

Jurisdiction Specific Terms to the Data Protection Addendum for Graphic Packaging International (“GPI”) Vendors

Effective Date: September 7, 2023

Last Updated: September 7, 2023

1. General

- 1.1. These Jurisdiction Specific Terms are an integral part of the GPI Data Processing Addendum (“**Addendum**”). Capitalized terms which are used but not defined in this document shall have the meaning given to those terms in the Addendum. By signing the Addendum, the Parties have agreed to comply with these Jurisdiction Specific Terms which apply to the extent that the Parties Process GPI Personal Data originating from, or protected by, Applicable Data Protection Laws in one of the jurisdictions identified herein.
- 1.2. GPI may update these Jurisdiction Specific Terms from time to time to reflect changes in or additions to Applicable Data Protection Laws to which relevant Processing operations are subject.
- 1.3. In case of any conflict or ambiguity between the Jurisdiction Specific Terms and any other terms of the Addendum, these Jurisdiction Specific Terms will prevail.

2. Argentina

- 2.1. Wherever the Processing pursuant to the Addendum falls within the scope of the Argentine Republic’s Personal Data Protection Law 25,326, Regulatory Decree 1558/2001, or any other corresponding decrees, regulations, or guidance governing the Processing of Personal Data in Argentina (collectively “**Argentine Data Protection Laws**”), the provisions of the Addendum and this Section shall apply to such Processing.
- 2.2. Any Restricted Transfer subject to Argentine Data Protection Laws from GPI to Vendor must comply with the applicable Data Protection Laws, and the transfer mechanism shall be one of the following, in the stated order of precedence:
 - (a) Where the Restricted Transfer both originates from and terminates in a country, a sector within a country, or an international organization which the Argentine National Bureau of Personal Data Protection (“**NBPDP**”) has determined provides an adequate level of protection to Personal Data, such adequacy determination shall be the transfer mechanism.
 - (b) Where it is not possible to rely on an NBPDP adequacy determination, the transfer mechanism shall be the Parties’ accession to Annex II of the SCCs promulgated by the NDPDP in its Provision 60-E/2016, or, in the event the NBPDP updates or amends such SCCs, the transfer mechanism shall be the Parties’ accession to the appropriate module of the updated or amended SCCs , as promulgated by the NDPDP.
- 2.3. Where it is necessary to do so, the Addendum therefore incorporates by reference Annex II of the SCCs. The contents required to be set forth in Annex A to Annex II of the Argentine SCCs are set forth in Exhibit A to the Addendum. For the purposes of Annex II of the Argentine SCCs and this Section, the Data Importer and Data Exporter roles are set out in Annex I, Exhibit A to the Addendum. The Parties are deemed to have accepted, executed, and signed Annex II of the SCCs where necessary in its entirety.

- 2.4. In cases where Annex II of the SCCs applies and there is a conflict between the terms of the Addendum and the terms of Annex II of the SCCs, the terms of Annex II of the SCCs shall prevail with regard to the Restricted Transfer in question.

3. Australia

When applicable, the Processing of GPI Personal Data shall be compliant with the Australian Privacy Principles, the Australian Privacy Act (1988), or any other applicable law, regulation, or decree of Australia pertaining to the protection of such information.

4. Brazil

When applicable, the Processing of GPI Personal Data shall be compliant with Brazil's Lei Geral de Proteção de Dados, Law No. 13.709 of 14 August 2018 and any corresponding decrees, regulations, or guidance.

5. Bulgaria

- 5.1. Wherever the Processing pursuant to the Addendum falls within the scope of Bulgaria's Personal Data Protection Act (as amended in November 2019) ("**PDPA**"), the Electronic Communications Act, or any other corresponding decrees, regulations, or guidance, the provisions of the Addendum and this Section shall apply to such Processing.
- 5.2. The Parties agree and acknowledge that, when Vendor acts as a Processor, Vendor shall comply with Article 25a of the PDPA which requires Vendor to:
 - (a) Return to GPI any Personal Data Processed pursuant to the Addendum within a period of one month after having become aware of any Personal Data that has been disclosed (i) without a legal basis pursuant Article 6 (1) of the GDPR, or (ii) contrary to the principles under Article 5 of the GDPR; or, if this is impossible or would involve disproportionate efforts, erase or destroy the Personal Data; and
 - (b) If the Personal Data is erased or destroyed in accordance with Section 5.2(a) of these Jurisdiction Specific Terms above, document such erasure and destruction.

6. California

6.1. Definitions

- (a) "**Business Purpose**" (as used in this Section) shall have the meaning ascribed to it by California Data Protection Laws.
- (b) "**California Data Protection Laws**" (as used in this Section) includes the California Consumer Privacy Act of 2018, and the California Consumer Privacy Act Regulations, and the California Privacy Rights Act of 2020.
- (c) "**Commercial Purpose**" (as used in this Section) shall have the meaning ascribed to it in the California Data Protection Laws.
- (d) "**Personal Data Breach**" (as used in the Addendum) includes "**Breach of the Security of the System**" as defined under paragraph (g) of Section 1798.82. of the California Civil Code.
- (e) "**Sell**" (as used in this Section) shall have the meaning ascribed to it in the California Data Protection Laws.

- (f) “**Share**” (as used in this Section) shall have the meaning ascribed to it in the California Data Protection Laws.
- 6.2. GPI discloses GPI Personal Data to Vendor solely for: (i) valid Business Purposes; and (ii) to enable Vendor to perform the Services under the Terms.
- 6.3. Vendor shall not: (i) Sell or Share GPI Personal Data; (ii) retain, use, or disclose GPI Personal Data for a Commercial Purpose other than providing the Services specified in the Terms or as otherwise permitted by the California Data Protection Laws; (iii) retain, use, or disclose GPI Personal Data except where permitted under the Terms between GPI and Vendor; nor (iv) combine GPI Personal Data with the personal data that it receives from another customer of Vendor. Vendor certifies that it understands these restrictions and will comply with them.
- 6.4. Vendor shall notify GPI if Vendor determines that it can no longer meet its obligations under California Data Protection Law. Upon notice of Vendor’s non-compliance with California Data Protection Law, GPI may take reasonable and appropriate steps to stop and remediate unauthorized use of GPI Personal Data.

7. Canada

When applicable, the Processing of GPI Personal Data shall be compliant with the Canadian Federal Personal Information Protection and Electronic Documents Act and any other applicable Canadian privacy or data protection laws.

8. Colombia

- 8.1. Wherever the Processing pursuant to the Addendum falls within the scope of Colombia’s Data Protection Law No. 1581 of 2012 (“**Data Protection Law No. 1581**”), Data Protection Decree No. 1377 of 2013 (“**Data Protection Decree**”), and any corresponding decrees, regulations, or guidance (collectively “**Colombian Data Protection Laws**”), the provisions of the Addendum and this Section shall apply to such Processing.
- 8.2. **Definitions**
 - (a) “**Information Processing Policy**” (“**Política de Tratamiento de la información**”) (as used in this Section) shall have the meaning set forth in Article 13 of the Data Protection Decree.
 - (b) “**Personal Data Breach**” (as used in the Addendum) includes “violations of security codes” [that] “result in risks to the administration of Data Subjects’ information” (“violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares”), as that phrase is construed under Articles 17(n) and 18(k) of the Data Protection Law No. 1581.
 - (c) “**Rights of the Data Subjects**” (as used in the Addendum) include such Data Subjects’ hábeas data rights, as that phrase is construed under the Constitution of Colombia and Colombian Data Protection Laws.
 - (d) “**Supervisory Authority**” (as used in the Addendum) includes Colombia’s Superintendency of Industry and Commerce (Superintendencia de Industria y Comercio).
- 8.3. When acting as a Processor or Sub-Processor in connection with the Processing of GPI Personal Data, Vendor shall comply with all requirements applicable to Processors under the Colombian Data Protection Laws, including but not limited to obligations under Article 18 of Data Protection Law No. 1581 and Articles 11, 23, and 25 of the Data Protection Decree. Vendor shall also comply with GPI’s Information Processing Policy, if any.

- 8.4. The Addendum sets out the additional required contractual elements under Article 25 of the Data Protection Decree, such as the scope of Processing, the activities that Vendor is authorized to perform on GPI's behalf, Vendor's obligations relative to GPI and Data Subjects, and Vendor's obligations to safeguard the security and confidentiality of Personal Data.

9. European Economic Area

9.1. Definitions

- (a) “**EEA**” (as used in this Section) means the European Economic Area, consisting of the EU Member States, and Iceland, Liechtenstein, and Norway.
- (b) “**EEA Data Protection Laws**” (as used in this Section) means the GDPR and all laws and regulations of the EU and the EEA countries applicable to the Processing of GPI Personal Data.
- (c) “**EU 2021 SCCs**” (as used in these Jurisdiction Specific Terms) means the contractual clauses adopted by the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on SCCs for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

- 9.2. With regard to any Restricted Transfer subject to EEA Data Protection Laws from GPI to Vendor, one of the following transfer mechanisms shall apply, in the following order of precedence:

- (a) A valid adequacy decision adopted by the European Commission on the basis of Article 45 of the GDPR
- (b) The appropriate SCCs adopted by the European Commission from time to time.
- (c) Any other lawful data transfer mechanism, as laid down in EEA Data Protection Laws, as the case may be.

9.3. SCCs:

- (a) The Addendum hereby incorporates by reference the SCCs. The Parties are deemed to have accepted, executed, and signed the SCCs where necessary in their entirety (including the annexures thereto)
- (b) The Parties agree that any references to sections, annexures, exhibits, modules and choices within the SCCs as set out in this Section 9.3 of these Jurisdiction Specific Terms, shall be deemed to be the same as the cognate and corresponding references to sections, annexures, exhibits, modules and choices within any appropriate, updated SCCs as may be applicable from time to time pursuant to the Addendum.
- (c) For the purposes of the annexures to the EU 2021 SCCs and any substantially similar SCCs which may be adopted by the relevant authorities in the future:
 - i. Annex I(A): The content of Annex I(A) is set forth in Part A of Annex I, Exhibit A to the Addendum.
 - ii. Annex I(B): The content of Annex I(B) is set forth in Part B of Annex I, Exhibit A to the Addendum.
 - iii. Annex I(C): The content of Annex I(C) is set forth in Section 9.3(d) of these Jurisdiction Specific Terms.
 - iv. Annex II: The content of Annex II is set forth in Annex II, Exhibit A to the Addendum.

- v. Annex III: The contents of Annex III is set out in Annex III, Exhibit A to the Addendum.
 - vi. The Parties agree to apply the following modules:
 - (A) With respect to any Controller-to-Processor Restricted Transfers, the Parties agree to implement Module Two of the EU 2021 SCCs.
 - (B) With respect to any Processor-to-Sub-Processor Restricted Transfers of EEA Personal Data, the Parties agree to implement Module Three of the EU 2021 SCCs.
 - (C) With respect to any Processor-to-Controller Restricted Transfers of EEA Personal Data, the Parties agree to implement Module Four of the EU 2021 SCCs.
- (d) The Parties further agree to the following choices under the EU 2021 SCCs:
- i. Clause 7: The Parties choose not to include the optional docking clause.
 - ii. Clause 9(a): The Parties choose Option 2, “General Written Authorization,” and the time period set forth in Section 4.5 of the Addendum. The procedures for designation and notification of new Sub-processors are set forth in more detail in Section 4.5 of the Addendum.
 - iii. Clause 11: The Parties choose not to include the optional language relating to the use of an independent dispute resolution body.
 - iv. Clause 13 (Annex I.C): The competent Supervisory Authority is as follows:
 - (A) If the Data Exporter is established in an EU member state, the competent Supervisory Authority shall be the Supervisory Authority for that member state.
 - (B) If the Data Exporter is not established within an EU member state, but the Data Exporter falls within the territorial scope of the GDPR pursuant to Article 3(2) and has appointed a Data Protection Representative, the competent Supervisory Authority shall be the Supervisory Authority in the member state where the Data Exporter’s Data Protection Representative is established.
 - (C) If the Data Exporter is not established in an EU Member State, but the Data Exporter falls within the territorial scope of the GDPR pursuant to Article 3(2) and has not appointed a Data Protection Representative, the competent Supervisory Authority shall be the Supervisory Authority of one of the Member States in which the Data Subjects whose Personal Data is transferred under the SCCs in relation to the offering of goods or services to them, or whose behaviour is monitored, are located. If one of those Member States is Ireland, then the competent Supervisory Authority is the Irish Data Protection Commission. If one of those Member States is not Ireland, then the Data Exporter shall select the competent Supervisory Authority and provide its selection to the Data Importer by sending an email to the applicable email address as set forth in Exhibit A to the Addendum. The Parties shall then agree on the competent Supervisory Authority.
 - v. Clause 17: The clauses shall be governed by the laws of the Republic of Ireland.
 - vi. Clause 18: The Parties agree that any dispute arising from the SCCs shall be resolved by the courts of the Republic of Ireland.

9.4. The terms contained in Annex IIB, Exhibit A to the Addendum supplement the SCCs.

- 9.5. In cases where the SCCs apply and there is a conflict between the terms of the Addendum and the terms of the SCCs, the terms of the SCCs shall prevail with regard to the Restricted Transfer in question.

10. Israel

- 10.1. Wherever the Processing pursuant to the Addendum falls within the scope of Israel's Protection of Privacy Law, 1981, the Protection of Privacy Regulations (Data Security) 5777-2017 ("**PPL Regulations**"), and any corresponding decrees, regulations, or guidance (collectively "**Israeli Data Protection Laws**"), the provisions of the Addendum and this Section shall apply to such Processing.
- 10.2. For purposes of Article 15 of the PPL Regulations, to the extent that Vendor acts as an external Vendor (ספק שירות) as that term is construed under Israeli Data Protection Laws, Exhibit A to the Addendum contains information about the Personal Data that Vendor shall Process, the purposes of the Processing, the database systems (if any) that Vendor will access in connection with the Processing, the types of Processing that Vendor will perform, the duration of the Processing, and the security measures that Vendor has implemented to protect Personal Data.
- 10.3. Vendor shall notify GPI in the event of a Security Incident and shall notify GPI, at least once annually (and in a format to be agreed upon by the Parties), on the manner in which Vendor has implemented its obligations in this Section.

11. Switzerland

11.1. Definitions

- (a) "**FDPIC**" (as used in this Section) means the Swiss Federal Data Protection and Information Commissioner.
- (b) "**Swiss Data Protection Laws**" (as used in this Section) includes the Federal Act on Data Protection of 19 June 1992 ("**FADP**") and the Ordinance to the Federal Act on Data Protection.

11.2. With regard to any Restricted Transfer subject to Swiss Data Protection Laws from GPI to Vendor within the scope of the Addendum, one of the following transfer mechanisms shall apply, in the following order of precedence:

- (a) The inclusion of the Third Country, a territory, or one or more specified sectors within that Third Country, or the international organization in question to which GPI Personal Data is to be transferred in the list published by the Swiss Federal Data Protection and Information Commissioner of states that provide an adequate level of protection for GPI Personal Data within the meaning of the FADP.
- (b) The SCCs (insofar as their use constitutes an "appropriate safeguard" under Swiss Data Protection Laws).
- (c) Any other lawful transfer mechanism, as laid down in Swiss Data Protection Laws.

11.3. SCCs:

- (a) The Addendum hereby incorporates by reference the SCCs, which have been adopted for use by the FDPIC with certain modifications. The Parties are deemed to have accepted, executed, and signed the SCCs where necessary in their entirety (including the annexures thereto).

- (b) The Parties incorporate and adopt the SCCs for Restricted Transfers subject to Swiss Data Protection Laws in the same manner set forth in Section 9.3 of these Jurisdiction Specific Terms, subject to the following:
- i. Clause 13 (Annex I.C): The competent authority shall be the FDPIC. Nothing about the Parties' designation of the competent Supervisory Authority shall be interpreted to preclude Data Subjects in Switzerland from applying to the FDPIC for relief.
 - ii. Clause 17: The clauses shall be governed by the laws of Switzerland.
 - iii. Clause 18: The Parties agree that any dispute arising from the SCCs shall be resolved by the courts of Switzerland. The Parties' selection of forum may not be construed as forbidding Data Subjects habitually resident in Switzerland from suing for their rights in Switzerland.
 - iv. References to "Regulation (EU) 2016/679" and specific articles therein shall be replaced with references to the FADP and the equivalent articles or sections therein, insofar as there any Restricted Transfers subject to Swiss Data Protection Laws.
 - v. The SCCs also protect the data of legal entities until the entry into force of the revised FADP.

11.4. In cases where the SCCs apply and there is a conflict between the terms of the Addendum and the terms of the SCCs, the terms of the SCCs shall prevail with regard to the Restricted Transfer in question.

12. Turkey

When applicable, the Processing of GPI Personal Data shall be compliant with Turkey's Personal Data Protection Law No. 6698 of 2016, Electronic Communications Law No. 5809 of 2008, the Personal Data in the Electronic Communications Sector Processing and Protection of Privacy Related Regulation (2020), and any corresponding decrees, regulations, or guidance.

13. United Kingdom

13.1. Definitions

- (a) "**UK Data Protection Laws**" (as used in this Section) includes the Data Protection Act 2018 and the UK GDPR (as defined below).
- (c) "**UK GDPR**" (as used in this Section) means the United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.
- (d) "**UK ICO**" (as used in this Section) means the UK Information Commissioner's Office.
- (e) "**UK IDTA**" (as used in this Section) means the International Data Transfer Agreement issued pursuant to Section 119A(1) of the Data Protection Act 2018 and approved by the UK Parliament.

13.2. With regard to any Restricted Transfer subject to UK Data Protection Laws from GPI to Vendor within the scope of the Addendum, one of the following transfer mechanisms shall apply, in the following order of precedence:

- (a) A valid adequacy decision adopted pursuant to Article 45 of the UK GDPR.
- (b) The UK IDTA.
- (c) Any other lawful data transfer mechanism, as laid down in the UK Data Protection Laws, as the case may be.

13.3. UK IDTA:

- (a) The Addendum hereby incorporates by reference the UK IDTA. The Parties are deemed to have accepted, executed, and signed the UK IDTA where necessary in its entirety.
- (b) For the purposes of the tables to the UK IDTA:
 - i. Table 1: The information required by Table 1 appears within Annex I, Exhibit A to the Addendum.
 - ii. Table 2:
 - (A) The UK IDTA, shall be governed by the laws of England and Wales.
 - (B) The Parties agree that any dispute arising from the UK IDTA shall be resolved by the courts England and Wales.
 - (C) The Parties' controllership and data transfer roles are set out in Annex I, Exhibit A to the Addendum.
 - (D) Whether the UK GDPR applies or does not apply to the Data Importer's Processing of the Personal Data is set out in Annex I, Exhibit A to the Addendum.
 - (E) The Addendum and the Terms set out the instructions for Processing Personal Data.
 - (F) The Data Importer shall Process Personal Data for the time period set out in Annex I, Exhibit A to the Addendum. The Parties agree that neither Party may terminate the UK IDTA before the end of such time period.
 - (G) The Data Importer may only transfer Personal Data to authorized Sub-processors (if applicable), as set out within Section 4.5 of the Addendum, or to such third parties that the Data Exporter authorizes in writing or within the Terms.
 - (H) Each Party must review the Addendum at regular intervals, to ensure that the Addendum remains accurate and up to date and continues to provide appropriate safeguards to the Personal Data. Each Party will carry out these reviews as frequently as at least once each year or sooner.
 - iii. Table 3: The content of Table 3 is set forth in Annex I, Exhibit A to the Addendum and may be updated in accordance with Sections 3 and 6.1 of the Addendum.
 - iv. Table 4: The content of Table 4 is set forth in Annex II, Exhibit A to the Addendum and may be updated in accordance with Sections 3, 4.4, and 6.1 of the Addendum.
- (c) Part 2 (Extra Protection Clauses) and Part 3 (Commercial Clauses) of the UK IDTA are noted throughout the Addendum.
- (d) The terms contained in Annex IIB, Exhibit A to the Addendum supplement the UK IDTA.
- (e) In cases where the UK IDTA applies and there is a conflict between the terms of the Addendum and the terms of the UK IDTA, the terms of the UK IDTA shall prevail.