ServiceNow Technical and Organizational Measures

CONFIDENTIAL
1. **PHYSICAL ACCESS CONTROL.** Without limitation, ServiceNow has implemented the following measures, to prevent unauthorized parties from accessing privacy installations that are used to process or use Personal Data and premises, buildings, areas, and rooms containing data processing equipment (server, client, or other system components).
   a. Alarm system on doors and windows
   b. Automatic access control system
   c. Photoelectric sensors/movement detectors
   d. Key management (issuance of keys, etc.)
   e. Logging of visitors
   f. Biometric and RFID cards
   g. A separate, specific, and documented access control for data centers and server rooms for authorized persons is implemented.
   h. CCTV at entry points (office and data centers)
   i. Visitor management at reception desks
   j. Mandatory wearing of visible access and identification badges
   k. Physical separation of ServiceNow’s own enterprise computing resources from those used to provide its service to customers
   l. Access by authorized persons is documented by name

2. **SYSTEM ACCESS CONTROL.** Without limitation, ServiceNow has implemented the following measures, to prevent unauthorized parties from using data processing systems or to have access to systems and relevant components (including the operating system).
   a. Authentication with username/password and multi-factor authentication
   b. Use of intrusion detection systems
   c. Complexity and forced password changes, use of virus scanners
   d. Assignment of user profiles to IT systems
   e. Use of VPN Technology
   f. Encryption of mobile storage media
   g. Disk encryption on laptops/notebooks
   h. Multi-tier architecture with internal firewalling
   i. Additional measures include but are not limited to regular vulnerability scans and penetration testing, patch management, minimum requirements for password

3. **DATA ACCESS CONTROL.** Without limitation, ServiceNow has implemented the following measures, to prevent that authorized users of a data processing system may access the data for which they are not authorized, and to prevent personal data from being read while the data is in use, in motion, or at rest without authorization.
   a. Usage of ‘Need to know’, ‘Least privileged’ and ‘Separation of Duties’ principles for administrators
   b. Logging of application access, modification, and deletion of data
   c. Secure media sanitization before re-use
   d. Use of shredders and/or shredder service
   e. Disk encryption for corporate laptops and mobiles
   f. Management of rights by system administrators
   g. Password policy including password length, password change management
   h. Secure storage of data carriers
4. DATA TRANSFER CONTROL. Without limitation, ServiceNow has implemented the following measures, to prevent that personal data can be read, copied, or modified during electronic transmission or during transportation or storage to disk.
   a. TLS encryption across public networks (Web-Client, APIs, mobile Apps)
   b. Full Disk encryption for Customer Data (Optional, if chosen by a Customer)
   c. Use of dedicated, private connections between data centers in a region
   d. During physical transport, secure transport containers/packaging
   e. Data classification based on best practices

5. DATA ENTRY CONTROL. Without limitation, ServiceNow has implemented the following measures, to review, and determine if and by whom, personal data has been entered, changed, or removed on data processing systems.
   a. Logging of input, access, modification, and deletion of data
   b. Traceability of input, modification, and deletion of data by individual usernames
   c. Granting of rights for the input, modification, or deletion of data based on an authorization concept
   d. Defined log retention schedules based on its value

6. ORDER CONTROL. In addition to the DPA, to which this schedule is attached, stating that the Personal Data that is Processed on behalf of the Customer can only be processed according to the Customer’s instructions, ServiceNow has put in place without limitation the following measures:
   a. Sub-contractors comply with ServiceNow’s security requirements, including security obligations to ServiceNow’s customers
   b. Established Security Incident Management aligned with NIST 800-61
   c. Secure destruction of data after termination of the contract
   d. Continual review of contractors and their activities (Vendor Risk Management)

7. AVAILABILITY CONTROL. ServiceNow has implemented, without limitation, the following measures, for the protection of personal data against accidental destruction or loss.
   a. Redundant Advanced High Available Infrastructure (AHA)
   b. Regional EU Data Center Pair to support the AHA infrastructure
   c. Minimum N+1 principal for all infrastructure
   d. Uninterruptible power supplies (UPS), redundant power feeds and generator fuel supplies
   e. Redundant ISPs
   f. Devices for monitoring temperature and humidity in server rooms
   g. Fire and smoke detection systems
   h. Annual Testing of service recovery
   i. Established Disaster Recovery and Business Continuity Plans
8. **SEGREGATED PROCESSING.** ServiceNow has implemented, without limitation, the following measures, to manage that data which is collected for different purposes can be processed separately.

   a. Logical separation of customer data using a multi-instance/logically single tenanted architecture
   b. Physical separation of production and test/development systems
   c. Treatment of all customer data using a single “sensitive” data classification
   d. Best practice usage of the “authorization concept”
   e. Customers retain full ownership of the data at all times

9. **ALTERNATIVE SUITABLE MEASURES.** ServiceNow is allowed to take alternative suitable measures if the security level of the measures mentioned above is not significantly undercut.