



4201 Wilson Blvd, Suite 504
North Tower,
Arlington, VA 22203
703-442-5500
www.gtt.net

SUPPLIER DATA PROCESSING AGREEMENT

THIS SUPPLIER DATA PROCESSING AGREEMENT ("DPA") is made on _____ BETWEEN

- (1) **GTT Communications, Inc.**, a company incorporated and registered in the State of Delaware whose registered office is at 4201 Wilson Blvd, Suite 504, Arlington, VA 22203, USA, and its Affiliates (to the extent designated on a Service Order Form) (the providing entity being "**GTT**"); and
- (2) _____, a company incorporated and registered under the laws of _____, whose registered office is at _____ (the "**Supplier**"),

each referred to as a "**party**" and together "**the parties**."

GTT has engaged the Supplier to provide goods, services, or other deliverables (the "**Services**") as described in the underlying agreements, contracts, orders, or statements of work governing Supplier's provision of the Services to GTT (the "**Terms**"). In connection with the provision of the Services, the Supplier may have access to or process GTT Personal Data (defined below). As such, the Parties agree to the terms of this DPA relating to Supplier's Processing of GTT Personal Data.

1. INTERPRETATION

- 1.1 The terms "**Controller**," "**Data Subject**," "**Business**," "**Service Provider**," "**Personal Data**," "**Processing**," "**Processor**," "**Special Category Data**," and "**Supervisory Authority**" shall have meanings ascribed under Data Protection Laws, or where not specifically defined, the same meaning as analogous terms under Data Protection Laws.

1.2 **Defined Terms:** In this DPA:

"**Data Protection Laws**" means all international, federal, state, and local laws, regulations, rules, guidance and recommendations issued by any government, agency, or authority relating to privacy and data protection that apply to the Processing of GTT Personal Data by the Parties, including but not limited to, the California Privacy Rights Act of 2020 ("CCPA"), the GDPR, and UK GDPR;

"**GDPR**" means the General Data Protection Regulation (Regulation (EU) 2016/679);

"**GTT Personal Data**" means any Personal Data disclosed by, made available by, or collected or generated on behalf of GTT as part of the Services;

"**Personnel**" means those employees and other personnel of the Supplier to whom disclosure of or access to Personal Data is necessary as part of providing the Services; and

“UK GDPR” 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.

2. STATUS OF THE PARTIES

- 2.1 The parties acknowledge that this DPA applies to the Terms if and to the extent that Supplier is processing GTT Personal Data under the Terms where (i) GTT acts as a Controller and Supplier acts as a Processor for GTT, or (ii) GTT acts as a Processor and Supplier acts as a sub-processor for GTT. In those cases, GTT's engagement of Supplier is conditioned upon Supplier's agreement to the terms and conditions of this DPA.

3. SUPPLIER OBLIGATIONS

- 3.1 The Supplier shall:

- (a) process GTT Personal Data strictly in accordance with GTT's written instructions, including as described in this DPA and in accordance with the nature and purpose of the processing set out in Schedule 1;
- (b) process GTT Personal Data at all times in compliance with Data Protection Laws, including any applicable jurisdiction-specific provisions in Schedule 4;
- (c) promptly inform GTT: (a) if, in Supplier's reasonable assessment, following GTT's instructions would result in a violation of applicable Data Protection Laws; (b) where Supplier must disclose GTT Personal Data in response to a legal obligation (unless the legal obligation prohibits Supplier from making such disclosure); or (c) if Supplier is unable to meet the requirements of this DPA at any point during the course of the Agreement. If Supplier is legally required to process GTT Personal Data in a manner not instructed by GTT, then it shall notify GTT without undue delay before such processing occurs (unless the law requiring such processing prohibits Supplier from providing such notification on an important ground of public interest, in which case Supplier shall notify GTT as soon as that law permits Supplier to do so).
- (d) disclose GTT Personal Data only to those Personnel to whom such disclosure is necessary to perform the Services and only if such Personnel are subject to confidentiality requirements by contract or appropriate statutory obligations;
- (e) not sell, share (as that term is defined under the CCPA), transfer, disclose or otherwise allow access to any GTT Personal Data to any party other than its Personnel pursuant to subprovision (c). Additionally, Supplier shall not combine GTT Personal Data with other Supplier Personal Data;
- (f) take all steps reasonably required to ensure that GTT Personal Data is accurately recorded and kept up to date;

- (g) not sub-contract, delegate, or purport to transfer to any third party any of its obligations under the Terms or the DPA or otherwise to perform the Services (i) without GTT's prior written consent (for the avoidance of doubt, GTT has authorized the engagement of the sub-processors set out in Schedule 2), (ii) without the third party contractually bound to obligations that are substantively equivalent to the provisions of this DPA, and (iii) without complying with any applicable onward transfer requirements under Data Protection Laws. Supplier shall remain at all times responsible for and fully liable to GTT for the sub-processors' performance of its obligations. For the avoidance of doubt, GTT authorizes the engagement of the sub-processors listed in Schedule 2 as of the effective date of this DPA. Supplier shall inform GTT of any intended changes concerning the addition or replacement of sub-processors, to which changes GTT has the right to object at its sole discretion within thirty (30) days. If GTT is acting as a Processor and Supplier is acting as a sub-processor, then an objection by any of GTT's Controller customers will be deemed a reasonable objection relating to the protection of the GTT Personal Data; and
- (h) make available to GTT all information reasonably necessary to demonstrate Supplier's compliance with Data Protection Laws, the Terms, or this DPA.

4. INTERNATIONAL DATA TRANSFERS

- 4.1 Where GTT transfers GTT Personal Data to Supplier, either directly or via onward transfer, Supplier shall Process the GTT Personal Data in accordance with all applicable laws, including Data Protection Laws, and with any applicable transfer requirements found in the relevant jurisdiction specific provisions in Schedule 4, to the extent that they apply to the transfer.
- 4.2 In the event of any conflict between the Terms or this DPA and the applicable jurisdiction specific provisions in Schedule 4, then precedence shall be given to the applicable jurisdiction specific provisions in Schedule 4.
- 4.3 In the event that the applicable jurisdiction specific provisions set forth in Schedule 4 are amended, replaced, or repealed under Data Protection Laws, the Parties shall work together in good faith to enter into any updated version of the jurisdiction specific provisions (to the extent required) or negotiate in good faith a solution to enable transfers of GTT Personal Data to be conducted in compliance with Data Protection Laws. GTT can terminate the Terms and this DPA without penalty if the parties are unable to come to an agreement pursuant to this provision.

5. SECURITY AND DATA BREACHES

- 5.1 Supplier shall implement reasonable and appropriate technical, organizational, and physical measures to prevent accidental or unauthorized processing, loss, destruction, damage, alteration, of GTT Personal Data or any unlawful or unauthorized access to GTT Personal Data in Supplier's custody, and Supplier shall ensure that its Personnel are aware of and comply with those measures. These security measures shall include at minimum the measures specified in Schedule 3 and any additional measures that GTT may specify or that are otherwise required by applicable laws. Supplier shall maintain strict logical or physical separation between GTT Personal Data and data belonging to Supplier or its other customers.

- 5.2 Supplier shall notify GTT of any suspected unauthorized access to or unauthorized use, alteration, disclosure, accidental loss or destruction of any Personal Data in the custody of the Supplier or for which Supplier is otherwise responsible under the Agreement (each a “**Data Breach**”). This notice must be delivered as soon as practicable and no later than 48 hours upon Supplier's becoming aware of a suspected Data Breach.
- 5.3 Upon becoming aware of a suspected Data Breach, Supplier shall:
- (a) at its own cost and expense, investigate and analyze the cause and extent of such Data Breach and take steps necessary to contain and remediate the Data Breach;
 - (b) at its own cost and expense, provide regular updates on the status and key findings of the investigation mentioned in subprovision (a) and provide any documents requested regarding the investigation and remediation steps taken by Supplier;
 - (c) at its own cost and expense, take any and all steps directed by GTT in its sole reasonable judgment to remediate the Data Breach, including but not limited to notifying government authorities, or other persons; or undertaking other remedial measures (including, without limitation, notice, credit monitoring, or call center services);
 - (d) at its own cost and expense, provide GTT with any information reasonably requested from GTT or GTT's customers, including information required to comply with obligations under Data Protection Laws.
- 5.4 GTT has final approval over the content, form, and timing of any notice regarding the data breach being delivered to regulatory authorities or data subjects whose Personal Data was found within the GTT Personal Data.
- 5.5 Supplier warrants and represents that it has an incident response plan that includes procedures to be followed in the event of any actual or potential Data Breach.
6. **DATA SUBJECT REQUESTS; COMPLAINTS**
- 6.1 Supplier shall as soon as practicable (and no later than 5 business days) notify GTT of any request to exercise rights under Data Protection Laws or complaint if the request or complaint is from a data subject whose Personal Data is found within the GTT Personal Data.
- 6.2 Supplier shall not comply with any request from or respond to any complaint from a data subject whose Personal Data is found within the GTT Personal Data except on GTT's written instructions.
- 6.3 Supplier shall provide appropriate technical and organizational measures to enable GTT to fulfil its obligations to respond to data subject rights requests.

7. **AUDIT RIGHTS**

- 7.1 Supplier shall, at no additional cost, keep full and accurate records relating to all Processing of GTT Personal Data on behalf of GTT as part of the Processing Services, and GTT may request, upon ten (10) days written notice to Supplier (unless a shorter period is required to meet a legal requirement or request by a government authority), access to Supplier's facilities, systems, records, and supporting documentation in order to audit, itself or through an independent third-party auditor, Supplier's compliance with its obligations under or related to this DPA. The audit may be carried out once in any calendar year. Audits shall be subject to all applicable confidentiality obligations agreed to by GTT and Supplier, and shall be conducted in a manner that minimizes any disruption of Supplier's performance of services and other normal operations. In the event that any such audit reveals material gaps or weaknesses in Supplier's security program, GTT shall be entitled to suspend transmission of Personal Data to Supplier and terminate Supplier's Processing of Personal Data until such issues are resolved. GTT may also require Supplier to, upon request, make available to GTT, any information or certifications necessary to demonstrate compliance with the obligations set forth in this DPA.

8. **DEIDENTIFIED DATA**

- 8.1 Supplier shall not Process GTT Personal Data to create deidentified data without first obtaining authorization from GTT.

9. **DESTRUCTION AND DELIVERY OF DATA**

- 9.1 Supplier shall, upon termination of this DPA and upon GTT's request at any time, immediately and securely return to GTT or destroy all GTT Personal Data and certify such return or destruction in writing to GTT within 30 days, unless Supplier is required to retain GTT Personal Data for regulatory or legal compliance, in which case Supplier shall: (i) notify GTT that it is retaining GTT Personal Data in accordance with applicable law; (ii) at GTT's request, provide all necessary information to allow GTT to verify that Supplier is subject to a legal obligation to retain the data; (iii) inform GTT about the types of GTT Personal Data retained and the duration of retention; (iv) process the retained data only as strictly necessary to comply with applicable laws to which Supplier is subject; and (v) securely delete the retained GTT Personal Data once retention is no longer necessary to comply with applicable laws to which Supplier is subject.

10. **INDEMNITY**

- 10.1 The Supplier shall indemnify, defend and hold harmless GTT on demand from and against any and all claim, suit, proceeding, judgment, loss, liability, cost, expense (including, without limitation, reasonable attorneys' fees, court costs, and expert witness costs), fee, penalty or fine ("**Loss**") suffered or incurred by GTT, arising out of or in connection with Supplier's provision of the Services or alleged breach of its obligations under Data Protection Laws, the Terms, or this DPA, including any liabilities resulting from a Data Breach.

11. **TERM AND TERMINATION**

- 11.1 **Commencement:** It is agreed, notwithstanding the date of execution of this DPA, that the relationship between the parties regarding the subject matter of this DPA shall be deemed to have been governed by this DPA since the date of the Terms (if that agreement is dated earlier than the date of this DPA) as if this DPA had been executed on or before, and had come into force on, that date. In any other case, this DPA shall come into full force and effect on the date hereof.
- 11.2 **Termination of Terms:** This DPA shall continue in full force and effect until termination or expiry of the Terms whereupon the Supplier's authority to process Personal Data in accordance with this DPA shall terminate automatically, unless otherwise agreed between the parties in writing.
- 11.3 **Survival of Obligations:** The DPA remains in full force and effect for so long as Supplier maintains GTT Personal Data.

12. **GENERAL**

- 12.1 **Severability:** If the whole or any part of a provision of this DPA is or becomes illegal, invalid or unenforceable, that will not affect the legality, validity or enforceability of the remainder of the provision in question or any other provision of this DPA
- 12.2 **Binding on Successors:** This DPA and all of its provisions shall be binding upon and inure to the benefit of the parties and their respective heirs, executors, administrators, successors and permitted assigns.
- 12.3 **Counterparts:** This DPA may be executed in two or more counterparts, each of which shall be deemed to be an original, but all of which together shall constitute one and the same instrument.
- 12.4 **IN WITNESS OF WHICH,** this DPA has been duly executed by the undersigned signatories on behalf of the parties on the date first above written, and each signatory represents and warrants to the party (other than that which he or she represents) that he or she has the authority to sign on behalf of the party which he or she purports to bind.

EXECUTION PAGE

SIGNED for and on behalf of
GTT Communications, Inc.

By: _____

Name: _____

Title: _____

Date: _____

SIGNED for and on behalf of

By: _____

Name: _____

Title: _____

Date: _____

SCHEDULE 1

Details of Processing for Controller-to-Processor Transfers

A. LIST OF PARTIES

Data exporter(s): The data exporter is GTT, acting as a data exporter on behalf of itself and its Affiliates.

Data importer(s): The data importer is the entity identified as the Supplier in this DPA, acting as a data importer on behalf of itself and its Affiliates

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

- ☐ Employees
- ☐ Contractors
- ☐ Applicants
- ☐ Individual Contacts of Customers
- ☐ Consumers/End-Users
- ☐ Other _____

Categories of personal data transferred:

- ☐ Name
- ☐ Address
- ☐ Phone Number
- ☐ Job Title
- ☐ Email Address
- ☐ Country of Residence
- ☐ Other _____

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:

- ☐ Yes
- ☐ No

If Yes, please specify categories of sensitive data transferred: _____

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

Ongoing throughout the duration of this DPA.

Nature of the processing:

Storage, consultation, analysis, communication, and other processing needed to support the purposes noted below.

Purpose(s) of the data transfer and further processing”:

Data Importer will process the Personal Data to provide the contracted services to the Data Exporter.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

The Data Importer may retain Personal Data for the duration of the DPA. Data Importer will retained and deleted the personal data in accordance with the DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

Data Importer Sub-processors may process, transfer and retain personal data in accordance with the DPA

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The competent supervisory authority shall be the supervisory authority which is competent to supervise the activities of the Data Exporter.

SCHEDULE 2

List of Supplier's sub-processors to be provided by Supplier

Subprocessor (Name, legal form)	Processing location	Type of service

Schedule 3

Technical and Organizational Measures

Supplier to provide their Technical and Organizational Measures

Schedule 4

Jurisdiction Specific Provisions

- 1.1 The terms below shall have the following meanings ascribed to them for the purposes of Schedule 4.

"Data Exporter" means GTT when exporting Personal Data to Supplier in circumstances where the Personal Data are transferred from one country to another directly or by onward transfer; and

"Data Importer" means Supplier when importing Personal Data from GTT in circumstances where the Personal Data are transferred from one country to another directly or by onward transfer.

I. European Economic Area

- A. The terms below shall have the following meanings ascribed to them for the purposes of this Section I:

1. **"C-to-P Transfer Clauses"** means Module Two (Controller-to-Processor) within the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
2. **"P-to-P Transfer Clauses"** means Module Three (Processor-to-Processor) within the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
3. **"Europe"** means the European Economic Area.
4. **"European Data Protection Laws"** means any applicable laws of Europe that relate to the Processing of GTT Personal Data under the Terms.
5. **"Transfer Clauses"** means either the C-to-P Transfer Clauses or the P-to-P Transfer Clauses, as the case may be.

- B. When Data Exporter transfers GTT Personal Data subject to European Data Protection Laws, either directly or via onward transfer, to Data Importer located in a country that does not ensure an adequate level of protection within the meaning of European Data Protection Laws, the Parties agree to Process the transferred GTT Personal Data in accordance with the Transfer Clauses as follows:

- 1.1.1 if the Data Exporter acts as a Controller of that Personal Data, the Parties shall comply with the terms of the C-to-P Transfer Clauses; and
- 1.1.2 if the Data Exporter acts as a Processor of that Personal Data, the Parties shall comply with the terms of the P-to-P Transfer Clauses.

- C. For the purposes of C-to-P Transfer Clauses the following additional provisions shall apply:

- 1.1.1 The contents of Schedule 1 to this DPA shall form Annex I to the C-to-P Transfer Clauses;
- 1.1.2 The Parties' signature to this DPA shall be considered as signature to the C-to-P Transfer Clauses.
- 1.1.3 Clause 7 (Docking Clause) shall apply.
- 1.1.4 Option 2 under paragraph (a) of Clause 9 (Use of sub-processors) shall apply and "[Specify time period]" be replaced with "thirty (30) business days".

- 1.1.5 The option under Clause 11 (Redress) shall not apply.
 - 1.1.6 For the purposes of paragraph (a) of Clause 13 (Supervision), each “[“ and “]” shall be deleted in their entirety.
 - 1.1.7 The governing law for the purposes of Clause 17 (Governing law) shall be the law of the Netherlands.
 - 1.1.8 The courts under Clause 18 (Choice of forum and jurisdiction) shall be the courts of the Netherlands.
 - 1.1.9 The Dutch Data Protection Authority shall act as competent supervisory authority for the purposes of Annex I.C of the C-to-P Transfer Clauses (Competent Supervisory Authority).
 - 1.1.10 The contents of Schedule 3 shall form Annex II of the C-to-P Transfer Clauses (Technical and organisational measures including technical and organisational measures to ensure the security of the data).
- D. For the purposes of P-to-P Transfer Clauses the following additional provisions shall apply:
- 1.1.11 The contents of Schedule 2 to this DPA shall form Annex I to the P-to-P Transfer Clauses;
 - 1.1.12 The Parties' signature to this Agreement shall be considered as signature to the P-to-P Transfer Clauses.
 - 1.1.13 Clause 7 (Docking Clause) shall apply.
 - 1.1.14 Option 2 under paragraph (a) of Clause 9 (Use of sub-processors) shall apply and “[Specify time period]” be replaced with “thirty (30) business days”.
 - 1.1.15 The option under Clause 11 (Redress) shall not apply.
 - 1.1.16 For the purposes of paragraph (a) of Clause 13 (Supervision), each “[“ and “]” shall be deleted in their entirety.
 - 1.1.17 The governing law for the purposes of Clause 17 (Governing law) shall be the law of the Netherlands.
 - 1.1.18 The courts under Clause 18 (Choice of forum and jurisdiction) shall be the courts of the Netherlands.
 - 1.1.19 The Dutch Data Protection Authority shall act as competent supervisory authority for the purposes of Annex I.C of the P-to-P Transfer Clauses (Competent Supervisory Authority).
 - 1.1.20 The contents of Schedule 3 shall form Annex II of the P-to-P Transfer Clauses (Technical and organisational measures including technical and organisational measures to ensure the security of the data).

II. **Switzerland**

- A. For the purposes of this Section II, the term “**Swiss Data Protection Laws**” means Switzerland's Federal Act on Data Protection of June 19, 1992, the Ordinance to the Federal Act on Data Protection, and the Ordinance on Data Protection Certification, and all Swiss laws relating to the Processing, privacy, protection, or use of Personal Data.
- B. When Data Exporter transfers Personal Data subject to Swiss Data Protection Laws, either directly or via onward transfer, to a Data Importer located in a country that does not ensure an adequate level of protection within the meaning of Swiss Data Protection Laws, the Parties agree to the Transfer Clauses in accordance with Section I of this

C. The following additional provisions shall apply so that the Transfer Clauses are suitable for providing an adequate level of protection for such transfer under Swiss Data Protection Laws:

1. "FDPIC" means the Swiss Federal Data Protection and Information Commissioner.
2. "Revised FADP" means the revised version of the Federal Act of Data Protection ("FADP") of 25 September 2020, which is scheduled to come into force on 1 January 2023.
3. The term "EU Member State" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility for suing their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c).
4. The Transfer Clauses also protect the data of legal entities until the entry into force of the Revised FADP.
5. The FDPIC shall act as the "competent supervisory authority" insofar as the relevant data transfer is governed by the FADP.

III. United Kingdom

A. The terms below shall have the following meanings ascribed to them for the purposes of this Section III:

1. "UK" means the United Kingdom.
2. "UK Data Protection Laws" means the UK GDPR, Data Protection Act of 2018, and all UK laws relating to the Processing, privacy, protection, or use of Personal Data.
3. "UK GDPR" 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.

B. When Data Exporter transfers Personal Data subject to UK Data Protection Laws, either directly or via onward transfer, to a Data Importer located in a country that does not ensure an adequate level of protection within the meaning of UK Data Protection Laws, the Transfer Clauses shall apply and be interpreted as follows:

1. The Transfer Clauses shall be read and interpreted in the light of the provisions of UK Data Protection Laws, and so that they fulfil the intention for them to provide the appropriate safeguards as required by UK Data Protection Laws as applicable.
2. The Transfer Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in UK Data Protection Laws.
3. The Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the Information Commissioner's Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under section 18 of those Mandatory Clauses, shall apply.
4. The information required by Part 1, Tables 1 to 3 of the Approved Addendum is set out in Schedules 1, 2, 3, and 4 of this DPA (as applicable).
5. For the purposes of Part 1, Table 4 of the Approved Addendum, neither party may end the Approved Addendum when it changes.