (i) is replaced with:
"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";
m. Clause 17 is replaced with:
"These Clauses are governed by the laws of England and Wales.";
n. Clause 18 is replaced with:
"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and
o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this UK Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
    a. From time to time, the ICO may issue a revised Approved Addendum which makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this UK Addendum including the Appendix Information. This UK Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.
18. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
    a its direct costs of performing its obligations under the Addendum; and/or
    b its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this UK Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.
19. The Parties do not need the consent of any third party to make changes to this UK Addendum, but any changes must be made in accordance with its terms.

Event Sponsorship Data Protection Addendum © S&P Global Market Intelligence LLC 2026
All rights reserved

Appendix 3

Security Safeguards Attachment

A. **For S&P Data:**

Minimum Security Safeguards:

Without limiting Client's obligation to implement and maintain the Security Safeguards, S&P expects that Client's will:

- Store S&P Data, using strong encryption techniques with a minimum of Advanced Encryption Standard with 256-bit key size (AES-256).
- Transmit S&P Data, using the versions of secure protocols and methods (HTTPS, TLS, SFTP, SSH, and IPSec), as recommended by NIST in their Guideline for using Cryptographic Standards;
- Maintain a process for analyzing the lawfulness of demands or orders received from government authorities or law enforcement about S&P Data and whether release of S&P Data is authorized or required by law;
- Ensure that, for as long as Client holds S&P Data, it will not purposefully create any process (e.g., "back doors" or similar programming) that does or could permit or facilitate unauthorized access to S&P Data or, if applicable law or policy in a Destination Jurisdiction requires any such process, notify S&P and permit S&P to terminate the Agreement without penalty;
- Maintain tamper-proof records of all Processing of S&P Data; and
- Deploy strict and granular access controls and enforce access and confidentiality restrictions through disciplinary measures.
- Maintain an effective vulnerability management program that is in line with industry best practices and/or frameworks such as NIST or CIS.
- Implement and maintain appropriate asset management measures to ensure all assets used in service delivery are accurately inventoried, tracked, protected, and securely disposed of at end-of-life.
- Maintain and annually review information security and topic-specific policies and provide them to S&P upon request.
- Maintain visibility on the accessing of such personal data, through appropriate logs, monitoring and review, for enabling detection of unauthorized access, its investigation and remediation to prevent recurrence.
- Maintain reasonable measures for continued processing in the event of confidentiality, integrity or availability of such personal data being compromised because of destruction or loss of access to personal data or otherwise, such as by way of data-backups in line with industry's best practices.
- Implement and maintain appropriate access control and identity management measures to ensure only authorized individuals can access systems and data, with access rights regularly reviewed and promptly revoked upon role changes or termination.
- Implement and maintain appropriate vulnerability management and security testing measures, including regular vulnerability scanning, timely remediation based on risk/criticality, and periodic security testing (e.g., penetration testing) to identify, track, and address security weaknesses in line with industry's best practices.
- Implement and maintain appropriate incident management measures, including a documented response plan, regular testing, timely reporting, and lessons learned reviews to effectively detect, respond to, and recover from security incidents.
- Implement and maintain appropriate Data loss prevention (DLP) measures to protect sensitive & personal information.
- Implement and maintain appropriate secure SDLC and change management measures (if applicable).

- Implement and maintain appropriate physical security measures to protect facilities, equipment, and sensitive areas from unauthorized access, theft, damage, and disruption, including access controls, surveillance, and environmental safeguards (if applicable).
- Implement and maintain appropriate network and communication security measures to protect systems and data from unauthorized access, malware, and other threats.
- Implement and maintain appropriate endpoint security measures to protect devices from malware, unauthorized access, and data loss, including the use of antivirus/anti-malware software, device encryption, regular patching, and monitoring for suspicious activity.

If Data Protection Law or any of Client's Security Safeguards are more protective of Personal Data than the measures set forth immediately above, then Client will maintain the measures that are most protective of S&P Data. Client agrees that it will discuss in good faith with S&P the method and means for addressing any gap among Client's measures, S&P's expectations as set forth in this Attachment and then-current industry practice and standards for companies engaged in providing services of similar

 © S&P Global Market Intelligence LLC 2026
All rights reserved

scope and complexity as the services provided by Client pursuant to the Agreement.
For processing personal data of Indian Data Principals as per the DPDP Act, the following data protection measures shall apply in addition to the afore-mentioned security measures:

- appropriate data security measures, such as securing of personal data through encryption, obfuscation, masking or the use of virtual tokens mapped to that personal data.
- appropriate measures to control access to the computer resources used by such Data Fiduciary or such a Data Processor, wherever applicable.
- visibility on the accessing of such personal data, through appropriate logs, monitoring and review, for enabling detection of unauthorised access, its investigation and remediation to prevent recurrence.
- reasonable measures for continued processing in the event of confidentiality, integrity or availability of such personal data being compromised as a result of destruction or loss of access to personal data or otherwise, such as by way of data-backups; and
- for enabling the detection of unauthorised access, its investigation, remediation to prevent recurrence and continued processing in the event of such a compromise, retain such logs and personal data for a period of one year, unless compliance with any law for the time being in force requires otherwise.

For Client Data:

S&P Global Technical and Organizational Measures

Security Measure	Summary
Risk Management Program Overview	S&P Global's Risk Management program includes Information Security to manage risk through three lines of defense.
Information Security Organization and Governance Structure	The Chief Information Security Officer (CISO) manages and coordinates S&P Global's Information Security Program.
Information Security Policy	S&P Global's Information Security policies and standards are based on the best practices recommendations for information security management as published in ISO/IEC-27002 and NIST 800 Standards. The governance team uses the NIST Cybersecurity Framework to assess, measure and monitor the maturity of the organization's Information Security practices and target state. S&P Global's Code of Business Ethics (COBE) defines the behaviors expected of employees at S&P Global. S&P Global requires employees to personally reaffirm this code on a yearly basis.
Information Security Pillars: Information Security Awareness & Training	S&P Global has an Information Security Awareness and Training program that trains employees on information security policies and security best practices. All employees are required to take annual computer-based information security training and refresher course(s), which reinforces information security policies and data privacy. Security awareness training for non-employees is available and limited to those who have been identified as having access to the company's global systems.
Information Security Pillars: Cyber Defense, Threat Intelligence & Monitoring	S&P Global's cyber incident response program is managed by the Information Security Monitoring & Cyber Incident Response Team ("CIRT") in conjunction with the Security Operations Center (SOC) where security analysts monitor security events and escalate validated or suspicious security incidents for further probing and invoke Incident Management Procedure as necessary.
Information Security Pillars: Application Security	S&P Global's Information Security Application Security Program provides an operational governance role that monitors, reports on and remediates vulnerabilities. Penetration Testing and Related Independent Third-Party Security Reviews: S&P Global regularly sponsors and conducts independent security reviews of its computing environment.
Information Security Pillars: Security Architecture	S&P Global's Information Security Program Security Architecture provides an oversight and review of new platforms/applications to ensure

All rights reserved

	they conform to Information Security policies, standards, procedures, and guidelines.
Information Security Controls: Infrastructure Security	Key routing and switching components are located in physically secured data centers or locations that provide physical security and monitoring of events. Authentication and access to these key components are governed by the company's authentication policies. Once authenticated, S&P Global's key core routing and switching components are managed by professional network service engineers.
Information Security Controls: Information Classification	The company classifies information into categories to determine how S&P Global protects, stores, and distributes the information, including client data.
Information Security Controls: Protection of Information in Transit	When the company is required to transmit or receive sensitive data via a public network, industry, best-practices standard methods are used.
Information Security Controls: Identity Management, Authentication & Authorization	The Identity Management Platform governs access for customers and employees and provides strong authentication, providing for granular entitlements.
Information Security Controls: Protection Against Viruses & Malware	S&P Global employs a defense-in-depth approach to virus and malware protection, using the traditional signature and heuristics-based End Point Protection suite of virus and malware prevention products and various gateway scanning products. Traditional and behavior-based end point protection and detection software is installed on desktops and Windows servers.
Information Security Controls: Technology Change Management	S&P Global's technology change management process implemented by its IT partners and various divisional IT Operations requires a consistent documentation and approval process with respect to changes that modify technical or applications environments, introduce risk, or require application downtime.
Physical Security Program	S&P Global's Global Security & Crisis Management ("GSCM") is responsible for overseeing the protection of the corporation's global physical assets and is headed by the VP and Chief Security Officer. S&P Global's physical security and security ID policy requires the issuance to, and use of identification badges by, all employees and contractors.

 © S&P Global Market Intelligence LLC 2026
All rights reserved