DELL Technologies

Table of Contents

Entrance Control 3
Authentication Controls 3
Access Controls 4
Separation Controls 4
Transmission Control 4
Input Control 4
Job Control 5
Availability Control 5
Resiliency 5
Incident Response 5
Pseudonymization 6
Encryption 6
Back-up concepts, redundant storage locations, mirrored IT infrastructure 6

Dell values the confidence that our customers, partners and employees have in us, and we take the responsibility of protecting information, including personal data, seriously. Our GDPR compliance program contains a layered approach that incorporates people, operational procedures and technology in appropriate balance to protect personal data. With this approach, Dell provides controls on how data is stored, kept up to date, accessed, transferred and deleted.

Our Global Privacy Program provides the foundational tenets for protecting personal data worldwide, and includes a dedicated team of experienced certified privacy professionals and privacy attorneys, led by our Chief Privacy Officer. Our Security & Resiliency organization, led by our Chief Security Officer, has a team of qualified professionals to govern and protect enterprise information. Our Dell Digital (IT) organization is led by our Chief Information Officer and includes technical experts who architect and support the enterprise infrastructure for Dell data.

Our executive level Global Regulatory Compliance Council oversees our privacy compliance and risk mitigation activities. In addition, all Dell team members are responsible for the protection of personal data and may only use personal data for authorized purposes.

Our Global Privacy Program, together with our Information Security policies, standards and procedures, provide confidence that personal data, including personal data received from data subjects in the European Union, the European Economic Area and Switzerland, will be adequately protected when entrusted to Dell.

Technical and organizational security measures included in Dell's global compliance programs include the following:

Measures to ensure security of processing

Entrance Control

Appropriate measures preventing unauthorized persons from gaining physical access to data processing systems on which personal data are processed or used:

- Visitors need to register; date and time of arrival, time of leaving the building as well as the name of the person being visited shall be recorded; visitors shall be accompanied by an authorized person at all times;
- All office units are secured by an access control system. Access to the office units is granted with an activated entry card only;
- CCTV covers appropriate areas (e.g. entrances to data centers);
- Data centers are located in separated areas with special access requirements;
- Access is recorded in logs;
- Security guard service for all main, operational buildings is provided;
- Outside areas may partly be under video surveillance or under monitoring by a security service.

Authentication Controls

Appropriate measures preventing unauthorized persons from using data processing systems.

- Access to IT systems is granted only to a user when registered under a valid username and password;
- Internal password policy requires periodical mandatory password changes and minimum complexity requirements (e.g., length and the use of special characters);
- Policy includes automatic computer lock after a short period, with renewed access to the PC only after re-authentication;
- Access from outside Dell's network requires two-factor authentication.

Access Controls

Appropriate measures ensuring that persons entitled to use a data processing system have access only to the data to which they should have the right of access, and that personal data cannot be read, copied, modified or removed without authorization in the course of processing or use and after storage:

- Access authorization is issued in respect of the specific area of work to which the employee is assigned (work roles);
- Policy requires regular verification of access authorizations;
- Adjustment is made to access authorizations in case of changes of the working area or role or in case of resignations of employees.

Separation Controls

Appropriate measures ensuring that data collected for different purposes can be processed separately:

- Personal data received from different controllers shall be processed separately;
- Functional separation between test and production systems is employed.

Measures to ensure integrity of processing

Transmission Control

Appropriate measures ensuring that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is made:

- Encrypted data transfer when handling confidential data and when accessing the company network;
- Registration of suspicious data traffic;
- Restrictive usage of Wireless LAN;
- Restrictive remote-access to the Dell network (using two-factor authentication);
- Data media shall be disposed of in accordance with data protection policies by use of safety container and document shredders; magnetic data storage media shall be destroyed physically; compliance with guidelines concerning erasure and/or destruction of data storage media and documents;
- In case of remote support (screen sharing), the connection will be encrypted and requires an affirmative action from the customer.

Input Control

Appropriate measures ensuring the possibility to check and establish whether and by whom personal data have been input into data processing systems, accessed, modified or removed:

- When using relevant applications, access is automatically recorded;
- In case of remote-support, the customer can terminate the data processing or support activity at any time.

Measures to ensure availability and resilience of processing

Job Control

No Processing according to Art. 28 GDPR shall take place without Controller's instructions, clear contract drafting, formalized assignment management, strict vetting processes and checks.

- Subcontractors are on-boarded in globally consistent processes. During the onboarding process, subcontractors are vetted and must contractually commit to consistent compliance standards;
- Subcontractors must agree to be audited for compliance with their contractual and legal obligations;
- The processor and its subcontractors shall agree on provisions equivalent to the provisions agreed between the controller and the processor;
- Contracts with any subcontractors in non-EEA-countries will contain the EU-Standard Contractual Clauses to ensure the adequacy of personal data transfers from inside the EEA to those countries outside the EEA which are not subject to an adequacy decision on EU data protection laws;

Availability Control

Appropriate measures ensuring that personal data are protected from accidental destruction or loss:

- Anti-virus software is installed on all systems;
- Protection of the company network via Firewall;
- Network segmentation;
- Use of content filter/Proxys;
- Interruption-free power supply for all critical systems;
- Regular generation of backups of relevant data;
- Fire safety system;
- Water protection system;
- Emergency/ Disaster recovery plans;
- Air-conditioned server rooms.

Resiliency

Punctual peak demands or long-term high demands are reflected in the design of systems and services (memory, access and throughput capacities, etc.) in order to ensure resilience and consistency of processing.

- The infrastructure is designed to function under high demand and can handle peak demands.

Incident Response

Appropriate processes to address cybersecurity events.

- A corporate response plan for cybersecurity incidents is in place that outlines Purpose, Scope, Identification, Assessment, Response and Remediation of security incidents, including notifications to Regulators, controllers and/or data subjects as may be required.

Measures to pseudonymize or encrypt personal data

Pseudonymization

Separation of customer names and customer revenue data or usage of personal IDs, Customer-IDs or Vendor-IDs

- During provision of IT Support Services, processor mainly processes pseudonymized data (e.g. IP-addresses, MAC-addresses);
- Personal data will partly be pseudonymized (e.g. via customer-numbers).

Encryption

- Data is saved encrypted on employees' laptops;
- Identifiable sensitive personal data is encrypted in transit and at rest;
- Encryption standards are specific and clearly defined.

Measures to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Back-up concepts, redundant storage locations, mirrored IT infrastructure

- Disaster Recovery plans exist for relevant data;
- Critical data is backed up or mirrored.

Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the personal data processing

- All IT security policies are regularly checked to ensure they are effective and up-to-date;
- Annual review of all security Policies, Standards and corresponding Procedures occurs with the final review/approval of the Chief Security Officer.