

ANNEXE TO THE DATA PROTECTION POLICY

1 Definitions

- 1.1 For the purposes of this Annexe, capitalised terms (singular or plural) have the meaning listed in article 12.
- 1.2 The terms "data subjects", "processing", "controller", "file owner" and "subcontractor" used in this Annexe have the meaning given to them by the GDPR or the Swiss Protection Legislation on data protection, according to their respective scope.

2 Data protection legislation

The Parties acknowledge and agree that the following data protection legislation may, depending on the circumstances, apply to the processing of Personal Data:

- a. the EU General Data Protection Regulation;
- b. Swiss data protection legislation;

3 Data processing

3.1 Roles and compliance

- 3.1.1 Responsibility of the subcontractor and the data controller/file owner. If the EU General Data Protection Regulation, and respectively the Swiss Data Protection Legislation, applies to the processing of Personal Customer Data, the Parties acknowledge and agree that:
- a. T2i is a subcontractor of the Personal Customer Data under the EU General Data Protection Regulation, and respectively the Swiss Data Protection Legislation;
 - b. the Customer is a data controller and respectively a file owner or subcontractor of a third-party, as the case may be, for this Personal Customer Data under the EU General Data Protection Regulation, and respectively the Swiss Data Protection Legislation; and
 - c. each Party shall comply with its obligations under the EU General Data Protection Regulation and/or the Swiss Data Protection Legislation with respect to the processing of Personal Customer Data.
- 3.1.2 Authorisation by a third-party controller. If the EU General Data Protection Regulation applies to the processing of the Personal Customer Data and the Customer is a subcontractor of a third-party, the Customer guarantees to T2i that the Customer's instructions and actions regarding the Personal Customer Data, including the appointment of T2i for the performance of the Services as another subcontractor, have been expressly authorised by the respective controller.

3.1.3 Other legislations. If the other States' Data Protection Legislation applies to the processing of the Personal Customer Data, the Customer agrees, in regard to T2i, to comply with all legislation applicable to the processing of Personal Customer Data and to inform T2i in writing of any provision contained in such legislation that may have an impact on the processing of Personal Customer Data by T2i as the Customer's subcontractor.

3.2 **Scope of processing**

3.2.1 Processing type and purpose. T2i shall process Personal Customer Data that is transmitted, stored, or processed in any other way by the Customer (or any person or entity acting for the Customer) via the Services for the purpose of providing the Services and the associated technical support to the Customer in accordance with this Annexe.

3.2.2 Customer Instructions. By accepting this Addendum, the Customer instructs T2i to process Personal Customer Data only in strict compliance with applicable legislation and, moreover:

- a. if the EU General Data Protection Regulation applies, only to provide the Services and associated technical support as listed (i) in any applicable Contract, including this Addendum, or (ii) in any other written document;
- b. if the Swiss Data Protection Legislation applies to the processing of Personal Customer Data with regard to processing that the Customer would be entitled to perform itself and provided that no legal or contractual confidentiality obligation prohibits intervention by T2i.

3.2.3 T2i compliance with the instructions. Starting on the Effective Date, T2i shall comply with the instructions described in section 3.2.2 unless legislation applicable to T2i requires Customer Data to be subject to specific processing.

3.3 **Category of personal data and data subjects**

If the GDPR applies to the processing of your data as part of your collaboration with T2i, the information relating to the categories of personal data and data subjects must be included in your contract with T2i.

The Customer agrees to provide T2i with a list of the categories of Personal Customer Data that T2i may have access to during the Service, as well as a list of the categories of data subjects. The Customer shall provide this information by sending it to T2i at the address mentioned in section 10 "T2i Data Protection Contact".

If you do not send the required information, T2i shall assume that it will be able to access all types of data provided by the Customer, which may include all categories of Personal Customer Data, and will be able to process all Personal Customer Data relating to all categories of data subjects during the Services. T2i is not responsible for your failure to provide this information in a timely manner.

4 **Data deletion**

4.1 **Deletion during the Period of Validity.** T2i allows the Customer to delete or modify Personal Customer Data during the Period of Validity provided that such deletion is compatible with the functionality of the Services.

- 4.2 **Deletion after the Period of Validity.** The Customer irrevocably requests T2i to delete all Customer Data (including any copies that may exist) from the T2i systems after the Period of Validity in accordance with applicable law. T2i shall comply with this instruction as soon as possible, unless T2i is retaining any Customer Data for a technical or legal reason. The Customer acknowledges and accepts that it is personally responsible for transferring and/or saving any Customer Data that it wishes to keep thereafter.

5 Data security

5.1 Security measures

- 5.1.1 T2i security measures. T2i implements and maintains appropriate technical and organisational measures to protect Customer Data against security incidents. These measures include:

- infrastructure to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- infrastructure to limit access to Customer Data only to staff who need access to it in connection with providing the Services;
- infrastructure to restore the availability of Personal Customer Data and access to this data promptly in the event of a Security Incident;
- a procedure to regularly test, analyse and evaluate the effectiveness of technical and organisational measures to ensure secure processing.

- 5.1.2 Security compliance by T2i staff. T2i shall take appropriate measures to require compliance with the afore mentioned security measures by its staff and subcontractors by ensuring all persons authorised to process Personal Customer Data agree to maintain confidentiality or are subject to an appropriate legal confidentiality obligation.

5.2 Security Incidents

- 5.2.1 Customer notification of Security Incidents. If T2i becomes aware of a Security Incident, T2i agrees to inform the Customer as soon as possible by any useful method (including by contacting the contact person indicated by the Customer). T2i shall describe the nature of the Safety Incident as thoroughly as possible as well as any steps it will take to mitigate potential risks and any measures it recommends the Customer to take. T2i's actions in relation to this Article 5.2.1 shall not constitute and cannot be interpreted as a recognition by T2i of any fault or liability related to the security incident.

- 5.2.2 Customer Obligations. T2i shall not evaluate the content of the Customer Data to identify the type of data concerned. The Customer is solely responsible for performing any analysis of this Customer Data and for complying with any applicable legal provisions, including any obligation to notify a competent authority and/or the data subjects of this Security Incident. In this context, T2i shall provide the Customer with any reasonable assistance requested so it can comply with its obligations.

5.3 Information and audits on security measures

- 5.3.1 **Information.** If the EU General Data Protection Regulation applies to the processing of Personal Customer Data, T2i shall provide the Customer with all documents and information reasonably necessary to demonstrate T2i's compliance with the GDPR and its resulting obligations (in addition to the information contained in the applicable Contract and this Annexe).
- 5.3.2 **Right to audit.** T2i shall authorise the Customer or an independent auditor designated by the Customer to perform audits (including inspections) to verify T2i's compliance with its obligations under the GDPR. T2i shall make a reasonable contribution to the audits described in this Article 5.3.2. Upon completion of the audit, the Customer shall send the complete audit report to T2i at no charge.
- 5.3.3 **Request.** Any request under Articles 5.3.1 or 5.3.2 must be communicated to T2i in writing and indicate (i) the Personal Customer Data concerned, (ii) the reasons for which the conditions referred to in Articles 5.3.1 or 5.3.2 are performed for this data, (iii) the specific documents that are pertinent, respectively the specific obligations of T2i for which the audit is to be carried out and (iv) the Customer's expressed agreement to use the information collected only to ensure T2i's compliance with its obligations in relation to the Personal Customer Data and that the information collected shall not be used in the context of a judicial or administrative procedure against T2i. Except in exceptional circumstances, the Customer may only make one request per year.
- 5.3.4 **Practice.** After T2i receives a request in accordance with Article 5.3.3, and provided that all conditions are fulfilled, T2i shall respond to the request as follows:
- a. For document consultation (Article 5.3.1), T2i shall notify the Customer of the period during which it can consult the documents at the T2i headquarters. Unless expressly agreed otherwise by T2i, the Customer is not authorised to make copies of the consulted documents. Alternatively, T2i may decide to communicate the documents by other methods, such as by sending them electronically;
 - b. For audits (Article 5.3.2), T2i shall notify the Customer of (i) the date(s) when the audits may take place and (ii) the scope of the audit, including the inspections that may be carried out to monitor T2i's compliance with its obligations under this Annexe. The Customer's internal costs, including the costs of the independent auditor it designates, are entirely its own responsibility. T2i may charge the Customer the costs it incurred for setting up and carrying out the audit. T2i may object to any independent auditor appointed by the Customer if it thinks that the auditor is not sufficiently qualified, is a competitor of T2i, or in any other way would not be able to properly complete the task. In this case, the Customer may either perform the audit itself or offer another auditor to T2i.
- 5.3.5 **Confidential information.** The provisions contained in this Article 5.3 shall not be interpreted as requiring T2i to communicate to the Customer (i) any information relating to its business secrets, including any confidential information, or (ii) any information concerning T2i customers (except the Customer). T2i may require that the document consultation (Article 5.3.1) or audit (Article 5.3.2) be subject to the signing of a specific confidentiality agreement.

6 T2i assistance

- 6.1 **Compliance.** T2i shall provide the Customer with all necessary information for the Customer to prove compliance with its obligations under the EU General Data Protection Regulation, and respectively the Swiss Data Protection Legislation. The Customer also agrees to provide T2i with all necessary information for T2i to prove compliance with its obligations under the EU General Data Protection Regulation, and respectively the Swiss Data Protection Legislation.
- 6.2 **Data subject requests.** During the Period of Validity, if T2i receives a request from a data subject concerning Personal Customer Data, T2i shall inform the data subject to submit the request to the Customer, and the Customer shall be responsible for responding to the request. The Parties agree that it is the Customer's sole responsibility to respond to the requests from data subjects.
- 6.3 **Customer actions.** During the Period of Validity, T2i shall provide assistance to a reasonable extent for the Customer to comply with its legal obligations related to data subjects, if this assistance is compatible with the functionality of the Services. The measures shall apply all the rights conferred by legislation on the protection of applicable data, including the access, rectification, limitation, opposition, deletion and portability of its Personal Customer Data.
- 6.4 **Impact analysis and prior consultation.** If the EU General Data Protection Regulation applies to the processing of Personal Customer Data, T2i agrees, to a reasonable extent based on the nature of the processing and information available to it, to assist the Customer to ensure compliance with its obligations in terms of impact analysis and prior consultation in accordance with articles 35 and 36 of the GDPR.

7 Data transfer

- 7.1 **Authorised countries.** Unless otherwise stipulated in the applicable Contract, the Customer agrees that T2i shall store and process Customer Data in Switzerland, France, Canada and any other member country of the European Union or shall provide an adequate level of personal data protection, which T2i or one of its subcontractors shall maintain the logistics of.
- 7.2 **Special authorisation.** Unless bound by a legal non-disclosure obligation, T2i shall notify the Customer prior to any transfer of Personal Customer Data to a state not mentioned in Article 7.1. The Customer agrees to authorise this transfer as long as T2i can guarantee an adequate level of protection of the Personal Customer Data by any means available.

8 Sub-delegation

- 8.1 **Consent.** The Customer specifically authorises T2i to use other subcontractors, which may be T2i Affiliated Entities or other third-parties. If the EU General Data Protection Regulation applies, T2i agrees to inform the Customer in advance and in writing of any proposed addition or replacement of subcontractors to give the Customer the opportunity to raise objections against such subcontractors.

- 8.2 **Requirements.** In the case of delegation in accordance with Article 8.1, T2i agrees to ensure in writing that:
- a. the subcontractor only accesses and processes Customer Data to the extent required to fulfil the obligations entrusted to it; and
 - b. if the EU General Data Protection Regulation applies, the obligations set out in Article 28 (3) of the GDPR shall be imposed on the subcontractor;
- 8.3 **Objections.** If the EU General Data Protection Regulation applies, the Customer has a period of 30 days after being informed of the planned subcontractor addition or replacement (including the name and location this subcontractor and the activities it shall carry out) to present its objections. If T2i confirms to the Customer that it shall appoint that subcontractor, the Customer is entitled to terminate the applicable Contract with immediate effect by written notification within 14 days of receiving this confirmation from T2i. This right of cancellation is the Customer's sole and exclusive remedy if it objects to a new subcontractor. If the Customer does not respond within the time limits referred to in this Article 8.3, this shall be construed as an acceptance of the new subcontractor.

9 Register of processing operations.

The Customer acknowledges that T2i may be required, including by the EU General Data Protection Regulation, to: (a) collect and store certain information, including the name and contact details of each subcontractor and/or controller with whom T2i acts and, where appropriate, the local representative of the controller and/or the data protection officer; and (b) make that information available to any competent authority. The Customer agrees to provide T2i with all information that is reasonably necessary for T2i to fulfil its obligations.

10 T2i data protection contact

The T2i contact person for data protection can be contacted by email at the following address : privacy@groupe-t2i.com

11 Customer data protection contact

- 11.1 **Data protection officer.** If the GDPR imposes on the Customer to name a data protection officer, the Customer shall communicate the contact details to T2i. T2i must keep the contact details of the Customer's data protection officer in a register of processing operations. If the Customer does not communicate the contact details of a data protection officer, the Customer confirms that this obligation does not apply to him.
- 11.2 **Contact person.** If the GDPR does not impose on the Customer to name a data protection officer, the Customer can nevertheless communicate to T2i the contact details of the person in charge of the data protection matters. This person will be the first contact of T2i for any communications regarding the data protection. This will make the transfer of information quicker and easier.

12 Definitions

Annexe	this document.
Contract	any agreement, including as amended by amendment if applicable, between the Customer and T2i for the purpose of performing the Services.
Affiliated Entity	any entity controlling, controlled by, or under common control with, a Party. For the purposes of this definition "control" means: (a) the ownership of at least 50% of the entity's capital; (b) the ownership of at least 50% of the voting rights in the entity; or (c) the power to exercise decisive influence over the management of the entity.
Customer Data	data (i) transmitted by the Customer to T2i, or collected by T2i from the Customer, in connection with the execution of the Services (ii) that are kept or processed by T2i.
Personal Customer Data	data of a personal nature, meaning any information relating directly or indirectly to an identified or identifiable natural person, including by reference to an identifier, such as name, identification number, location data, online identifier, or one or more elements specific to its physical, physiological, genetic, psychological, economic, cultural or social identity, according to and in compliance with the data protection legislation applicable to this data contained in the Customer Data.
Security Incident	a security breach resulting in the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of Customer Data or unauthorised access to Customer Data.
Other States' Data Protection Legislation	any data protection legislation other than the Swiss Data Protection Legislation and the EU General Data Protection Regulation.
Swiss Data Protection Legislation	the Federal Data Protection Act of 19 June 1992 in Switzerland and its implementing ordinances. In Switzerland, in case of a public administration, the cantonal Data Protection Legislation applies in priority.
The EU General Data Protection Regulation	(EU) regulation 2016/679 of the European Parliament and Council of 27 April 2016 to protect individual rights to personal data processing and the free movement of such data, which replaces Directive 95/46/EC (GDPR).
Services	all Services provided by T2i to the Customer under a Contract.