DASSAULT SYSTEMES
TECHNICAL AND ORGANIZATIONAL MEASURES

While providing 3DS's customers and other stakeholders with 3DS Offerings, 3DS is considered as data processor of personal data provided by customer according to Article 28 of the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (GDPR). To help them to comply with the GDPR and their obligation to keep and maintain records of processing activities, the description of the technical and organizational measures 3DS Group has implemented are detailed hereinafter. These technical and organizational measures may be updated from time to time to reflect evolutions according to DS's standards.

When 3DS is acting as data controller, its data privacy policy available at 3ds.com/privacy-policy will be applicable.

1.1. Awareness of 3DS Users and Data Protection Management

Since 2014, 3DS has organized mandatory e-learning awareness sessions, including to all newcomers related to data privacy. An IT charter and a HR policy are also applicable to all individuals working for 3DS ("3DS Users"). An updated training has been communicated to all 3DS employees to take into consideration the new European General Data Protection Regulation enforceable on May 25th 2018. 3DS has created an internal network of people to monitor data privacy aspects per stream (R&D, Finance, Services…).

A center of competence, which is mainly focused on data privacy, has been implemented cross Geos in the 3DS legal department.

3DS Users working with personal data are educated to the risks related to the rights and freedoms of natural persons and are informed of the processes to handle those risks and the potential consequences in case of failure.

A 3DS dedicated internal community and guidelines are available to 3DS Users.

3DS has set up different means to disseminate to all 3DS Users the action to take in the event of a security incident or the occurrence of an unusual event affecting 3DS information and communication systems.

Data Protection team has been enhanced and a new Global Data Protection Officer has been appointed.

1.2. Authentication of 3DS Users

1.2.1. Password

Authentication through a strong password is implemented in 3DS organization as well as regular mandatory renewal. The requirements on the complexity of password are industry standard. Additional technical means to enforce the rules relating to authentication (for example blocking the account in case of non-renewal of the password or after repeated failed login attempts) are also implemented.

When 3DS is acting as data processor, it is data controller's responsibility to implement its own policy related the length and the complexity of the passwords. 3DS can provide help to its customers within the implementation of such policy when using 3DS Offerings.

1.2.2. Clearance management

Empowerment profiles in 3DS systems are implemented by separating tasks and areas of responsibility, in order to limit 3DS Users' access to the only personal data necessary for the performance of their tasks.

The access permissions are removed from 3DS users when they are no longer eligible to access a local or IT resource, as well as at the end of their contract.

An annual review of entitlements is operated to identify and delete unused accounts and realign rights granted to the functions of each 3DS User.

2.1. Physical access control

3DS has installed in its critical sites inter alia the following access control measures:

- Intruder alarms;
- Set up of smoke detectors and firefighting equipment;
- Protected mechanisms allowing access to certain critical premises and, when applicable dedicated access control to certain rooms or buildings;
- Specific rules and means of access control for visitors, at least by accompanying visitors outside public reception areas by a person of 3DS;
- Physical protection for certain computer equipment by specific means (dedicated fire-fighting system, elevation against floods, redundancy of power supply and / or air-conditioning, etc.);
- Video surveillance of the buildings and server rooms

Those mechanisms are regularly controlled.

2.2. Workstations, laptops, Windows tablets, mobile devices

All laptops are equipped with physical locking systems. Moreover, an automatic session locking mechanism is provided on workstations laptops, Windows tablets and mobile devices in case of non-use of them during a given time. .

New Windows Laptops and Windows tablets installation process imposes hard drives encryption.

3DS Users' data are stored on a regularly backed up storage space accessible via 3DS network. Where data is stored on Workstations, laptops, Windows tablets, means of synchronization or backup are also implemented.

Industry standard antivirus software is regularly updated. 3DS has implemented internal processes to securely erase data on a workstation prior to its reassignment to another person.

3DS regularly perform security checks on the software and hardware used in its information system.

2.3. 3DS internal network

Internal protective measures to fight against malware are crucial to 3DS. Several people within 3DS organization are dedicated to the IT security of 3DS's employees and data provided by 3DS's customers and other stakeholders.

3DS internal network is protected according to industrial best practices, including but not limited to firewalls. Automatic identification of hardware is implemented by using network card identifiers to prohibit the connection of an unlisted device.

Intrusion Detection Systems (IDS) can analyze network traffic to detect attacks, which are considered of high importance for 3DS. Network partitioning reduces impacts in the event of compromise.

In large 3DS locations, documents can be printed only after authentication on the printer (via a password or a badge)

Workspaces dedicated to specific projects (professional services by 3DS to its customers) can be implemented.

2.4. 3DS Servers

3DS limits access to administrative tools and interfaces to only authorized people.

In terms of database administration, 3DS organization to access databases is named-user based.

3DS performs backups and checks them regularly as detailed hereinafter.

Where appropriate, 3DS implements the TLS protocol, or a protocol ensuring the encryption and authentication for any data exchange on the Internet.

3.1. Backups

3DS implements the following technical measures related to backup:

- Frequent backups of data, whether in paper or electronic form. Some backups may be daily incremental while full backups are operated on regular intervals.
- Backups are stored in different locations of data centers, each of them being secured.
- The data are saved at the same level of security as those stored on the operating servers.
- When backups are transmitted over the network, the transmission channel is encrypted if it is not internal to 3DS.

3DS Online Services provided to 3DS's customers are subject to a Service Level Agreement available at https://www.3ds.com/terms/sla.

3.2. Disaster recovery and business continuity

3DS has set up for its critical activity a disaster recovery plan that is regularly tested and updated when appropriate

3.3. Secured Archives

Archive management processes are implemented within 3DS related to the management of personal data. Specific access procedures for archived data are available as the use of an archive must occur on an ad hoc and exceptional basis.

3DS, as data processor, will archive personal data provided by customers according to the applicable agreement signed with its customers and 3DS internal processes

With regard to the destruction of the archives, procedures guaranteeing that the entire archive has been destroyed are also implemented.

3DS's concern related to confidentiality and data privacy has always been of high importance.

For Support Services, all service requests from 3DS's customers are registered in dedicated 3DS systems. The 3DS Support Team is a worldwide multi-tiered organization, located in the Americas, Asia and Europe to provide customer with responsive and proactive Support Services. In that globalized context, when submitting a Service Request, customer shall ensure that among the information sent to 3DS to analyze the submitted case, there is no personal data, nor information that customer considers as confidential, or which requires a governmental authorization to be exported unless this authorization is required solely for export to countries subject to trade sanctions.

For Online Services, 3DS Users have access to data provided by 3DS's customers to provide, maintain and improve the Online Services. They are not entitled to modify them except in case of critical emergency, such as virus or malware that may compromise the customers' tenants. If a customer has ordered 3DS Online Services on a private mode, dedicated servers will host such personal data provided by customers

3DS however takes all reasonable measures to manage processing of personal data within its organization and with its own processors, including but not limited to, minimization, pseudonymisation or anonymization, when they are necessary for the analysis of the Service Requests.

3DS however takes all reasonable measures to manage processing of personal data within its organization and with its own processors, including but not limited to, minimization, pseudonymisation or anonymization, when they are necessary for the analysis of the Service Requests.

3DS only uses sub-processors with sufficient guarantees (especially in terms of specialist knowledge, reliability and resources) and requires strict commitment from its providers related to its information system security policy.

To ensure the effectiveness of the guarantees offered by the sub-processors in terms of data protection, 3DS asks its processors to implement all or part of the following measures:

- The encryption of data according to their sensitivity or, failing that, the existence of procedures guaranteeing that the sub-processors do not have access to the personal data entrusted to it;
- The encryption of data transmissions (eg: HTTPS type connection, VPN, etc.);
- Guarantees regarding network protection, traceability (newspapers, audits), authorization management, authentication, etc.

3DS templates to be signed with its suppliers specify, in particular

- Suppliers' obligation regarding the confidentiality of the personal data entrusted;
- The conditions of return and / or destruction of personal data upon termination or expiration of the applicable contract.

The list of sub-processors for support and online services is available to customers on the 3DS knowledge base.