

## ITCI Data Processing Terms & Conditions

In the provision of certain services under the terms of the Principal Agreement(s) as defined below, Customer, as controller will require ITCI to process certain personal data received from Customer.

The parties agree that these terms and conditions shall apply to all such processing undertaken by ITCI on behalf of Customer and shall be supplemental to the terms of the Principal Agreement.

### 1. Appointment

Customer as controller of certain personal data appoints ITCI as processor to process the personal data listed in Schedule 1 (the "Data") for the purposes also described in the Schedule 1 (or as otherwise agreed in writing by the parties) (the "**Permitted Purpose**"). Each party shall comply with the obligations that apply to it under Applicable Data Protection Law.

that has executed standard contractual clauses adopted or approved by the European Commission.

### 2. Definitions

In these terms and conditions, the following terms shall have the following meanings:

(a) "**Principal Agreements**": Any agreement between ITCI and Customer under the terms of which ITCI provides services Customer;

(b) "**controller**", "**processor**", "**data subject**", "**personal data**", "**personal data breach**", "**processing**" (and "**process**") and "**special categories of personal data**" and "**supervisory authority**" shall have the meanings given in Applicable Data Protection Law; and

(c) "**Applicable Data Protection Law**" shall mean, where personal data of EU residents is processed (i) prior to 25 May 2018, the EU Data Protection Directive (Directive 95/46/EC); (ii) on and after 25 May 2018, the EU [General Data Protection Regulation \(Regulation 2016/679\)](#), and (iii) where personal data of non-EU residents is processed any applicable privacy law in the relevant jurisdiction.

All other terms shall be as defined in the applicable Principal Agreement.

### 3. International transfers

As a global company ITCI may need to transfer personal data out of the country that the Customer or the data subjects are located. All such transfers shall be in accordance with measures that permit the lawful transfer of personal data out of the EEA such as transferring the personal data to a recipient

### 4. Confidentiality of processing

ITCI shall ensure that any person it authorizes to process the personal data (an "Authorized Person") have committed themselves to preserve the confidentiality of such personal data.

### 5. Security

ITCI shall implement the technical and organizational measures as set out in the Schedule 1 to protect the personal data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorized disclosure of, or access to the personal data.

### 6. Subcontracting

Customer as controller consents to ITCI engaging third party subprocessors mentioned in Schedule 2 to process the Data for the Permitted Purpose. The list of subprocessors mentioned in Schedule 2 shall be updated with details of any change in subprocessors at least 10 days' prior to any such change taking effect; (ii) ITCI imposes data protection terms on any subprocessor it appoints that require it to protect the personal data to the standard required by Applicable Data Protection Law; and (iii) ITCI remains liable for any breach of this Clause that is caused by an act, error or omission of its subprocessor. Customer may object to ITCI's appointment or replacement of a subprocessor prior to its appointment or replacement, provided such objection is based on reasonable grounds relating to data protection. In such event, Customer may require ITCI to suspend or terminate all processing activities (without prejudice to any fees incurred by or committed to by Customer under the terms of the Principal Agreement prior to suspension or termination).

### 7. Cooperation and data subjects' rights

ITCI shall provide reasonable and timely assistance to Customer (at Customer's

expense) to enable Customer to respond to: (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Data. In the event that any such request, correspondence, enquiry or complaint is made directly to ITCI, ITCI shall promptly inform Customer providing full details of the same.

#### **8. Personal Data Breach**

If it becomes aware of a confirmed personal data breach, ITCI shall inform Customer without undue delay and shall provide reasonable information and cooperation to Customer so that Customer can fulfil any data breach reporting obligations it may have under (and in accordance with the timescales required by) Applicable Data Protection Law. ITCI shall further take such any reasonably necessary measures and actions to remedy or mitigate the effects of the personal data breach and shall keep Customer informed of all material developments in connection with the personal data breach.

#### **9. Deletion or return of Personal Data**

Upon termination or expiry of the Principal Agreement, ITCI shall (at Customer's election) destroy or return to Customer all personal data in its possession or control. This requirement shall not apply to the extent that ITCI is required by applicable law to retain some or all of the personal data, or to personal data it has archived on backup systems, which personal data ITCI shall securely isolate and protect from

any further processing except to the extent required by such law.

#### **10. Audit**

Customer acknowledges that ITCI is regularly audited for compliance with various internationally recognized standards as more specifically detailed in the Schedule(s) by independent third party auditors. Upon request, ITCI shall supply a summary / redacted copy of its audit report(s) to Customer, which reports shall be subject to the confidentiality provisions these terms and conditions. ITCI shall also respond to any written audit questions submitted to it by Customer, provided that Customer shall not exercise this right more than once per year. Notwithstanding the foregoing, in the event of an audit request directly from a Supervisory Authority, ITCI shall always assist Customer in answering the request and organizing an audit.

#### **11. Liability**

Each party's liability to the other in respect of any individual claim for breach of contract, negligence, breach of statutory duty or otherwise in relation to these terms and conditions will be limited in accordance with the terms of the Principal Agreement.

#### **12. General**

The laws governing the Principal Agreement shall apply to these terms and conditions except in the case where personal data of EU citizens is being processed and the jurisdiction of the Principal Agreement is not that of a member state of the EU, in which case the laws of the Republic of Ireland shall apply in default. These terms and conditions and the terms of the Principal Agreement referred to herein embody the whole agreement of the parties with respect to its subject matter.

## Security Measures

### Description of the technical and organizational security measures implemented by ITCI as processor:

1. Secure user authentication protocols including:
  - Control user IDs and other identifiers
  - Provide a reasonably secure method of assigning and selecting passwords (or use an alternative authentication technology such as biometrics or Multifactor authentication)
  - Control data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect
  - Restrict access to active users and active user accounts only
  - Block access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system
  - Restrict access to records and files containing personal information to those who need such information to perform their job duties
  - Assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with customer access, that are reasonably designed to maintain the integrity of the security of the access controls
2. Encrypt (to the extent technically feasible) all transmitted records and files containing personal information that will travel across public networks, and encryption of all data to be transmitted wirelessly
3. Implement reasonable monitoring of systems, for unauthorized use of or access to personal information
4. Encrypt all personal information stored on laptops or other portable devices
5. Provide reasonably up-to-date operating system security patches for files containing personal information on a system that is connected to the Internet, designed to maintain the integrity of the personal information
6. Provide reasonably up-to-date versions of endpoint detection and response agent software for malware protection and reasonably up-to-date sensor versions, or a version of such a software that can still be supported with up-to-date sensor versions, and is set to receive the most current sensor updates on a regular basis
7. Educate and train employees on the proper use of the computer security system and the importance of personal information security
8. Ensure that any third party that may have access to the systems by way of providing services to ITCI, but which are not providing data processing services, guarantee an equivalent level of security.

### Security Certifications:

ISO 27001:2013



**DATA:**

**Data subjects**

The Personal Data relating to the following categories of data subjects:

- Individuals who are authorized by Customer to use access ITCI services being Customer's employees, consultants, subcontractors, suppliers, business partners and customers.
- Other individuals whose personal data may be uploaded by Customer to ITCI services.

**Personal Data Categories**

Name, Company, organization, business contact details, interactions with ITCI's services such as logfiles and incident reports, training records and other personal data that an individual may share with ITCI. IP addresses, cookie data, device identifiers and similar device-related information.

**Permitted Purpose:**

To DELIVER ITCI SERVICES to Customer in accordance with the terms of the Principal Agreement and Customer's instructions.



## **Schedule 2**

ITC Infotech India Ltd. group entities/affiliates may also act as sub-processors.  
Refer to ITCI affiliates list at [www.itcinfotech.com/dxp-services/resources/legal-documents](http://www.itcinfotech.com/dxp-services/resources/legal-documents)