DASSAULT SYSTEMES

3DEXPERIENCE® PLATFORM CLOUD SECURITY & PRIVACY

Whitepaper

TABLE OF CONTENTS

INTRODUCTION

OUR PHILOSOPHY

Cloud computing represents a paradigm shift in how we do business. Organizations are running applications, managing data, and shifting operations to the cloud to benefit from the speed and simplicity of cloud provisions, as well as benefiting from the operational effectiveness of maintenance, IT services, and security from specialist providers.

Dassault Systèmes has been providing cloud-based services since the creation of the **3D**EXPERIENCE® platform in 2012. We have built a full cloud-based ecosystem, the **3D**EXPERIENCE Cloud platform, that enables our clients to benefit from secure, flexible, scalable cloud resources. We have made it our mission to support our clients with trust and reliability in every aspect of our solutions.

Our approach to risk management is multi-faceted and proactive, based on best practices and designed to anticipate security threats across our operations. We run an Information Security and Privacy Management System (ISPMS) that is ISO/IEC 27001:2017 and ISO/IEC 27701:2019 certified and subject to routine auditing. Our ISPMS is based on the core values of confidentiality, integrity, availability and accountability.

This whitepaper outlines Dassault Systèmes's approach to security and compliance for **3D**EXPERIENCE, our cloud-based platform where customers access applications, d ata storage, and scalable computing resources. In this whitepaper we address the core aspects of our cloud security, privacy and compliance practices.

OUR INFORMATION SECURITY AND PRIVACY MISSION STATEMENT

The Dassault Systèmes Information Security and Privacy Mission Statement is as follows[1].

Manage information security risk exposure and safeguard personally identifiable information (PII) for **3D**EXPERIENCE platform Software as a Service (SaaS) and continually improve the confidentiality, integrity, and availability of information and protection of the following:

- Customer intellectual property and user data, PII included
- Dassault Systèmes' reputation and intellectual property
- Cloud availability and resilience
- Compliance with applicable cybersecurity and data protection regulations and standards

This mission statement is available to employees as documented information and to interested parties upon request.

DISCLAIMER

This content represents **3D**EXPERIENCE Cloud platform security, privacy, quality and compliance practices as of March 2022. The content of our practices set forth herein is subject to change at the sole discretion of Dassault Systèmes. "We" and "our" as used throughout this document refer specifically to Dassault Systèmes.

1. This corresponds to the ISO 27001 Information Security & Privacy Policy.

DASSAULT SYSTÈMES: A SECURITY AND PRIVACY FOCUSED ORGANIZATION

3DEXPERIENCE PLATFORM SAAS CYBERSECURITY & PRIVACY GOVERNANCE

Dassault Systèmes R&D operates a centrally controlled Information Security & Privacy Management System (ISPMS) for **3D**EXPERIENCE platform SaaS that is ISO/IEC 27001:2017 and ISO/IEC 27701:2019 certified by SGS International Certification Services (SGS-ICS). The scope of the certification includes:

1. Design, development, delivery, deployment, cloud operations and support of **3D**EXPERIENCE platform SaaS.

2. Data privacy management when Dassault Systèmes acts as a:

a. Controller for handling of personal data provided in the context of **3D**EXPERIENCE platform SaaS.

b. Processor for PII under the control of a customer and processed in **3D**EXPERIENCE platform SaaS.

Our ISPMS is administered and subject to management review by the Dassault Systèmes R&D Executive Committee. It is built on a well-established Quality Management System (QMS) that is operated on the **3D**EXPERIENCE platform and is certified to ISO 9001:2015 by SGS-ICS.

The QMS and ISPMS share many fundamental and supporting processes that are based on a Secure Software Development Lifecycle (Secure SDLC) methodology. The ISPMS also includes additional risk-based processes focused on information security and data protection.

All ISPMS processes and controls are continually evaluated for compliance and effectiveness by the Dassault Systèmes R&D **3D**EXPERIENCE Compliance Audit program. Resulting corrective actions and continual improvements are tracked in the **3D**EXPERIENCE platform.

Audit criteria are based on ISO 9001, ISO 27001 and ISO 27701 management system and control requirements. All ISO 27001 Annex A controls, and ISO 27701 Annex A and B controls are included in the scope of the management system as Dassault Systèmes acts in the role of both PII controller and PII processor (see Data Protection & Privacy, p.11).

The ISPMS is supported by a **3D**EXPERIENCE platform Information Security & Privacy Mission Statement (Policy Statement) and annual objectives. Objectives provide measurable goals and Key Performance Indicators (KPIs) that are monitored by operational teams. Cybersecurity and data protection objectives are reviewed regularly for suitability as part of the Dassault Systèmes annual planning process.

OUR SECURITY, PRIVACY AND COMPLIANCE PERSONNEL

R&D Executive Committee

The Dassault Systèmes R&D Executive Committee is ultimately responsible for the effectiveness of the **3D**EXPERIENCE Information Security & Privacy Management System (ISPMS) with the support of the General Counsel of Dassault Systèmes for data protection requirements and privacy. The R&D Executive Committee actively demonstrates its commitment to the ISPMS and to customer expectations through various means, including:

- Ensuring that the Information Security and Privacy Policy and annual objectives are compatible with the strategic direction of the organization;
- Ensuring the integration of the ISPMS requirements into the organization's business processes;
- Ensuring that the resources needed for the ISPMS are available;
- Communicating the importance of the ISPMS;
- Ensuring that the ISPMS achieves its intended outcomes;
- Directing and supporting persons to contribute to the effectiveness of the ISPMS;
- Promoting continual improvement of ISPMS processes and operations.

Cybersecurity, Data Privacy and Compliance Teams

Dassault Systèmes maintains an enterprise role model that defines the mission, description, deliverables, KPIs, role profile and skills associated with each position or role.

A team of Chief Information Security Officers (CISOs) and security leaders have overall responsibility for implementing the Dassault Systèmes Information Security Program. They are responsible for establishing, maintaining and enforcing information security policies, standards, guidelines and procedures at a global level.

Dassault Systèmes R&D Cybersecurity and Data Privacy are responsible for ensuring that the **3D**EXPERIENCE ISPMS is planned, implemented, maintained, and continually improved in accordance with the requirements of ISO 27001 and ISO 27701. They are responsible for monitoring compliance to, and effectiveness of, the ISPMS and for reporting on this to executive management as part of standard governance meetings.

A Group Data Protection Officer (DPO) informs and advises Dassault Systèmes on PII protection to ensure best practices, accountability, and Dassault Systèmes sustainable growth. The Group DPO is the privileged interlocutor of the data protection supervisory authorities and reports on the compliance and effectiveness of the ISPMS to the Dassault Systèmes General Counsel.

An R&D Compliance & Risk team runs an internal compliance audit program to assess Dassault Systèmes compliance to internal processes and industry certifications such as ISO 9001, ISO 27001, and ISO 27701. Audit findings and corresponding corrective and preventative action plans (CAPAs) are managed in the platform.

A Group Internal Audit team defines and assesses compliance to and effectiveness of the Dassault Systèmes Internal Control Evaluation (ICE) framework through an enterprise-level internal audit program. The Internal Control Framework helps to mitigate risks through the establishment and verification of General Controls and Information Technology General Controls (ITGC).

ONBOARDING AND TRAINING FOR ALL EMPLOYEES

Employees who join Dassault Systèmes must agree to follow our code of conduct, IT charter and data protection policies. All new employees follow mandatory ethics and compliance training addressing security and privacy, including:

- Preventing threats to data security.
- Securing physical data and workstations; clean desk policy.
- Personal data protection and confidentiality.
- Ethical business behavior; anti-corruption and competition law principles.
- Incident management; recognizing and reporting potential threats.

We continually foster security and privacy awareness throughout the organization.

SECURITY IN TELEWORK

When working remotely, Dassault Systèmes employees can access their data, applications and platform utilities only through a VPN. This applies to both company and personal devices. Only registered and approved personal devices with VPN access are permitted.

OUR PARTNERS IN CLOUD SECURITY

We work closely with our cloud infrastructure (IaaS) providers, including 3DS Outscale, to ensure security and compliance across our operations. We require our IaaS providers to be ISO 27001 certified, among other criteria.

OUR SECURITY STANDARDS

Our approach to cybersecurity is rooted in the most respected industry standards. Independent cybersecurity experts actively collaborate to establish global standards for software providers. OWASP, NIST and ISO/IEC are three such expert bodies that guide our cybersecurity and privacy teams with best practices, requirements, controls, tests and other tools for reducing risk and mitigating vulnerabilities.

OWASP: OPEN WEB APPLICATION SECURITY PROJECT[1]

OWASP is dedicated to enabling organizations to develop and maintain highly secure applications. The OWASP Foundation is the leading source for cutting-edge research, prevalent frameworks and vital information related to application security.

With the help of global alliances, OWASP provides:

- Application security tools, standards and methodologies
- Resources for secure code development, security code reviews, and application security testing
- Standard security controls and libraries

OWASP's major publications include:

- Top 10 Web Application Security Risks
- Secure Coding Practices
- Code Review Guide
- Application Security Verification Standard

NIST: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY[2]

NIST is the preeminent source for critical measurement solutions and equitable standards in electronics, software and other technologies. NIST Special Publication (SP) 800-53 defines security controls and privacy controls for information systems and organizations.

NIST SP 800-53 is designed to protect organizational operations and assets, individuals, and other entities from "a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks." These controls address security and privacy from both functionality and assurance perspectives.

ISO/IEC: INTERNATIONAL ORGANIZATION FOR STANDARDIZATION AND THE INTERNATIONAL ELECTROTECHNICAL COMMISSION[3]

ISO/IEC is a joint technical committee that works to promote standards in IT and communications technology. Our ISPMS for **3D**EXPERIENCE platform SaaS is ISO/IEC 27001:2017 and ISO/IEC 27701:2019 certified, while our QMS is ISO 9001:2015 certified, both by SGS-ICS (see "**3D**EXPERIENCE Platform SaaS Cybersecurity & Privacy Governance", p. 4).

ISO 9001 specifies requirements for a quality management system when an organization:

a. needs to demonstrate its ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements, and

b. aims to enhance customer satisfaction through the effective application of the system, including processes for improvement of the system and the assurance of conformity to customer and applicable statutory and regulatory requirements.

Our Quality Management System (QMS) is rooted in the processes used for design, development, delivery, deployment, cloud operations, and support of the **3D**EXPERIENCE platform. Many of our application security practices are embedded in our QMS.

ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS). ISO/IEC 27001 Annex A articulates the expected controls for everything from securing application services on public networks, protecting application security transactions, enforcing a secure development policy, restricting changes to software packages, abiding by secure system engineering principles, and so on.

ISO/IEC 27701 specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization. The standard provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing. Annex A specifies control objectives and controls for PII controllers and Annex B specifies control objectives and controls for PII processors.

1. Learn more: www.owasp.org
2. Learn more: csrc.nist.gov
3. Learn more: iso.org/isoiec-27001-information-security

KEY SECURITY FEATURES

AUTHENTICATION AND AUTHORIZATION

The authentication and authorization mechanism for the **3D**EXPERIENCE Cloud platform is **3D** Passport, a personalized login which allows users secure access to all their roles, apps and services. Administrators maintain user authentication policies like password strength, expiry and configure patterns to detect brute-force attempts at unlocking passwords.

3D Passport Features

Data Privacy

Every user of our online solutions has access to the Dassault Systèmes Privacy Policy and is required to accept it when creating their **3D** Passport. Users may exercise their rights according to Dassault Systèmes policies and processes by submitting a request via a webform.

In addition, a company may also present its own Privacy Policy to users for acceptance. In this case, the platform administrator uploads its own Privacy Policy through the Platform Management dashboard.

Single Sign-On (SSO)

By exchanging authentication and authorization data in a standard format, **3D** Passport provides a seamless single sign-on experience across the apps on the **3D**EXPERIENCE Cloud platform.

Multi-Factor Authentication (MFA)

A higher level of security can be achieved by leveraging MFA capabilities on the platform. For example, once MFA has been configured by an admin, the user can use a mobile app to generate a code to be entered along with the password for added security.

ACCESS CONTROL

Access control regulates who can access, view, or use resources in our cloud computing environment. These authorizations help secure customer data as well as supporting customer compliance and certification processes achievable within the **3D**EXPERIENCE Cloud platform.

ENCRYPTION

Data in transit is secured using an end-to-end HTTPS/TLS encryption protocol to protect integrity and confidentiality.

HIGH AVAILABILITY AND ANTI-DDOS

All services are protected by a high availability, high performance, load balancing proxy service which integrates with anti-DDoS (distributed denial of service) attack and blacklisting mechanisms.

OPERATIONAL SECURITY

OUR CLOUD OPERATIONS

Our cloud solutions are built and operated on a three-layer structure. We identify and monitor threats and perform mitigation at every layer using industry standards to consider and prioritize risks.

Software as a Service (SaaS)

At the highest layer is the Software as a Service (SaaS) or application layer. This is where **3D**EXPERIENCE Cloud platform users access and use their applications.

Platform as a Service (PaaS)

The middle layer is the Platform as a Service (PaaS) or platform layer. This is where our **3D**EXPERIENCE platform is built and operated. This layer allows us to securely manage our relationship with our infrastructure providers and store the databases that our SaaS layer interacts with.

Our PaaS team determines the configuration, operating system, structure, and virtual resources that make up the **3D**EXPERIENCE Cloud platform and determine how we receive information from our cloud infrastructure providers.

Critical risk mitigation strategies for our SaaS and PaaS layers include authentication, role-based access control, encryption, monitoring and auditing, DAST and SAST, middleware hardening, server hardening and SSL/TLS Checks.

Infrastructure as a Service (IaaS)

The Infrastructure as a Service (IaaS) or infrastructure layer is where our cloud computing resources are located. They provide virtualization capabilities and maintain backups and Disaster Recovery Services.

This layer offers scalability to Dassault Systèmes and our customers, with additional processing power and storage available on demand.

Our primary cloud providers are 3DS Outscale, a Dassault Systèmes Group company, and Amazon Web Services.

THE SHARED RESPONSIBILITY MODEL

In a cloud computing model, cloud providers and cloud users have a shared responsibility to ensure the highest level of security and compliance for online services. Each party is accountable for different aspects of cloud security:

- The cloud provider is responsible for the security of cloud infrastructure.
- The platform provider (Dassault Systèmes) is responsible for security configuration, management, and operation.
- The customer is responsible for security at the application layer, including admin / tenant management.
- We follow security best practices to harden and operate the cloud environment, in accordance with our cloud providers' best practices in addition to CSA (Cloud Security Alliance) and NIST guidelines.

For further information, please refer to Outscale Best Practices.

AVAILABILITY SLA (SERVICE LEVEL AGREEMENT)

Our target is to provide availability of our online services for a minimum of 99.5% of the time under which the online services are not under (i) a Planned Service Interruption or (ii) an interruption which is the result of a Customer's request.

For further information, please see our Service Level Agreement for Online Services.

VULNERABILITY MANAGEMENT

As part of our measures to continuously monitor and mitigate vulnerabilities, we apply comprehensive risk assessment to identify, analyze and evaluate risks and select risk treatment controls based on NIST SP 800-53, ISO/IEC 27001 and ISO/IEC 27701.

We employ a multi-layer vulnerability management system based on NIST best practices, combining external and in-house systems for identifying, testing and controlling vulnerabilities. A major part of our vulnerability management system is our usage of network and vulnerability scanners. If a vulnerability requiring remediation has been identified, it is logged and prioritized according to severity, then tracked until it has been remediated.

We use static code analysis (SAST), dynamic analysis (DAST) and intensive manual penetration tests in addition to controls based on OWASP best practices to continually add new security measures against potential threats.

Threat Detection Methods

Our threat detection methods include:

Malware Prevention

We prohibit the use of unauthorized software and train employees regarding the acceptable use of equipment. We have technical controls to identify malicious code and we conduct employee awareness training. In addition, we have put in place procedures to ensure an efficient and swift response in the event of a malware incident.

Monitoring

We monitor for control effectectiveness and security events on all cloud layers including middleware, network, OS Access, and OS. Automated monitoring provides real-time data on operational and functional performance.

Incident Management

We employ a systematic approach to identifying, classifying, recording, and communicating security and privacy incidents. All incidents are evaluated by the contact point based on our classification scale and dealt with through our established incident management and data breach processes.

Application-Layer Vulnerability Management

Running secure cloud SaaS and PaaS requires continuous identification and mitigations of vulnerabilities, which are common among Information and Communication Technologies. As part of our Secure Software Development Lifecycle (Secure SDLC) we integrated several key measures to identify software vulnerabilities and validate our existing security controls. These measures include static and dynamic scans in various stages of development, as well as extensive manual penetration tests.

Static Application Security Testing (SAST)

SAST automatically assesses the source code during the development process to fix issues before the code is passed to the next phase of the Secure SDLC. We work with a Gartner-leading SAST provider.

Dynamic Application Security Testing (DAST)

DAST automatically assesses the platform through the front end for architectural weaknesses and potential security vulnerabilities. Our DAST is performed using leading industry security tools.

Manual Penetration Testing

Authorized third-party security professionals manually simulate attacks on the **3D**EXPERIENCE Cloud platform or specific set of apps to confirm their security posture.

Cross-Functional Quality Engineering Testing

Our independent Quality Engineering teams contribute to the security verification process by routinely running threat scenarios. Their extensive product knowledge and strong command of key security concepts serve as an extra layer of security verification and validation.

Middleware, Network and Operating System Vulnerability Management

We use multiple vulnerability checks and credentialed scanning to identify internet-facing assets, using a Gartner-leading vulnerability scanner to quickly and efficiently identify potential flaws in our network and assets.

PATCH MANAGEMENT

We routinely apply software updates, including functional and security-related patches. Planned service interruptions occur regularly as set out in our SLA. In addition, our patch management and incident management processes take into account emergency security patches which can be applied within hours, which entail occasional unplanned service interruptions.

SECURITY MONITORING AND INCIDENT MANAGEMENT

Our comprehensive security monitoring and incident management system identifies, analyzes and responds to security threats in real time. We adopt a two-pronged approach of identifying and fixing vulnerabilities, on the one hand, and responding swiftly to security incidents.

Security Monitoring

Logs and events are centrally collected and analyzed through our SIEM (Security, Incident and Event Management) solution and monitored 24/7 by our dedicated SOC (Security Operations Center) team. Our SIEM platform collects data centrally and uses an advanced correlation engine to proactively identify security events, analyzing large volumes of security log data to identify attempted malicious activity.

Our **3D**EXPERIENCE Cloud Platform supervision and monitoring service includes dozens of indicators across the cloud layers to monitor functionality, performance and security.

Incident Response Processes

Our SOC team continuously monitors and assesses risks as identified by our SIEM solution based on the nature of the incident. We deal with incidents immediately based on our risk assessment, following our incident management procedure to NIST SP 800-61 guidelines. This includes the main phases of containment, eradication, recovery and notification.

As part of our patch management process, emergency patches are made within hours (see Patch Management).

BUSINESS RECOVERY PLANS (BCP) AND DISASTER RECOVERY PLANS (DRP)

Business Recovery Plans (BCP) and Disaster Recovery Plans (DRP) are critical to any cloud-based software provision. Our BCP addresses planning to restore computing services, software services, connections and data to full functionality in the event of a loss. Our DRP address procedures to limit or reverse losses in the case of major events.

We follow industry best practices for BCP/DRP, including:

1. Maintaining a consistent plan for the backup and recovery of customer data, and ensuring all plan components are accessible in the event of a major disaster.

2. Maintaining copies of critical data outside our production region, away from our primary data center.

3. Keeping our BCP/DRP up to date and ensuring it takes into account any changes in the production environment.

4. Exercising our BCP/DRP yearly.

5. Leveraging virtualization capabilities, such as load-balancing and failover systems, to ensure minimal service interruptions.

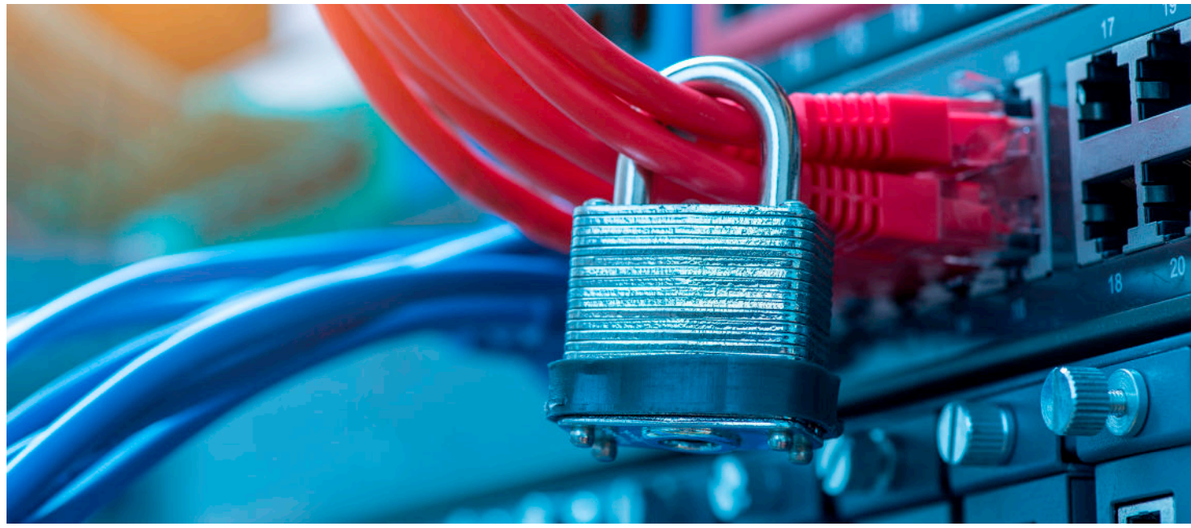
We aim for an aggressive Recovery Time Objective (RTO) and Recovery Point Objective (RPO) to ensure our customers' business continuity in all scenarios.

Data Backup and Retrieval

In keeping with our Service Level Agreement, we ensure daily back-ups of customer and user data, which is kept according to the SLA. We perform continuous hot and cold backups to minimize downtime while maximizing data protection.

3DEXPERIENCE Cloud platform customer data continues to be available for retrieval for a defined period as specified in the SLA.

For further information, please refer to our Service Level Agreement for Online Services.



DATA PROTECTION & PRIVACY

Our cloud solutions are built with respect for the privacy of our customers and users. We follow high standards to ensure that all PII is stored and handled securely, in accordance with relevant laws and standards such as the European General Data Protection Regulation 2016/679 (GDPR).

Controller

Controllers, as defined in the GDPR, need to determine policies and procedures for handling personal data, including determination of the storage retention period, compliance with PII minimization and dealing with data subjects' requests. Dassault Systèmes acts in the role of controller when processing PII related to its internal business processes and information systems.

A customer of Dassault Systèmes SaaS solutions is responsible for the handling of PII maintained in the solution and is therefore acting in the role of controller.

The GDPR and other data protection laws aim to strengthen the fundamental rights of their residents by expanding privacy rights and giving individuals control over their PII. As a global company, Dassault Systèmes complies with the GDPR, as well with other data protection laws where Dassault Systèmes conducts its business. The GDPR and other country-specific laws are referenced in the Dassault Systèmes Privacy Policy available on 3ds.com.

For the **3D**EXPERIENCE Cloud platform, Dassault Systèmes acts in the role of controller for the following:

- **3D** Passport except for private cloud offerings
- **3D** Passport created by an individual through 3ds.com
- **3D**EXPERIENCE public communities available on Dassault Systèmes public platforms
- Dassault Systèmes Customer Support
- **3D**EXPERIENCE Marketplace

In addition to the GDPR, other local data protection laws and regulations are monitored by regionally-based Dassault Systèmes Data Protection Officers and are enforced by local processes and procedures.

3D Passport is the authentication profile that is created per user. The processing of PII within **3D** Passport is under the responsibility of Dassault Systèmes. The PII associated with the **3D** Passport is stored in Europe with some specific exceptions due to regulatory requirements.

Processor

When Dassault Systèmes provides cloud-based offerings, such as the **3D**EXPERIENCE Cloud platform, Dassault Systèmes is acting as a processor for the PII it has been asked to process and store. In this capacity, Dassault Systèmes processes PII according to the contractual agreement signed between parties.

Dassault Systèmes acts in the role of processor, as defined in the GDPR, for the following:

- Dassault Systèmes Cloud offerings (private and public) provided to customers and business partners
- **3D** Passport for private Cloud offerings

When acting as processor, platform data will be stored by a third party IaaS provider (e.g. 3DS Outscale or Amazon Web Services) in a local data center.

CONCLUSION

Dassault Systèmes puts security and privacy at the heart of its operations. Our cybersecurity and data protection measures are based on the most reputable industry standards and are systematically applied through training, design requirements, security controls, privacy measures, and third-party audits and testing. We continually improve our security and privacy measures in a spirit of innovation and excellence, ensuring that we support our customers in the best way possible.

Our **3D**EXPERIENCE® platform powers our brand applications, serving 11 industries, and provides a rich portfolio of industry solution experiences.

Dassault Systèmes, the **3DEXPERIENCE** Company, is a catalyst for human progress. We provide business and people with collaborative virtual environments to imagine sustainable innovations. By creating 'virtual experience twins' of the real world with our **3DEXPERIENCE** platform and applications, our customers push the boundaries of innovation, learning and production.

Dassault Systèmes' 20,000 employees are bringing value to more than 270,000 customers of all sizes, in all industries, in more than 140 countries. For more information, visit **www.3ds.com**.

3DEXPERIENCE®

MB CAD
EIN UNTERNEHMEN DER VISIATIV GRUPPE

MB CAD GmbH | Kirchdorfer Str. 14b | D-83052 Bruckmühl
T: +49 8062 7190 | F: +49 8062 7192 | post@mbcad.de | www.mbcad.de