Data Processing Agreement Ansys Discovery Named User License

The Parties agree that for Ansys Discovery Named User License the Ansys Data Processing Addendum, available at https://www.ansys.com/legal/agtc#tab1-5, together with the below annex(es), apply to and sets forth the rights and obligations of the Parties with regard to the Processing of Personal Data.

ANNEX I

List of Parties and Description of Transfer

Applicable to European Data Transfers

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter: As identified in the DPA by and between the data exporter and data importer.

Data importer(s): ANSYS, Inc., 2600 Ansys Dr., Canonsburg, PA 15317, U.S.A., acting on its own behalf and as agent for each ANSYS Affiliate.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Users of Ansys Discovery Named User License as identified by data exporter.

Categories of personal data transferred

Name, email address, username, MAC address.

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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures

None.

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

As identified in the DPA and/ or the Main Agreement by and between the data exporter and data importer.

Nature of the processing

As identified in the DPA and/ or the Main Agreement by and between the data exporter and data importer.

Purpose(s) of the data transfer and further processing

As identified in the DPA and/ or the Main Agreement by and between the data exporter and data importer.

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

As identified in the DPA and/ or the Main Agreement by and between the data exporter and data importer and according to data importer's retention policies and schedules.

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

Microsoft - Storage of usage data;

Flexera - Provision of licensing software and service;

Salesforce - Support of ticket portal.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority in accordance with Clause 13

Bavarian Data Protection Authority Germany.

ANNEX II

Technical and Organizational Measures to Ensure the Security of the Data

1. Security Program

   1.1. Program Management: Processor maintains a risk-based security program to systematically manage and protect the organization's business information and the information of its customers and partners.

   1.2. Security incident response policy: Processor shall maintain policies and procedures to (1) investigate and respond to security incidents, including procedures to assess the threat of relevant vulnerabilities or security incidents using defined incident classifications and categorizations and (2) establish remediation and mitigation actions for events, including artifact and evidence collection procedures and defined remediation steps.

2. Personnel Security

   2.1. Confidentiality obligations: Personnel who have access to Personal Data shall be subject to confidentiality obligations with Processor to keep the Personal Data confidential.

   2.2. Security awareness training: Personnel shall receive training upon hire and at least annually thereafter covering security practices and privacy principles.

   2.3. Code of conduct: Processor shall maintain a code of conduct and business ethics policy requiring ethical behavior and compliance with applicable laws and regulations.

3. Third-Party Security

   3.1. Screening: Processor shall maintain policies and procedures designed to ensure that all new Subprocessors are subject to reasonable due diligence to confirm their ability to meet corporate security and compliance requirements as well as business objectives.

   3.2. Contractual obligations: Processor shall maintain controls designed to ensure that contractual agreements with Subprocessors include confidentiality and privacy provisions as appropriate to protect Processor's interests and to ensure Processor can meet its security and privacy obligations.

   3.3. Monitoring and Review: As practicable, Processor shall periodically review existing third-party Subprocessors in a manner designed to ensure the Subprocessor's compliance with contractual terms and to ensure that the Subprocessor's performance, security, and compliance postures are still appropriate given the type of access and classification of data being processed.

4. System Security

   4.1. Encryption: Processor ensures that industry-standard encryption methods are used to protect data in transit and at rest as appropriate to the sensitivity of the data and the risks associated with loss.

   4.2. Network Security: Processor shall maintain commercially reasonable controls, policies, and technologies to protect the Processor network including firewalls, VPN, and intrusion protection and monitoring systems.

   4.3. Data Segregation: Processor shall maintain logical, operational, and technical controls to ensure the separation of Personal Data from Processor data and the data of other Processor customers.

5. Physical Security

5.1. Corporate facility security: A facility security program shall be maintained that manages the overall security of its offices. All employees, contractors, and visitors shall be required to wear identification badges that distinguish their respective roles.

5.2. Corporate data center security: Systems installed on Processor's premises and used to process Personal Data shall be protected by measures designed to control logical or physical access; equipment used to process Personal Data cannot be moved, removed, upgraded, or reconfigured without appropriate authorization and protection of the information; and, when equipment processing Personal Data is decommissioned, Personal Data shall be disposed of in a manner that would prevent its reconstruction.

6. Operational Security

6.1. Access controls: Processor shall maintain policies, procedures, and logical controls to establish access authorizations for employees and third parties. Such controls shall include:

6.1.1. requiring unique user IDs to identify any user who accesses systems or data;

6.1.2. requiring that user passwords are (a) changed at regular intervals; (b) of sufficient length and complexity; (c) stored in an encrypted format; (d) subject to reuse limitations; and (e) not assigned to other users, even at a different time; and

6.1.3. automatically locking out users' IDs when a number of erroneous passwords have been entered.

6.2. Least privilege: Personnel shall only be permitted access to systems and data as required for the performance of their roles and access rights are reviewed and certified at least annually.

6.3. Malware: Processor shall utilize measures intended to detect and remediate malware, viruses, ransomware, spyware, and other intentionally harmful programs that may be used to gain unauthorized access to information or systems.

6.4. Business Continuity and Disaster Recovery (BCDR): Processor shall maintain BCDR plans designed to ensure Processor's systems and services remain resilient in the event of a failure, including natural disasters or system failures, and such plans shall be reviewed, updated, and approved by management at least annually.

6.5. Network security: Processor shall implement industry-standard technologies and controls designed to protect network security, including firewalls, intrusion prevention systems, monitoring, network segmentation, VPN, and wireless security. Networks shall be designed and configured to restrict connections between trusted and untrusted networks, and network designs and controls shall be reviewed at least annually.

6.6. Data segregation: Processor shall implement logical controls, including logical separation, access controls and encryption, to segregate Personal Data from other data.

ANNEX III

Explanation of Personal Information in Cross-Border Transfers from the PRC

Applicable to China Data Transfers

---

(1) Personal Information transmitted belongs to the following types of Individuals:

- Users of Ansys Discovery Named User License as identified by data exporter.

(2) Transfers are made for the following purposes:

- As identified in the DPA and/ or the Main Agreement by and between the data exporter and data importer.

(3) Amount of Personal Information transferred:

- Personal Information related to fewer than 10000 data subjects since January 1st of the preceding year.

(4) Cross-border transferred Personal Information types:

- Name, email address, username, and MAC address.

(5) Types of cross-border transferred Sensitive personal information:

- None.

(6) Oversea recipients will only provide Personal Information to the following recipients outside the PRC:

- Microsoft, Flexera, and Salesforce.

(7) Transfer method:

- Transmission via cloud (SaaS platform).

(8) Storage time after cross-border transferred:

- Duration of the Main Agreement and according to data importer's retention policies and schedules.

(9) Storage location after cross-border transferred:

- USA.