DASSAULT SYSTEMES

3DEXPERIENCE PLATTFORM CLOUD-SICHERHEIT UND DATENSCHUTZ

Ratgeber

INHALTSVERZEICHNIS

EINFÜHRUNG

UNSERE PHILOSOPHIE

Cloud-Computing bedeutet einen Paradigmenwechsel in der Art und Weise, wie wir Geschäfte tätigen. Unternehmen führen Anwendungen aus, verwalten Daten und verlagern Vorgänge in die Cloud, um von der Geschwindigkeit und Einfachheit der Cloud-Bereitstellung sowie von der operativen Effektivität spezialisierter Anbieter in den Bereichen Wartung, IT-Dienste und Sicherheit zu profitieren.

Dassault Systèmes bietet seit der Einführung der **3D**EXPERIENCE® Plattform im Jahr 2012 cloudbasierte Dienste an. Wir haben ein vollständiges cloudbasiertes Ökosystem geschaffen, die **3D**EXPERIENCE Cloud-Plattform, die es unseren Kunden ermöglicht, von sicheren, flexiblen und skalierbaren Cloud-Ressourcen zu profitieren. Wir haben es uns zur Aufgabe gemacht, unsere Kunden bei jedem Aspekt unserer Lösungen mit Vertrauen und Zuverlässigkeit zu unterstützen.

Unser Ansatz für das Risikomanagement ist vielschichtig und proaktiv. Er wurde auf der Grundlage von Best Practices entwickelt und ist darauf ausgerichtet, Sicherheitsbedrohungen in allen Bereichen unserer Betriebsabläufe vorherzusehen. Wir betreiben ein Managementsystem für Informationssicherheit und Datenschutz (Information Security and Privacy Management System, ISPMS), das gemäß ISO/IEC 27001:2017 und ISO/IEC 27701:2019 zertifiziert ist und regelmäßigen Prüfungen unterliegt. Unser ISPMS basiert auf den Kernwerten Vertraulichkeit, Integrität, Verfügbarkeit und Rechenschaftspflicht.

Dieses Whitepaper beschreibt den Ansatz von Dassault Systèmes in Bezug auf Sicherheit und Compliance für **3D**EXPERIENCE, unserer cloudbasierten Plattform, über die Kunden auf Anwendungen, Datenspeicher und skalierbare Computing-Ressourcen zugreifen. In diesem Whitepaper werden die Kernaspekte unserer Verfahren für Cloud-Sicherheit, Datenschutz und Compliance behandelt.

UNSER LEITBILD ZU INFORMATIONSSICHERHEIT UND DATENSCHUTZ

Das Leitbild von Dassault Systèmes zu Informationssicherheit und Datenschutz[1]:

Steuerung der Risiken im Zusammenhang mit Informationssicherheit und dem Schutz personenbezogener Daten (PII) für Software as a Service (SaaS) auf der **3D**EXPERIENCE Plattform, die kontinuierliche Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sowie:

- Schutz des geistigen Eigentums und der Nutzerdaten von Kunden, einschließlich PII
- Schutz des Rufs und geistigen Eigentums von Dassault Systèmes
- Garantierte Verfügbarkeit und Ausfallsicherheit der Cloud
- Einhaltung geltender Vorschriften und Standards für Cybersicherheit und Datenschutz

Dieses Leitbild steht den Mitarbeitern als schriftliches Dokument sowie interessierten Parteien auf Anfrage zur Verfügung.

HAFTUNGSAUSSCHLUSS

Dieser Inhalt stellt die Praktiken für Sicherheit, Datenschutz, Qualität und Compliance auf der **3D**EXPERIENCE Cloud-Plattform gemäß Stand März 2022 dar. Der Inhalt unserer hier dargelegten Praktiken kann nach alleinigem Ermessen von Dassault Systèmes geändert werden. Die Begriffe „wir" und „unser" in diesem Dokument beziehen sich konkret auf Dassault Systèmes.

1. Entsprechend der Richtlinie ISO 27001 zu Informationssicherheit und Datenschutz.

DASSAULT SYSTÈMES: EIN AUF SICHERHEIT UND DATENSCHUTZ AUSGERICHTETES UNTERNEHMEN

3DEXPERIENCE PLATTFORM: GOVERNANCE VON CYBERSICHERHEIT UND DATENSCHUTZ FÜR SAAS

Die Forschungs- und Entwicklungsabteilung (F&E) von Dassault Systèmes betreibt ein zentral gesteuertes Managementsystem für Informationssicherheit und Datenschutz (Information Security & Privacy Management System, ISPMS) für SaaS auf der **3DEXPERIENCE** Plattform, das von SGS International Certification Services (SGS-ICS) gemäß ISO/IEC 27001:2017 und ISO/IEC 27701:2019 zertifiziert ist. Die Zertifizierung umfasst Folgendes:

1. Design, Entwicklung, Bereitstellung, Einsatz, Cloud-Betrieb und Support der **3DEXPERIENCE** Plattform als SaaS
2. Datenschutzmanagement durch Dassault Systèmes als:
   - **a.** Verantwortlicher für den Umgang mit personenbezogenen Daten, die auf der **3DEXPERIENCE** Plattform als SaaS bereitgestellt werden
   - **b.** Auftragsverarbeiter für PII, die unter der Kontrolle eines Kunden stehen und als SaaS auf der **3DEXPERIENCE** Plattform verarbeitet werden

Unser ISPMS unterliegt der Verwaltung und Überprüfung durch die Entwicklungsleitung von Dassault Systèmes. Es basiert auf einem etablierten Qualitätsmanagementsystem (QMS), das auf der **3DEXPERIENCE** Plattform betrieben wird und von SGS-ICS gemäß ISO 9001:2015 zertifiziert ist.

Das QMS und das ISPMS haben viele grundlegende und unterstützende Prozesse gemeinsam, die auf einer Methodik des sicheren Softwareentwicklungszyklus, Secure SDLC (Secure Software Development Lifecycle), basieren. Das ISPMS umfasst zudem zusätzliche risikobasierte Prozesse, die sich auf Informationssicherheit und Datenschutz konzentrieren.

Alle ISPMS-Prozesse und -Kontrollen werden im Rahmen des Dassault Systèmes F&E **3DEXPERIENCE** Compliance-Prüfungsprogramms kontinuierlich im Hinblick auf Einhaltung und Effektivität bewertet. Die resultierenden Korrekturmaßnahmen und kontinuierlichen Verbesserungen werden auf der **3DEXPERIENCE** Plattform nachverfolgt.

Die Prüfungskriterien basieren auf den Anforderungen an das Managementsystem und die Kontrolle gemäß ISO 9001, ISO 27001 und ISO 27701. Alle Kontrollen gemäß ISO 27001 Anhang A und ISO 27701 Anhang A und B sind in den Geltungsbereich des Managementsystems eingeschlossen, da Dassault Systèmes sowohl als PII-Verantwortlicher als auch PII-Auftragsverarbeiter fungiert (siehe „Datenschutz und Privatsphäre", S. 11).

Das ISPMS wird durch das Leitbild der **3DEXPERIENCE** Plattform zu Informationssicherheit und Datenschutz sowie durch jährliche Zielvorgaben unterstützt. Zielvorgaben bieten messbare Ziele und Leistungskennzahlen (KPIs), die von operativen Teams überwacht werden. Die Zielvorgaben im Bereich Cybersicherheit und Datenschutz werden regelmäßig im Rahmen des jährlichen Planungsprozesses von Dassault Systèmes auf ihre Eignung überprüft.

UNSERE MITARBEITER IN DEN BEREICHEN SICHERHEIT, DATENSCHUTZ UND COMPLIANCE

Leitung der Abteilung Forschung und Entwicklung (F&E)

Die Entwicklungsleitung von Dassault Systèmes ist letztendlich für die Effektivität des **3DEXPERIENCE** Managementsystems für Informationssicherheit und Datenschutz (ISPMS) verantwortlich und wird dabei von der Rechtsabteilung von Dassault Systèmes in Bezug auf Datenschutzanforderungen unterstützt. Die Entwicklungsleitung zeigt ihr Engagement für das ISPMS und die Kundenerwartungen durch verschiedene Maßnahmen:

- Sicherstellung, dass die Informationssicherheits- und Datenschutzrichtlinie und die jährlichen Zielvorgaben mit der strategischen Ausrichtung des Unternehmens vereinbar sind
- Sicherstellung der Integration der ISPMS-Anforderungen in die Geschäftsprozesse des Unternehmens
- Sicherstellung, dass die für das ISPMS benötigten Ressourcen verfügbar sind
- Vermittlung der Relevanz des ISPMS
- Sicherstellung, dass das ISPMS die beabsichtigten Ergebnisse erzielt
- Anleitung und Unterstützung von Personen, um zur Effektivität des ISPMS beizutragen
- Förderung der kontinuierlichen Verbesserung der ISPMS-Prozesse und -Abläufe

Teams für Cybersicherheit, Datenschutz und Compliance

Dassault Systèmes verfügt über ein Unternehmensrollenmodell, das die Aufgaben, Merkmale, Ergebnisse, KPIs, Rollenprofile und die mit jeder Position oder Rolle verbundene Qualifikation definiert.

Ein Team von Chief Information Security Officers (CISOs) und Sicherheitsverantwortlichen trägt die Gesamtverantwortung für die Umsetzung des Informationssicherheitsprogramms von Dassault Systèmes. Sie sind für die Einrichtung, Pflege und Durchsetzung von Strategien, Standards, Leitlinien und Verfahren zur Informationssicherheit auf globaler Ebene verantwortlich.

Die Forschungs- und Entwicklungsabteilung (F&E) für Cybersicherheit und Datenschutz von Dassault Systèmes ist dafür verantwortlich, dass das **3D**EXPERIENCE ISPMS gemäß den Anforderungen von ISO 27001 und ISO 27701 geplant, implementiert, gewartet und kontinuierlich verbessert wird. Sie ist für die Überwachung der ISPMS-Einhaltung und -Effektivität sowie für die entsprechende Berichterstattung gegenüber der Geschäftsleitung im Rahmen von regulären Governance-Meetings verantwortlich.

Ein Konzerndatenschutzbeauftragter (DSB) informiert und berät Dassault Systèmes in Bezug auf den Schutz personenbezogener Daten, um bewährte Verfahren, Rechenschaftspflicht und ein nachhaltiges Wachstum von Dassault Systèmes zu gewährleisten. Der Konzern-DSB ist Ansprechpartner für die Datenschutzaufsichtsbehörden und erstattet gegenüber der Rechtsabteilung von Dassault Systèmes Bericht in Bezug auf die Einhaltung und Effektivität des ISPMS.

Ein Compliance- und Risikoteam der Entwicklungsabteilung (F&E) führt ein internes Prüfungsprogramm durch, um die Einhaltung interner Prozesse und Branchenzertifizierungen wie ISO 9001, ISO 27001 und ISO 27701 durch Dassault Systèmes zu überprüfen. Die Prüfungsergebnisse und die entsprechenden Pläne für Korrektur- und Vorbeugungsmaßnahmen (CAPAs) werden über die Plattform verwaltet.

Ein konzerninternes Revisionsteam definiert und bewertet die Einhaltung und Effektivität des Dassault Systèmes ICE-Frameworks (Internal Control Evaluation) mithilfe eines internen Prüfungsprogramms auf Unternehmensebene. Das ICE-Framework trägt dazu bei, Risiken durch die Einrichtung und Überprüfung allgemeiner Kontrollen und informationstechnologischer allgemeiner Kontrollen (ITGC) zu mindern.

ONBOARDING UND SCHULUNG FÜR ALLE MITARBEITER

Mitarbeiter, die für Dassault Systèmes tätig werden, müssen sich zur Einhaltung unseres Verhaltenskodex, unserer IT-Charta und unserer Datenschutzrichtlinien verpflichten. Alle neuen Mitarbeiter erhalten obligatorische Ethik- und Compliance-Schulungen zu Sicherheit und Datenschutz, einschließlich folgender Themen:

- Vermeidung von Bedrohungen für die Datensicherheit
- Sicherung von physischen Daten und Arbeitsplätzen; Clean-Desk-Richtlinie
- Schutz personenbezogener Daten und Vertraulichkeit
- Ethisches Geschäftsverhalten; Grundsätze der Korruptionsbekämpfung und des Wettbewerbsrechts
- Incident Management; Erkennen und Melden potenzieller Bedrohungen

Wir fördern kontinuierlich das Bewusstsein für Sicherheit und Datenschutz im gesamten Unternehmen.

SICHERHEIT BEI DER TELEARBEIT

Bei der Telearbeit können Mitarbeiter von Dassault Systèmes nur über ein VPN auf ihre Daten, Anwendungen und Plattform-Dienstprogramme zugreifen. Dies gilt sowohl für unternehmenseigene als auch für persönliche Geräte. Nur registrierte und genehmigte persönliche Geräte mit VPN-Zugang sind erlaubt.

UNSERE PARTNER IM BEREICH CLOUD-SICHERHEIT

Wir arbeiten eng mit unseren Anbietern von Cloud-Infrastrukturen (IaaS), darunter 3DS Outscale, zusammen, um die Sicherheit und Compliance in unseren Betriebsabläufen zu gewährleisten. Unsere IaaS-Anbieter müssen u. a. gemäß ISO 27001 zertifiziert sein.

UNSERE SICHERHEITSSTANDARDS

Unser Ansatz für Cybersicherheit basiert auf etablierten Branchenstandards. Unabhängige Experten für Cybersicherheit arbeiten aktiv zusammen, um globale Standards für Softwareanbieter festzulegen. OWASP, NIST und ISO/IEC sind drei dieser Expertengremien, die unsere Teams für Cybersicherheit und Datenschutz mit Best Practices, Formulierung von Anforderungen, Kontrollen, Tests und anderen Tools zur Reduzierung von Risiken und Schwachstellen unterstützen.

OWASP: OPEN WEB APPLICATION SECURITY PROJECT[1]

OWASP ermöglicht Unternehmen die Entwicklung und Pflege hochsicherer Anwendungen. Die OWASP Foundation ist die führende Organisation für Spitzenforschung, maßgebliche Frameworks und wichtige Informationen zur Anwendungssicherheit.

Mithilfe globaler Allianzen bietet OWASP Folgendes:

- Tools, Standards und Methoden für die Anwendungssicherheit
- Ressourcen für die Entwicklung eines sicheren Codes, Sicherheitsprüfungen des Codes und die Überprüfung der Anwendungssicherheit
- Standard-Sicherheitskontrollen und -Bibliotheken

Zu den wichtigsten Publikationen von OWASP gehören:

- Top 10 Web Application Security Risks (Die 10 kritischsten Sicherheitsrisiken für Webanwendungen)
- Secure Coding Practices (Sichere Kodierverfahren)
- Code Review Guide (Leitfaden zur Codeprüfung)
- Application Security Verification Standard (Verifikationsstandard zur Anwendungssicherheit)

NIST: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY[2]

NIST ist die führende Informationsquelle für wichtige Messlösungen und Standards in Bezug auf Elektronik, Software und andere Technologien. Die NIST Special Publication (SP) 800-53 definiert Sicherheits- und Datenschutzkontrollen für Informationssysteme und Organisationen.

NIST SP 800-53 wurde entwickelt, um die Betriebsabläufe und Anlagen von Organisationen, Einzelpersonen und anderen Einrichtungen vor einer Vielzahl von Bedrohungen und Risiken zu schützen, darunter feindliche Angriffe, menschliches Versagen, Naturkatastrophen, strukturelle Ausfälle, ausländische Geheimdienste und Datenschutzrisiken. Diese Kontrollen berücksichtigen Sicherheit und Datenschutz aus der Funktions- und Gewährleistungsperspektive.

ISO/IEC: INTERNATIONAL ORGANIZATION FOR STANDARIZATION UND INTERNATIONAL ELECTROTECHNICAL COMMISION[3]

ISO/IEC ist ein gemeinschaftliches technisches Komitee, das sich für die Förderung von Standards in der Informations- und Kommunikationstechnologie einsetzt. Unser ISPMS für SaaS auf der **3D**EXPERIENCE Plattform ist gemäß ISO/IEC 27001:2017 und ISO/IEC 27701:2019 zertifiziert, während unser QMS gemäß ISO 9001:2015 zertifiziert ist, beide durch SGS-ICS (siehe „**3D**EXPERIENCE Plattform: Governance von Cybersicherheit und Datenschutz für SaaS", S. 4).

ISO 9001 legt die Anforderungen an ein Qualitätsmanagementsystem fest, wenn eine Organisation:

a. nachweisen muss, dass sie in der Lage ist, konsistent Produkte und Dienstleistungen zu liefern, die den Anforderungen des Kunden und den geltenden gesetzlichen Auflagen entsprechen

b. darauf abzielt, die Kundenzufriedenheit durch die effektive Anwendung des Systems zu steigern, einschließlich der Prozesse zur Verbesserung des Systems und zur Sicherstellung der Konformität mit den Kundenanforderungen und mit geltenden gesetzlichen Auflagen.

Grundlage unseres Qualitätsmanagementsystems (QMS) bilden die Prozesse, die für das Design, die Entwicklung, die Bereitstellung, den Einsatz, den Cloud-Betrieb und den Support der **3D**EXPERIENCE Plattform verwendet werden. Viele unserer Verfahren zur Anwendungssicherheit sind in unser QMS integriert.

ISO/IEC 27001 legt die Anforderungen für die Einrichtung, Implementierung, Pflege und kontinuierliche Verbesserung eines Managementsystems für Informationssicherheit (ISMS, Information Security Management System) fest. ISO/IEC 27001 Anhang A erläutert die erwarteten Kontrollen für alle Bereiche, von der Sicherung von Anwendungsdiensten in öffentlichen Netzwerken über den Schutz von Transaktionen im Rahmen der Anwendungssicherheit, die Durchsetzung einer sicheren Entwicklungsrichtlinie, die Beschränkung von Änderungen an Softwarepaketen bis hin zur Einhaltung von Grundsätzen der Systementwicklung.

ISO/IEC 27701 legt Anforderungen fest und bietet Anleitungen für die Einrichtung, Implementierung, Pflege und kontinuierliche Verbesserung eines Managementsystems für Datenschutzinformationen (PIMS, Privacy Information Management System) in Form einer Erweiterung von ISO/IEC 27001 und ISO/IEC 27002 für das Datenschutzmanagement im Kontext der Organisation. Der Standard enthält Leitlinien für PII-Verantwortliche und PII-Auftragsverarbeiter, die für die PII-Verarbeitung zuständig und verantwortlich sind. In Anhang A sind die Kontrollzielvorgaben und Kontrollen für PII-Verantwortliche und in Anhang B die Kontrollzielvorgaben und Kontrollen für PII-Auftragsverarbeiter aufgeführt.

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

WICHTIGE SICHERHEITS-FUNKTIONEN

AUTHENTIFIZIERUNG UND AUTORISIERUNG

Der Authentifizierungs- und Autorisierungsmechanismus für die **3D**EXPERIENCE Cloud-Plattform ist der **3D** Passport, eine personalisierte Anmeldefunktion, die Anwendern einen sicheren Zugriff auf alle Rollen, Apps und Dienste ermöglicht. Administratoren verwalten die Richtlinien für die Benutzerauthentifizierung, z. B. Passwortstärke und -ablaufdatum, und konfigurieren Muster, um Brute-Force-Angriffsversuche zur Entschlüsselung von Passwörtern zu erkennen.

Sicherheitsfunktionen des 3D Passport

Datenschutz
Jeder Nutzer unserer Online-Lösungen hat Zugang zu der Datenschutzrichtlinie von Dassault Systèmes und muss diese akzeptieren, wenn er seinen **3D** Passport erstellt. Nutzer können ihre Rechte gemäß der Richtlinien und Verfahren von Dassault Systèmes ausüben, indem sie eine Anfrage über ein Webformular einreichen.

Darüber hinaus kann ein Unternehmen seinen Nutzern eine eigene Datenschutzrichtlinie zur Annahme vorlegen. In diesem Fall lädt der Plattformadministrator die eigene Datenschutzrichtlinie über das Plattform-Management-Dashboard hoch.

Single Sign-On (SSO)
Durch den Austausch von Authentifizierungs- und Autorisierungsdaten in einem Standardformat bietet der **3D** Passport eine nahtlose Single Sign-On-Funktion für alle Apps auf der **3D**EXPERIENCE Cloud-Plattform.

Multi-Faktor-Authentifizierung (MFA)
Sie können die Sicherheit weiter erhöhen, indem Sie auf der Plattform MFA-Funktionen nutzen. Sobald die MFA von einem Administrator konfiguriert wurde, kann der Nutzer beispielsweise über eine mobile App einen Code generieren, der zusammen mit dem Passwort für zusätzliche Sicherheit eingegeben wird.

ZUGRIFFSSTEUERUNG

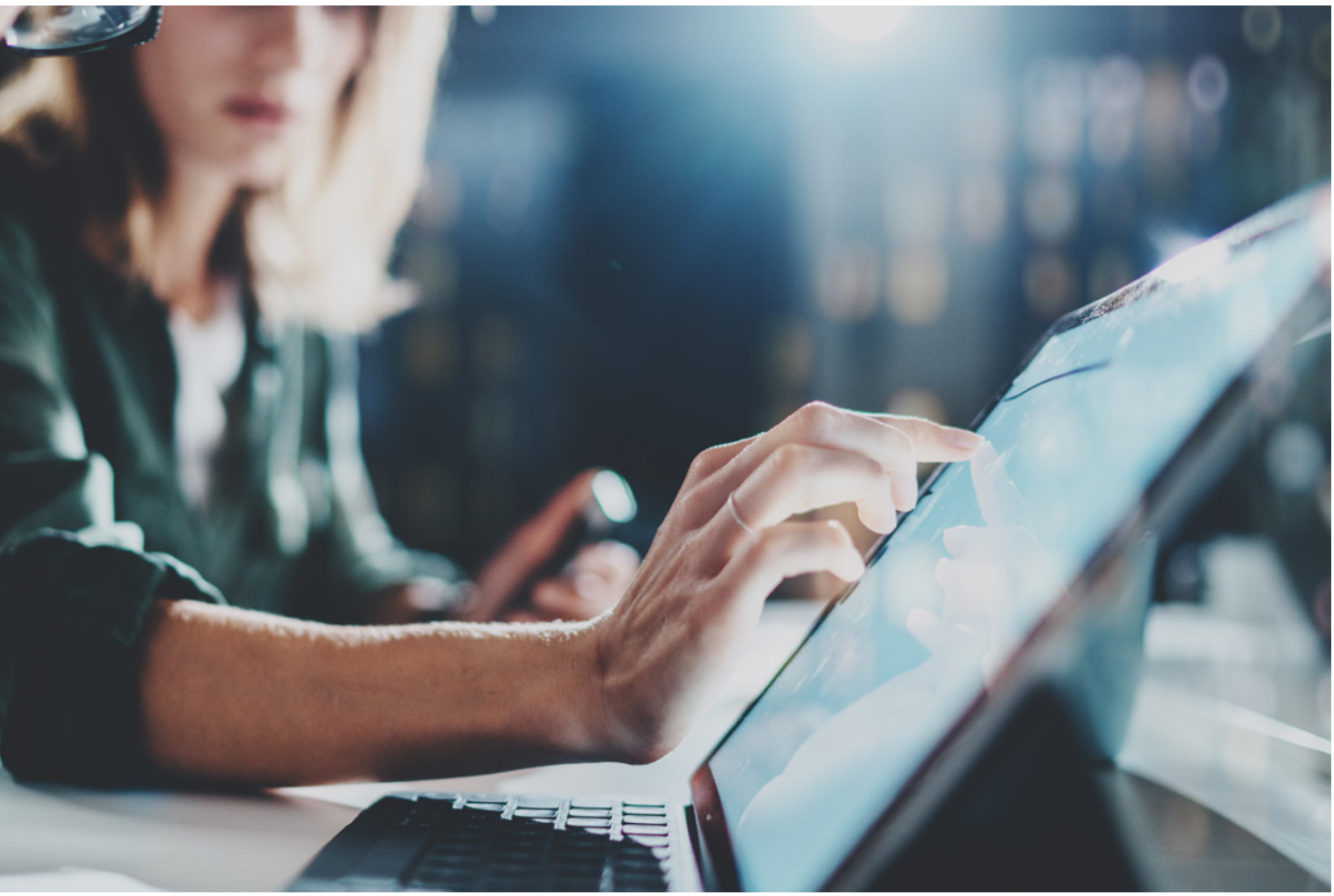
Die Zugriffssteuerung regelt, wer auf Ressourcen in unserer Cloud-Computing-Umgebung zugreifen, diese anzeigen oder nutzen kann. Diese Autorisierungen helfen dabei, Kundendaten zu schützen und die Compliance- und Zertifizierungsprozesse von Kunden zu unterstützen, die innerhalb der **3D**EXPERIENCE Cloud-Plattform eingerichtet werden können.

VERSCHLÜSSELUNG

Daten werden während der Übertragung mithilfe eines End-to-End-HTTPS/TLS-Verschlüsselungsprotokolls gesichert, um die Integrität und Vertraulichkeit zu gewährleisten.

HOCHVERFÜGBARKEIT UND ANTI-DDOS

Alle Dienste sind durch einen Hochleistungs-Proxy-Dienst mit Hochverfügbarkeit und Lastenausgleich geschützt, der in Maßnahmen zur Abwehr von DDoS-Angriffen (Distributed Denial of Service), einschließlich Blacklisting, integriert ist.



OPERATIVE SICHERHEIT

UNSER CLOUD-BETRIEB

Unsere Cloud-Lösungen basieren auf einer dreischichtigen Struktur. Wir identifizieren und überwachen Bedrohungen und ergreifen auf jeder Ebene Abwehrmaßnahmen. Dabei nutzen wir Branchenstandards, um Risiken zu berücksichtigen und zu priorisieren.

Software as a Service (SaaS)

Die oberste Ebene bildet die SaaS- oder Anwendungsebene. Hier greifen Nutzer der **3D**EXPERIENCE Cloud-Plattform auf ihre Anwendungen zu.

Platform as a Service (PaaS)

Die mittlere Ebene ist die PaaS- oder Plattformebene. Hier wird unsere **3D**EXPERIENCE Plattform eingerichtet und betrieben. Diese Ebene ermöglicht uns, die Beziehungen zu unseren Infrastrukturanbietern sicher zu verwalten und die Datenbanken zu speichern, mit denen die SaaS-Ebene interagiert.

Unser PaaS-Team legt die Konfiguration, das Betriebssystem, die Struktur und die virtuellen Ressourcen fest, aus denen die **3D**EXPERIENCE Cloud-Plattform besteht, und bestimmt, wie wir Informationen von unseren Cloud-Infrastrukturanbietern empfangen.

Zu den Strategien zur Risikominimierung für unsere SaaS- und PaaS-Ebenen gehören Authentifizierung, rollenbasierte Zugriffssteuerung, Verschlüsselung, Überwachung und Prüfung, DAST und SAST, Middleware- und Serverschutz sowie SSL/TLS-Prüfungen.

Infrastructure as a Service (IaaS)

Auf der IaaS- bzw. Infrastrukturebene befinden sich unsere Cloud-Computing-Ressourcen. Sie bieten Virtualisierungsfunktionen und verwalten Backups und Notfallwiederherstellungsdienste (Disaster Recovery Services).

Diese Ebene bietet Dassault Systèmes und unseren Kunden Skalierbarkeit, da bei Bedarf zusätzliche Rechenleistung und Speicherkapazität verfügbar ist.

Unsere primären Cloud-Anbieter sind 3DS Outscale, ein Unternehmen der Dassault Systèmes Group, und Amazon Web Services.

DAS MODELL DER GETEILTEN VERANTWORTUNG

In einem Cloud-Computing-Modell sind Cloud-Anbieter und Cloud-Nutzer gemeinsam dafür verantwortlich, ein Höchstmaß an Sicherheit und Compliance für Online-Dienste zu gewährleisten. Jede Partei ist für verschiedene Aspekte der Cloud-Sicherheit verantwortlich:

- Der Cloud-Anbieter ist für die Sicherheit der Cloud-Infrastruktur zuständig.
- Der Plattformanbieter (Dassault Systèmes) ist für die Sicherheitskonfiguration, die Verwaltung und den Betrieb verantwortlich.
- Der Kunde ist für die Sicherheit auf der Anwendungsebene zuständig, einschließlich Administration und Mandantenverwaltung.
- Wir befolgen bewährte Sicherheitsverfahren, um die Cloud-Umgebung zu stärken und zu betreiben, in Übereinstimmung mit den Best Practices unserer Cloud-Anbieter, zusätzlich zu den CSA (Cloud Security Alliance)- und NIST-Richtlinien.

Weitere Informationen finden Sie in den Best Practices von Outscale.

GARANTIERTE VERFÜGBARKEIT NACH SLA (SERVICE LEVEL AGREEMENT)

Unser Ziel ist es, die Verfügbarkeit unserer Online-Dienste für mindestens 99,5 % der Zeit zu gewährleisten, in der die Online-Dienste nicht durch (i) eine geplante Dienstunterbrechung oder (ii) eine Unterbrechung infolge einer Kundenanfrage eingeschränkt sind.

Weitere Informationen finden Sie in unserem Service Level Agreement für Online-Dienste.

SCHWACHSTELLEN-MANAGEMENT

Im Rahmen unserer Maßnahmen zur kontinuierlichen Überwachung und Minderung von Schwachstellen nehmen wir eine umfassende Risikobewertung vor, um Risiken zu identifizieren, zu analysieren und zu bewerten und Kontrollen zur Risikobehandlung basierend auf NIST SP 800-53, ISO/IEC 27001 und ISO/IEC 27701 auszuwählen.

Wir verwenden ein mehrschichtiges System für das Schwachstellenmanagement, das auf Best Practices von NIST basiert und externe und interne Systeme zur Identifizierung, Prüfung und Kontrolle von Schwachstellen kombiniert. Ein wichtiger Bestandteil des Systems ist die Verwendung von Netzwerk- und Schwachstellenscannern. Wenn eine Schwachstelle identifiziert wurde, die behoben werden muss, wird sie protokolliert, nach dem Schweregrad priorisiert und anschließend nachverfolgt, bis sie behoben ist.

Wir nutzen die statische Codeanalyse (SAST), die dynamische Analyse (DAST) und intensive manuelle Penetrationstests zusätzlich zu Kontrollen auf der Grundlage von OWASP-Best-Practices, um kontinuierlich neue Sicherheitsmaßnahmen gegen potenzielle Bedrohungen hinzuzufügen.

Methoden zur Bedrohungserkennung

Unsere Methoden zur Bedrohungserkennung umfassen Folgendes:

Malware-Schutz

Wir verbieten die Verwendung von nicht autorisierter Software und schulen Mitarbeiter in der zulässigen Verwendung von Geräten. Wir verfügen über technische Kontrollen, um Schadcode zu identifizieren, und führen Schulungen zur Sensibilisierung unserer Mitarbeiter durch. Darüber hinaus haben wir Verfahren eingeführt, um eine effiziente und schnelle Reaktion bei einem Malware-Vorfall zu gewährleisten.

Überwachung

Wir überwachen die Effektivität der Kontrollen und das Auftreten von sicherheitsrelevanten Ereignissen auf allen Cloud-Ebenen, einschließlich Middleware, Netzwerk, Betriebssystemzugriff und Betriebssystem. Die automatisierte Überwachung liefert Echtzeitdaten zur operativen und funktionalen Leistung.

Vorfallmanagement (Incident Management)

Wir verfolgen einen systematischen Ansatz zur Identifizierung, Klassifizierung, Aufzeichnung und Kommunikation von Sicherheits- und Datenschutzvorfällen. Alle Vorfälle werden von der Kontaktstelle anhand unserer Klassifizierungsskala bewertet und im Rahmen unserer etablierten Vorfallmanagement- und Datenschutzverletzungsprozesse behandelt.

Schwachstellenmanagement auf Anwendungsebene

Sicheres SaaS und PaaS in der Cloud erfordert eine kontinuierliche Identifizierung und Verringerung von Schwachstellen, die bei Informations- und Kommunikationstechnologien häufig auftreten. Im Rahmen unseres Secure Software Development Lifecycle (Secure SDLC) haben wir mehrere wichtige Maßnahmen integriert, um Softwareschwachstellen zu identifizieren und unsere bestehenden Sicherheitskontrollen zu validieren. Zu diesen Maßnahmen gehören statische und dynamische Scans in verschiedenen Entwicklungsphasen sowie umfangreiche manuelle Penetrationstests.

Statische Anwendungssicherheitstests (SAST)

SAST bewertet den Quellcode automatisch während des Entwicklungsprozesses, um Probleme zu beheben, bevor der Code an die nächste Phase des Secure SDLC weitergeleitet wird. Wir arbeiten mit einem bei Gartner führenden SAST-Anbieter zusammen.

Dynamische Anwendungssicherheitstests (DAST)

DAST bewertet die Plattform über das Frontend automatisch hinsichtlich Architekturschwächen und potenziellen Sicherheitslücken. Unser DAST-Verfahren wird mit führenden Sicherheitstools der Branche durchgeführt.

Manuelle Penetrationstests

Autorisierte Sicherheitsexperten von Drittanbietern simulieren manuell Angriffe auf die **3D**EXPERIENCE Cloud-Plattform oder bestimmte Anwendungen, um die Sicherheitslage zu prüfen.

Funktionsübergreifende Qualitätssicherungstests

Unsere unabhängigen Qualitätssicherungsteams tragen durch die regelmäßige Ausführung von Bedrohungsszenarien zur Sicherheitsüberprüfung bei. Ihr umfassendes Produktwissen und ihre Vertrautheit mit wichtigen Sicherheitskonzepten dienen als zusätzliche Ebene der Sicherheitsüberprüfung und -validierung.

Management von Middleware-, Netzwerk- und Betriebssystemschwachstellen

Wir führen mehrere Schwachstellentests sowie Scans unter Verwendung von Anmeldedaten durch, um über das Internet von außen zugängliche Punkte zu identifizieren. Wir nutzen dabei einen bei Gartner führenden Schwachstellenscanner, um potenzielle Schwachstellen in unserem Netzwerk und unseren Assets schnell und effizient zu identifizieren.

PATCH-MANAGEMENT

Wir führen regelmäßig Software-Updates durch, einschließlich funktionaler und sicherheitsrelevanter Patches. Geplante Dienstunterbrechungen erfolgen regelmäßig, wie in unserem SLA festgelegt. Darüber hinaus berücksichtigen unsere Patch-Management- und Incident-Management-Prozesse Sicherheitspatches für Notfälle, die innerhalb von Stunden angewendet werden können und die gegebenenfalls zu ungeplanten Dienstunterbrechungen führen.

SICHERHEITSÜBERWACHUNG UND INCIDENT MANAGEMENT

Unser umfassendes Sicherheitsüberwachungs- und Vorfallmanagementsystem identifiziert, analysiert und reagiert in Echtzeit auf Sicherheitsbedrohungen. Wir verfolgen einen zweigleisigen Ansatz, um einerseits Schwachstellen zu identifizieren und zu beheben und andererseits schnell auf Sicherheitsvorfälle zu reagieren.

Sicherheitsüberwachung

Protokolle und Ereignisse werden zentral über unsere SIEM-Lösung (Security, Incident and Event Management) erfasst und analysiert und rund um die Uhr von unserem dedizierten SOC-Team (Security Operations Center) überwacht. Unsere SIEM-Plattform erfasst Daten zentral und verwendet eine fortschrittliche Korrelations-Engine, um Sicherheitsereignisse proaktiv zu identifizieren. Dabei werden große Mengen an Sicherheitsprotokolldaten analysiert, um Versuche schädlicher Aktivitäten zu erkennen.

Der Kontroll- und Monitoring-Service der **3D**EXPERIENCE Cloud-Plattform umfasst Dutzende von Indikatoren auf den verschiedenen Cloud-Ebenen zur Überwachung von Funktionalität, Leistung und Sicherheit.

Incident Response-Prozesse

Unser SOC-Team überwacht und bewertet kontinuierlich die von unserer SIEM-Lösung identifizierten Risiken basierend auf der Art des Vorfalls. Wir behandeln Vorfälle sofort auf der Grundlage unserer Risikobewertung und befolgen dabei unser Vorfallmanagementverfahren gemäß den NIST SP 800-61-Richtlinien. Dies umfasst die Hauptphasen der Eindämmung, Beseitigung, Wiederherstellung und Benachrichtigung.

Im Rahmen unseres Patch-Management-Prozesses werden innerhalb von Stunden Notfallpatches erstellt (siehe „Patch-Management").

BETRIEBS- UND NOTFALLWIEDERHERSTELLUNGSPLÄNE (BCP/DRP)

Betriebswiederherstellungspläne (Business Recovery Plans, BCPs) und Notfallwiederherstellungspläne (Disaster Recovery Plans, DRPs) sind für jede cloudbasierte Softwarebereitstellung von entscheidender Bedeutung. Unser BCP umfasst im Schadensfall die vollständige Wiederherstellung der Computing-Dienste, Softwaredienste, Verbindungen und Daten. Unser DRP beinhaltet Verfahren zum Begrenzen oder Rückgängigmachen von Verlusten bei größeren Ereignissen.

Wir befolgen die Best Practices der Branche für BCP/DRP, einschließlich:

1. Pflege eines konsistenten Plans für die Sicherung und Wiederherstellung von Kundendaten sowie Zugänglichkeit aller Plankomponenten bei einem bedeutenden Zwischenfall

2. Pflege von Kopien kritischer Daten außerhalb der Produktionsregion, fern vom primären Rechenzentrum

3. Gewährleistung der Aktualität unseres BCP/DRP sowie Berücksichtigung eventueller Änderungen in der Produktionsumgebung

4. Jährliche Durchführung des BCP/DRP

5. Nutzung von Virtualisierungsfunktionen wie Lastausgleichs- und Ausfallsicherungssystemen zur Minimierung von Dienstunterbrechungen

Wir streben ein ehrgeiziges RTO- und RPO-Ziel (Recovery Time Objective und Recovery Point Objective) an, um die Geschäftskontinuität unserer Kunden in allen Szenarien zu gewährleisten.

Datensicherung und Datenwiederherstellung

In Übereinstimmung mit unserem Service Level Agreement erstellen wir täglich Sicherungen von Kunden- und Benutzerdaten, die gemäß SLA aufbewahrt werden. Wir führen kontinuierliche Hot und Cold Backups durch, um Ausfallzeiten zu minimieren und gleichzeitig die Datensicherheit zu maximieren.

Die Kundendaten der **3D**EXPERIENCE Cloud-Plattform sind gemäß SLA für einen festgelegten Zeitraum weiterhin abrufbar.

Weitere Informationen finden Sie in unserem Service Level Agreement für Online-Dienste.

DATENSCHUTZ UND PRIVAT-SPHÄRE

Bei der Entwicklung unserer Cloud-Lösungen achten wir auf den Schutz der Privatsphäre unserer Kunden und Anwender. Wir befolgen hohe Standards, um sicherzustellen, dass alle personenbezogenen Daten (PII) in Übereinstimmung mit den relevanten Gesetzen und Standards, wie der europäischen Datenschutz-Grundverordnung 2016/679 (DSGVO), sicher gespeichert und gehandhabt werden.

Verantwortlicher

Verantwortliche, wie in der DSGVO definiert, müssen Richtlinien und Verfahren für den Umgang mit personenbezogenen Daten festlegen, einschließlich der Bestimmung der Aufbewahrungsfrist, der Einhaltung der Minimierung der PII-Datenerfassung und des Umgangs mit Anfragen von betroffenen Personen. Dassault Systèmes übernimmt bei der Verarbeitung von personenbezogenen Daten im Zusammenhang mit internen Geschäftsprozessen und Informationssystemen die Rolle des Verantwortlichen.

Ein Kunde der SaaS-Lösungen von Dassault Systèmes ist für den Umgang mit in der Lösung gespeicherten personenbezogenen Daten verantwortlich und agiert daher ebenfalls in der Rolle eines Verantwortlichen.

Die DSGVO und andere Datenschutzgesetze zielen darauf ab, die grundlegenden Rechte der Bürger zu stärken, indem sie das Recht auf Privatsphäre erweitern und Einzelpersonen die Kontrolle über ihre personenbezogenen Daten geben. Als globales Unternehmen hält Dassault Systèmes die DSGVO und andere Datenschutzgesetze ein, wo immer Dassault Systèmes tätig ist. Die DSGVO und andere länderspezifische Gesetze sind in der Datenschutzrichtlinie von Dassault Systèmes aufgeführt, die auf 3ds.com verfügbar ist.

In Bezug auf die **3D**EXPERIENCE Cloud-Plattform übernimmt Dassault Systèmes die Rolle des Verantwortlichen für Folgendes:

- **3D** Passport mit Ausnahme von privaten Cloud-Angeboten
- **3D** Passport, der von einer Einzelperson über 3ds.com erstellt wurde
- Öffentliche **3D**EXPERIENCE Communitys, die auf öffentlichen Plattformen von Dassault Systèmes verfügbar sind
- Dassault Systèmes Kundensupport
- **3D**EXPERIENCE Marketplace

Zusätzlich zur DSGVO wird die Einhaltung sonstiger lokaler Datenschutzgesetze und -vorschriften von den regional ansässigen Datenschutzbeauftragten (Data Protection Officers) von Dassault Systèmes überwacht und durch lokale Prozesse und Verfahren sichergestellt.

Der **3D** Passport ist das Authentifizierungsprofil, das für jeden Benutzer erstellt wird. Die Verarbeitung von personenbezogenen Daten innerhalb des **3D** Passports unterliegt der Verantwortung von Dassault Systèmes. Die mit dem **3D** Passport verknüpften personenbezogenen Daten werden in Europa gespeichert, mit gewissen Ausnahmen aufgrund gesetzlicher Auflagen.

Auftragsverarbeiter

Wenn Dassault Systèmes cloudbasierte Angebote wie die **3D**EXPERIENCE Cloud-Plattform anbietet, fungiert Dassault Systèmes als Auftragsverarbeiter für die personenbezogenen Daten, mit deren Verarbeitung und Speicherung es beauftragt wurde. In dieser Rolle verarbeitet Dassault Systèmes personenbezogene Daten gemäß der zwischen den Parteien geschlossenen vertraglichen Vereinbarung.

Dassault Systèmes übernimmt für Folgendes die Rolle des Auftragsverarbeiters, wie in der DSGVO definiert:

- Cloud-Angebote von Dassault Systèmes (private und öffentliche) für Kunden und Geschäftspartner
- **3D** Passport für private Cloud-Angebote

Wenn Dassault Systèmes als Auftragsverarbeiter fungiert, werden Plattformdaten von einem IaaS-Drittanbieter (z. B. 3DS Outscale oder Amazon Web Services) in einem lokalen Rechenzentrum gespeichert.

FAZIT

Bei Dassault Systèmes stehen Sicherheit und Datenschutz im Mittelpunkt der Unternehmensaktivität. Unsere Maßnahmen zur Cybersicherheit und zum Datenschutz basieren auf etablierten Branchenstandards und werden systematisch über Schulungen, Designanforderungen, Sicherheitskontrollen, Datenschutzmaßnahmen sowie Prüfungen und Tests durch Drittanbieter umgesetzt. Wir verbessern unsere Sicherheits- und Datenschutzmaßnahmen kontinuierlich durch Innovationen und herausragende Leistungen und stellen sicher, dass wir unsere Kunden bestmöglich unterstützen.

Die **3D**EXPERIENCE® Plattform bildet die Grundlage unserer, in 11 Branchen eingesetzten, Anwendungen und bietet ein breites Spektrum an Branchenlösungen.

Dassault Systèmes, die **3DEXPERIENCE** Company, begreift sich als Katalysator für menschlichen Fortschritt. Wir stellen Unternehmen und Menschen virtuelle Arbeitsumgebungen bereit, um gemeinsam nachhaltige Innovationen zu entwickeln. Mit Unterstützung der **3DEXPERIENCE** Plattform und ihren Anwendungen erstellen unsere Kunden virtuelle Zwillinge der realen Welt, um die Grenzen von Innovation, Wissen und Produktion stetig zu erweitern.

Die 20.000 Mitarbeiterinnen und Mitarbeiter von Dassault Systèmes schaffen Mehrwert für mehr als 270.000 Kunden aller Größenordnungen aus sämtlichen Branchen in über 140 Ländern. Weitere Informationen finden Sie unter **www.3ds.com/de**.

3DEXPERIENCE®

DASSAULT SYSTEMES | The **3D**EXPERIENCE® Company

Europa /Mittlerer Osten /Afrika
Dassault Systèmes
10, rue Marcel Dassault
CS 40501
78946 Vélizy-Villacoublay Cedex
Frankreich

Amériques
Dassault Systèmes
175 Wyman Street
Waltham, MA 02451
Etats-Unis

Asie-Pacifique
Dassault Systèmes K.K.
ThinkPark Tower,
2-1-1 Osaki, Shinagawa-ku,
Tokyo 141-6020
Japon