# Data Processing Agreement

This Data Processing Agreement (this “Agreement”) is incorporated into and made a part of the most recent Terms & Conditions in effect between Indusface Pvt Ltd.(Indusface) and a legal entity that has purchased Services from Indusface Pvt ltd (“Customer”). "Terms & Conditions" shall mean the terms and conditions as~~,~~ set forth at https://www.indusface.com/terms-of-service.php) governing the purchase of Indusface offerings signed by and between Customer, or its Affiliate(s) (as defined in the Terms & Conditions), and Indusface, or its applicable Affiliate(s), as the same may be or have been amended by the parties from time to time. If the provisions of this Agreement and the Terms & Conditions conflict, including any previously executed or incorporated data protection agreement or privacy terms and conditions, then the provisions of this Agreement shall control. Except for any changes made by this Agreement, the Terms & Conditions remain unchanged and in full force and effect.

1. **Definitions**. Unless otherwise defined herein, all capitalized terms used in this Agreement shall have the meanings assigned to such terms in the Terms & Conditions.

| | |
|---|---|
| **“Agreement Personal Data”** | means all Personal Data that **Indusface** processes on behalf of Customer as a Data Processor as specified in Schedule 1. |
| **“Authorized Sub-Processor”** | means any third party appointed by **Indusface** in accordance with this Agreement to process Agreement Personal Data on behalf of and as instructed by the Customer. For the avoidance of doubt, suppliers to Indusface that provide bandwidth connectivity and/or colocation services for Indusface controlled servers globally, where such providers have no access to communications or any data located on Indusface servers (i.e., such suppliers acting as “mere conduits”), shall not be considered Authorized Sub-Processors. |
| **“Cross-Border Transfer Mechanism”** | means applicable legal mechanisms required for the transfer of Personal Data from a Data Controller or Data Processor in a given jurisdiction to another Data Controller or Data Processor operating in a separate jurisdiction where applicable Data Protection Laws require a legal mechanism for cross-border transfer as described in Art. 46 of GDPR as fro time to time varied, amended or substituted by the European Commission or the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (the "**UK GDPR**") |
| **“Data Protection Laws”** | means all applicable laws (including decisions and guidance by relevant Supervisory Authorities) relating to data protection, the processing of personal data, and privacy applicable to Indusface and the Customer in respect of the processing of Agreement Personal Data to provide the Services, including such laws, by way of example and without limitation, the General Data Protection Regulation, the California Consumer Privacy Act, and the Personal Information Protection and Electronic Documents Act, UK Data Protection act 2018 (“UK GDPR”) |
| **“Data Controller,**<br>**“Data Exporter”, “Data Importer”, “Data Processor” “Data Subject”, “Personal Data”, and “Personal Data Breach”** | shall each have the definitions and meanings ascribed to them by the applicable Data Protection Laws, and shall include any equivalent or corresponding terms applied by such applicable Data Protection Laws (e.g., “Business” instead of “Data Controller” and “Service Provider” instead of “Data Processor” under the California Consumer Privacy Act, or “organization” or “agency” under the Australian Privacy Principles). |
| **“Supervisory Authority”** | means the government agency, department or other competent organization given authority over the processing of Personal Data relevant to this Agreement. |

## 2. Data Processing

2.1 **Compliance with Law.** Customer and Indusface each shall comply with their respective obligations as Data Controller and Data Processor, as applicable, under the Data Protection Laws.

2.2 **Data Processor Terms.** The parties agree and acknowledge that (i) Indusface, (and any relevant **Affiliates**, if applicable), when providing the Services to Customer, will be acting as a Data Processor in respect of the processing by or for it of Agreement Personal Data and, (ii) Customer hereby authorizes Indusface to process Agreement Personal Data as a Data Processor (on its and its Affiliates' behalf, if applicable) for the purposes of providing the Services necessary for the fulfillment of the preestablished purpose only.

2.2.1 Indusface is authorised to engage, use or permit an Authorized Sub-Processor for the Processing of Agreement Personal Data provided that:

(a) Indusface undertakes reasonable due diligence on them in advance to ensure appropriate safeguards for Agreement Personal Data and respective individual rights in accordance with applicable Data Protection Laws;

(b) Indusface shall provide Customer with advance written notice of any intended changes to any Authorized Sub-Processor, allowing Customer sufficient opportunity to object; and

(c) The Authorized Sub-Processor's activities must be specified in accordance with the obligations set out in this Section 2.2.

Without prejudice to this Section 2.2.1, Indusface shall remain responsible for all acts or omissions of the Authorized Sub-Processor as if they were its own. Customer hereby approves the Authorized Sub-Processors that Indusface uses to provide the Services, listed at https://www.indusface.com/compliance/Authorized-Subprocessor.pdf. Further, to the extent that any Data Protection Laws would deem an Indusface Affiliate, by sole virtue of its ownership of Indusface servers used to provide the Services, to be a sub-processor for purposes of this Agreement, Customer hereby authorizes Indusface's use of such Indusface Affiliates as Authorized Sub-Processors.

2.2.2 Indusface shall (and procure that any Authorized Sub-Processor shall):

(a) process Agreement Personal Data only on documented instructions from Customer, including those set forth in the Terms & Conditions, this Agreement, technical specifications provided for administration of the Services, and configuration settings set in any of **Indusface's** customer portals provided for administration of the Services;

(b) without prejudice to Section 2.2.2(a), ensure that Agreement Personal Data will only be used by Indusface as set forth in this Agreement or the Terms & Conditions;

(c) ensure that any persons authorized to process Agreement Personal Data:

(i) have committed themselves to appropriate confidentiality obligations in relation to Agreement Personal Data or are under an appropriate statutory obligation of confidentiality;

(ii) access and process Agreement Personal Data solely on written documented instructions from Customer; and

(iii) are appropriately reliable, qualified and trained in relation to their processing of Agreement

Personal Data;

(d) implement technical and organizational measures at a minimum to the standard set out in Schedule 2 to ensure a level of security appropriate to the risk presented by processing Agreement Personal Data, including as appropriate:

(i) encryption of Personal Data;

(ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

(iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;

(e) notify Customer without undue delay (and in any event no later than 48 hours) after becoming aware of a Personal Data Breach as set forth in Section 4;

(f) assist Customer in:

(i) responding to requests for exercising the Data Subject's rights under the Data Protection Laws, by appropriate technical and organizational measures, insofar as this is reasonably possible, provided that Indusface shall not be required to store or process any data for the purpose of re-identifying an individual when such information is not normally processed or stored by Indusface;

(ii) responding to any requests or other communications from the Customer as Data Controller relating to the processing of Agreement Personal Data under this Agreement;

(iii) reporting any Personal Data Breach to any Supervisory Authority or Data Subjects and documenting any Personal Data Breach;

(iv) taking measures to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects; and

(v) conducting mandatory privacy impact assessments of any processing operations and consulting with any applicable Supervisory Authority or appropriate persons accordingly;

(g) at the choice of Customer and where appropriate, to the extent that Agreement Personal Data is stored by Indusface, securely delete or return all Agreement Personal Data to Customer after the end of the provision of relevant Services relating to processing, and securely delete any remaining copies and certify when this exercise has been completed; Indusface may retain the data during times (after intimating the customer) wherein such retention is necessary for the fulfillment of a lawsuit or if such data holds an evidentiary value.

(h) make available to Customer all information necessary to comply with its obligations to do so under Data Protection Laws;

(i) immediately inform Customer if Indusface is of the opinion that an instruction of Customer regarding the processing of Agreement Personal Data violates applicable Data Protection Laws; and

(j) not sell, rent, disclose, release, transfer, make available or otherwise communicate, Agreement Personal Data to a third party for monetary or other valuable consideration.

### 2.3 Cross-Border Transfers.

2.3.1 The Customer hereby acknowledges and accepts that the Indusface platform is made up of servers owned and operated by Indusface and/or its Affiliates globally and that Indusface processes Agreement Personal Data not only in the applicable jurisdiction(s) where the Customer operates as a Data Controller, but also transfers Agreement Personal Data outside of such jurisdictions, dependent upon the location of the Customer's end user and the Indusface servers serving those connections. Such cross-border transfers shall take place in accordance with applicable Data Protection Laws, including, without limitation, completing any required prior impact assessments. A list of all countries in which Indusface operates servers, a list of all Indusface Affiliates that own such servers, as may be updated from time to time, is available https://www.indusface.com/compliance/point-of-presence.pdf

2.3.2 To the extent that Agreement Personal Data is subject to a cross-border transfer to a non-EU member country that does not have an EU adequacy determination, at least one of the Cross-Border Transfer Mechanism(s) listed below shall apply in the order of preference listed in the event that more than one mechanism applies:

(a) Binding Corporate Rules -- To the extent Indusface has adopted Binding Corporate Rules, it shall maintain such Binding Corporate Rules and promptly notify Customer in the event that the Binding Corporate Rules are no longer a valid transfer mechanism between the Parties.

(b) EU Standard Contractual Clauses (processors) -- To the extent applicable, the EU standard contractual clauses for Data Processors established in third countries pursuant to European Commission Decision (2010/87/EC) under the EU Directive (95/46/EC), and as may be updated or replaced from time to time, are available at https://www.indusface.com/privacy-policy.php ("Standard Clauses"), are hereby agreed and incorporated herein by Customer (as Data Exporter) and the relevant Indusface Authorized Sub-Processor (as Data Importer, as specified in the Standard Clauses), whereby Appendix 1 shall be deemed to be prepopulated with the relevant sections of Schedule 1 of this Agreement and Appendix 2 shall be deemed to be prepopulated with Schedule 2 of this Agreement. For the avoidance of doubt, the Customer hereby authorizes Indusface to agree on these Standard Clauses on its behalf as Data Exporter with the relevant Indusface Authorized Sub-Processor (as Data Importer).

2.3.3 In addition to the foregoing Section 2.3.2, any similarly applicable standard contractual clauses adopted by a Supervisory Authority or other body of competent jurisdiction to govern the cross-border transfer of Personal Data subject to applicable Data Protection Laws shall be incorporated herein by the parties hereto in accordance with their respective roles pursuant to such clauses as analogous to those set out herein. Such clauses shall be supplemented and/or prepopulated (as applicable) with the relevant sections of this Agreement and its appended Schedules.

### 3. Audits

Indusface shall conduct periodic audits of its processing of Agreement Personal Data to ensure compliance with Data Protection Law. Upon request, Indusface shall deliver to Customer relevant compliance documentation from such audit(s) (e.g., Indusface's then-current ISO 27001 audit report (or its successor report) and certain, selected policies, procedures and evidence that have been approved for distribution to customers.

### 4. Personal Data Breach

4.1 Indusface shall notify Customer without undue delay (and in any event within 48 hours), after becoming aware of a Personal Data Breach via e-mail to the users contact provided by Customer from time to time in the Indusface portal. Such notice shall include a description of the nature of the Personal Data Breach and, where possible, other information as is required by applicable Data Protection Law(s); provided, that, where, and insofar as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

4.2 Indusface shall take all commercially reasonable measures and actions as are appropriate to remedy or mitigate the effects of the Personal Data Breach and shall keep Customer (and where applicable the Supervisory Authority) up-to-date about developments in connection with the Personal Data Breach.

## Schedule 1 of the Data Processing Agreement: Details of Indusface's Processing Activities

### 1. Data Processor

Indusface is a provider of content delivery, media acceleration, web performance and Internet security services.

### 2. Data Subjects

Indusface processes data on behalf of its Customers that may contain the Personal Data of the end users accessing Customer Content and/or using Customer services when performing Services for the Customer under the Terms & Conditions. "Customer Content" means all content and applications, including any third-party content or applications, provided to Indusface in connection with Customer's access to or use of the Services.

### Categories of data processed

a) End User Personal Data

Indusface processes Personal Data included within Customer Content ("End User Personal Data") when providing the Services to Customer. Upon the Customer's choice, End User Personal Data may include data such as:

a. Login credentials;

b. Subscriber name and contact information;

c. Financial or other transaction information;

d. Other Personal Data relating to the individual data subject as set by Customer.

b) Logged Personal Data

Indusface processes Personal Data that is included in log files when performing the Services for Customer (Logged Personal Data"). Logged Personal Data is Personal Data logged by Indusface servers, relating to the access to Customer Content over the Indusface platform by Customer's end users, as well as logged personal data associated with user activity and interaction with web and internet protocol sessions transiting Indusface's servers as part of a data subject's session with the Customer's web property. Logged Personal Data include such data as:

a. End user IP addresses;

b. URLs of sites visited with time stamps (with an associated IP address);

c. Geographic location based upon IP address and location of Indusface server;

d. Telemetry data (e.g., mouse clicks, movement rates, and related browser data).

c) Site Personal Data

Indusface processes Personal Data associated with user activity and interaction with web and internet protocol sessions transiting Indusface's servers as part of a data subject's session with the Customer's web property ("Site Personal Data"). The Site Personal Data consists of user telemetry data (e.g., mouse clicks, movement rates, and user agent and related browser data) designed to measure website performance.

d) Special categories of data

Customer as the Data Controller decides which categories of data are included in the End User Personal Data. Where Customer chooses to include special categories of data in the Customer Content, Indusface will process this data as End User Personal Data, as instructed by the Customer. Such special categories of data include, but may not be limited to, information revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning an individual's health or sex life

e) Categories of data processed by particular Indusface Services

Indusface maintains a list of service categories that provide further information regarding the processing of Personal Data conducted in providing Services in each category. This list is available at <need to be update>

## 3. Description of Indusface's Personal Data processing activities:

The following processing activities are performed when providing the Services:

a) End User Personal Data

Indusface processes End User Personal Data on behalf of Customers, including instructions given through the Terms & Conditions, or via configuration of the Services via the relevant customer portals or support processes.

b) Logged Personal Data

Indusface collects Logged Personal Data and conducts analysis of Logged Personal Data to provide Customer with copies of traffic logs and data analytic reports related to the performance of its Services and the Customer' web properties.

Logged Personal Data is also be processed for purposes of Service issue resolution.

c) Site Personal Data

Indusface processes Site Personal Data to provide website monitoring and analytics services to Customers to enable them to understand the nature of end user traffic to their web properties, as well as to monitor the performance of such properties.

## Schedule 2 to the Data Processing Agreement
## Indusface's Technical and Organizational Measures

### 1. Confidentiality

**a) Access control**:

The Data Processor limits the access to its data systems according to its business requirements and the least privilege principle. For example, field technicians are not granted administrative access to servers processing Data Controller's content. Administrative access is restricted to trained and authorized employees of the Data Processor. Field technicians are not granted administrative access to the servers processing the Data Controller's content. Remote administrative access is only available via cryptographically secure connections, systems authenticate administrative connections using asymmetric key cryptography. User administrative access is provided through an access control gateway, which enforces a need-have access grant authorization model. All connections through the authorization gateway are logged. User SSH system are routinely rotated and access is immediately removed in case of reports of theft of devices or the termination of a person's employment. All access to Data Processor system can be done only through MFA and access is provided only on need basis.

In case of password authentication, the complexity of the password is ensured by the Data Processor's password policy (e.g. multiple character types, length of min. 8 characters, change requirements after 120 days, inability to reuse a password within the following 12 month).

The Data Processor does not provide user accounts to servers transmitting content. Administrative access to such servers is limited to a number of authorized employees of the Data Processor. Access to these servers by authorized employees on a user level is logged by an authentication gateway. Remote access via the authentication gateway utilizes SSH keys and asymmetric cryptography.

**b) Segregation control:**

The Data Processor separates the environment for development, software, engineering, from the environment for testing and the environment for operations and has put in place several controls to ensure the code development, testing and production data handling environments are separated. E.g. employees within the development team do not have access to the same systems as the employees within the test or operation team. Separate cryptographic credentials are used to access development, test, operations and production environments, critical network operations systems are further isolated from the corporate, development and test network environments. The separation is supervised by granular logging of access to the production and operations servers, change control processes and by the responsible management.

## 2. Pseudonymization

In most cases Data Processor does not pseudonymize the personal data it processes. For End User Personal Data this would require modifications of the End User Personal Data which would mean a violation of the integrity of the End User Personal Data.

For Logged Personal Data this data is required in raw and clean for the purpose of the processing activities. E.g. Data Processor could not deliver the End User Personal Data in case the IP addresses in the log files would not be clear to determine the best way to route the traffic via the Indusface Platform. Neither could security analytics be performed in case the IP addresses would be encrypted.

## 3. Integrity

**a) Transmission control**

The Data Processor has put in place a robust alert management system that provides for extensive monitoring of all servers. Fine grained monitoring of running processes allows the definition of predefined alerts to catch unexpected and suspicious behavior, including the execution of rogue processes.

In addition, the Data Controller can control access to the personal data in its content while having the Data Processor transmitting traffic to its server over encrypted and authenticated connections by its configuration of the services in the Data Processor's AppTrana portal. The Data Controller can control storage of personal data in its content by configuring property specific content caching rules. By it configuration the Data Controller can also limit the storage of personal data in its content to servers with enhanced physical security controls only. The integrity of the log data is ensured by various storage controls (e.g., log retention control) that are subject to several regular third-party assessments.

**b) Input control**

Access to the Data Processor's server is logged and monitored via audit systems and processes. Log data gathered by web-servers is digitally signed by "Edge Servers" and is audited by the distributed data processing facilities, to ensure that it is not modified or corrupted. Respective access logs consisting of aggregated and anonymized log datasets are provided to the Data Controller as part of the Data Processor's "Log Delivery Service" offering.

## 4. Availability and resilience

The Data Processor's web server networks have been created matching the principles of availability. The server network is self-curing and ensures that the content of the Data Controller is transmitted via the server network, even in case of an outage of single servers. This prevents an outage of the services which would require a fast recovery of the services.

## 5. Evaluation of effectiveness

The Data Processor has data protection management and incident response management policies and procedures in place, which are evaluated in the course of annual third-party audits, including Data Processor's annual ISO270001 and other assessments and certifications. Further the Data Processor ensures by its privacy by design processes that personal data is protected in all processing activities and that relevant data protection principles are applied. In addition, the Data Processor is offering, where reasonably possible tools for the de-identification of personal data to assist in complying with the data minimization principle.

### 6. Role Control

The Parties ensure that personal data is processed by the Data Processor only in accordance with the instructions of the Data Controller by agreeing on the data processing agreement. In addition, the Data Processor’s robust alert system ensures that it transmits the Data Controller’s web content only in accordance with the instructions of the Data Controller (which he has provided by way of its configuration how to process the content within the Data Processor’s Apptrana Portal).