Indentr Privacy Policy

Data Protection Agreement (DPA) - Updated

This Data Protection Agreement ("Agreement") is made between the Client ("Data Controller") and Indentr ("Data Processor"), collectively referred to as the "Parties."

1. Purpose:

The purpose of this Agreement is to outline the responsibilities and obligations of the Parties in relation to the protection of personal data, in compliance with applicable data protection laws and regulations.

2. Scope of Data Processing:

The Data Processor agrees to process personal data received from the Data Controller solely for the purpose of providing IT services, including but not limited to maintenance and support of software products, application and database monitoring, and customer support services. All data processing activities shall be carried out in accordance with the terms of this Agreement and the Data Controller's instructions.

3. Data Protection Measures:

The Data Processor commits to implementing appropriate technical and organizational measures to ensure a level of security appropriate to the risk. This includes encryption of personal data in transit and at rest, ensuring the ongoing confidentiality, integrity, availability, and resilience of processing systems and services, and regular testing, assessment, and evaluation of the effectiveness of technical and organizational measures for ensuring the security of the processing.

4. Subprocessing:

The Data Processor shall not engage any third party to process personal data without the prior written consent of the Data Controller. Where subcontracting is approved, the Data Processor shall ensure that the subprocessor is bound by data protection obligations no less stringent than those stipulated in this Agreement.

5. Data Transfer:

The Data Processor shall store and process all personal data within a MongoDB M10 cluster with a Virtual Private Cloud (VPC) setup between it and the Data Processor's backend. The Data Processor guarantees that personal data will not be transferred to, or stored at, a destination outside this secure environment, nor shared with any third parties, without the Data Controller's prior written consent.

6. Data Breach Notification:

In the event of a personal data breach, the Data Processor shall notify the Data Controller without undue delay and, where feasible, not later than 72 hours after having become aware of it.

7. Rights to Have Data Removed:

Upon request from the Data Controller, the Data Processor shall ensure that any specified personal data is removed from its systems in compliance with applicable data protection laws. This includes the right of the Data Controller to request the deletion of personal data pertaining to individuals associated with the Data Controller's operations when they exercise their right to be forgotten under relevant data protection legislation.

8. Termination:

Upon termination of the services, the Data Processor shall, at the choice of the Data Controller, delete or return all personal data to the Data Controller and delete existing copies unless required to retain the data by law.

This Agreement is binding upon the Parties from the date of signing and shall continue in effect until terminated by either Party in accordance with its terms.