AUTODESK

Data Transfer White Paper

Autodesk's role in data protection when transferring data across borders

Table of Contents

Introduction

This data transfer whitepaper intends to explain the safeguards and supplementary commitments Autodesk offers to protect our customers' data when transferring data across borders. On the 20th of July 2020, the European Court of Justice (CJEU) invalidated the EU-U.S. Privacy Shield data transfer mechanism. This Ruling is commonly referred to as "Schrems II". Following this ruling, entities who wish to export data to a non-EU country need to assess the laws of that third country to determine whether it provides protection essentially equivalent to that guaranteed by EU law in order to assess whether the Standard Contractual Clauses (SCCs) can ensure an adequate level of protection. Autodesk will continue to rely on the use of SCCs, which remain valid under "Schrems" II, as a legal mechanism for transferring personal data of its customers from the EU to the U.S. or other applicable jurisdictions. Furthermore, Autodesk is certified byt the new Data Privacy Framework to replace Privacy Shield.

This Whitepaper can assist Autodesk customers in assessing the impact of Schrems II, and the subsequent guidance on how to comply with data transfers published by the European Data Protection Board, when assessing compliance needs related to the transfer of EU personal data.

DISCLAIMER:

The content contained here is correct as of August 2023. However, Autodesk's security and privacy practices are subject to change as we continuously work to enhance data protection for our customers.

Controls to Protect Personal Data

Autodesk has implemented a combination of technical administrative, and organizational controls, to protect personal data when in transit and at rest.

Technical Controls

Autodesk has a Cryptographic Controls Policy based on industry practices and enforces industry standard encryption algorithms to secure data in transit and data at rest using encryption keys from trusted enterprise providers. Transport Layer Security (TLS) protects user access via the internet, helping to secure network traffic from passive eavesdropping, active tampering or message forgery. File-based integrations can be encrypted via PGP or a public/private key pair generated by the Recipient, using a customer-generated certificate. WS-Security is also supported for web services integrations to the Recipient. We have selected industry standard attestations and certifications for our products—SSAE-16 AT 101 SOC 2 attestation ISO 27001, ISO 27017, ISO 27018 certifications. For additional information on our security certification please visit our Trust Center.

Organizational Controls

Autodesk employees undertake Information security awareness training. The training includes an acknowledgement of and commitment to the Information Security Policy. Additional security training (e.g., secure development practices) is also required for certain job roles. Employees that have access to confidential data are hired under organizational procedures that address information security, including a detailed application form, background verification (where allowed by law), and agreement to confidentiality terms. Furthermore, all company employees are required to comply with Autodesk's Code of Business Conduct. Regular internal and external independent assessments are conducted to identify potential areas of improvement. Staff may undertake privacy training annually.

Administrative Controls

Autodesk has implemented internal procedures that govern how we will handle Government Access Requests. Autodesk will not transfer Personal Data to a requesting authority unless it is legally required to do and will legally challenge requests when it is appropriate to do so. Autodesk publishes a Transparency Report on its website annually. As outlined in our Transparency Report, Autodesk receives very few Government Requests and has not received a FISA 702, or an Executive Order 12333 request.

Physical Security Controls

Control of physical access to Autodesk facilities will be maintained by the use of a card access or other equivalent system that provides reasonable assurance that access to its facilities is limited to authorized individuals. Physical security measures are regularly assessed, including through review of independent reports.

Security Scans/Monitoring/Security Alerts

Autodesk monitors for unusual activity to detect potential compromises and vulnerabilities. Detected information security incidents are reported to and investigated by an Autodesk response team. Forensic and threat intelligence processes are employed to establish root cause, impact, and context of incidents. Incidents are categorized based on severity and directed to the appropriate team for response and remediation. The response team uses processes set forth in Autodesk's incident response plan to manage incidents and coordinate activities. This plan includes procedures for handling each phase of the incident lifecycle: detection, containment, eradication, and recovery.

Contractual Measures

We are committed to strong privacy and security protections for customer data that is entrusted to us. Autodesk will continue to use Standard Contractual Clauses (SCCs), which remain valid under the recent Schrems II decision by the CJEU, as a legal mechanism for the transferring of personal data of customers from the EEA to the U.S. or other applicable jurisdictions. In addition, Autodesk's Binding Corporate Rules (BCRs) for controller and processor data transfers have been approved by EU Data Protection Authorities. For further information on our data privacy practices, please visit the Privacy section of our website, and our Privacy Statement.

Autodesk already offers the following Data Protection terms:

New Standard Contractual Clauses

The European Commission introduced new Standard Contractual Clauses on June 5th. In response to these new regulatory changes, we revised our customer and vendor Data Protection Agreements to reflect these new changes. A copy of our newly revised data protection Agreement can be found here.

Binding Corporate Rules

Autodesk has adopted Binding Corporate Rules (BRCs) for controller and processor data transfers that have been approved by the Irish Data Protection Commission.

BCRs are a comprehensive set of internal policies and procedures designed to govern the processing of personal data within multinational organizations. By implementing BCRs, Autodesk ensures consistent and sufficient protection of personal data across all regions where it operates, bolstering its commitment to data privacy.

Schrems II Contractual Requirements

Following the decision in Schrems II, Autodesk has implemented processes and procedures to comply and help our customers comply with their EU data transfer obligations in line with the requirements of the European Data Protection Board and applicable data protection authorities. According to these new requirements, organizations must take the following 6 steps to ensure that they comply with EU data protection law when carrying out onward data transfers:

(i) **Identify international data transfers:** The EDPB Recommendations advise that all International Transfers are transparently identified. In this context, remote access from a third country, such as in IT support situations, also qualifies as an International Transfer. Autodesk transfers data in its capacity as a processor and controller. For assessing your obligations as a controller, Autodesk's Data Processing Addendum (DPA) governs data transfers when acting as a processor for your data.

The DPA has incorporated the new SCCs as a default. For other intracompany transfers, Autodesk has a data transfer Agreement in place which has been updated to reflect the new SCCs.

(ii) **Identify the Data Transfer Mechanism:** As noted previously, Autodesk relies on Standard Contractual Clauses to transfer data internationally. Autodesk will continue to use Standard Contractual Clauses (SCCs), which remain valid under the recent Schrems II decision by the CJEU, as a legal mechanism for transferring personal data of its customers from the EEA to the U.S. or other applicable jurisdictions. We have recently revised our Data Processing Agreement (DPA) to incorporate the new Standard Contractual Clauses which were adopted by the European Commission in June 2021. In addition, Autodesk's Binding Corporate Rules (BCRs) have been approved by EU Data Protection Authorities. Furthermore, we ensure that any sub-processor that Autodesk uses has undergone rigorous privacy and security checks to ensure that they comply with Schrems II requirements

(iii) **Assess the laws of third countries:** Following Schrems II, organizations around the world have begun conducting Transfer Impact Assessments. These TIAs typically consider the sufficiency of foreign protections on a case-by-case basis when data is transferred using SCCs, BCRs or other EU-approved data transfer mechanisms. Given the global impact of the ruling and breadth of sectors affected, there are many ways to approach such assessments in line with EU guidance. As a way of ensuring that our customers have sufficient information to adequately assess Autodesk's data transfers, we have compiled a TIA document that we can share on request from our customers

(iv) **Adopt Supplementary Measures:** If our customers determine that in all the circumstances of the transfer, and following their assessment of our Transfer Impact Assessment, that additional Technical and Organizational Measures are required, Autodesk has drafted a 'Supplementary Measures Addendum' which supplements the new SCCs.

(v) **Adopt necessary procedural steps:** As noted previously in this document, Autodesk has implemented technical and organizational controls to mitigate against any unauthorized disclosure of data from unauthorized third party sources. Autodesk also publishes a Transparency Report annually on its website which shows that to date Autodesk has received very few Government Access Requests.

(vi) **Re-evaluate at appropriate intervals:** Autodesk is constantly evaluating its compliance with EU data transfer requirements. In addition to the SCCs, and the BCRs we are monitoring progress on the new EU-U.S. Data Privacy Framework (see below) and plan to take the steps to participate in that when available.

EU-U.S. Data Privacy Framework

The European Commission and U.S. Government have developed a new EU-U.S. Data Privacy Framework to replace the Privacy Shield invalidated by the CJEU/ECJ in 2020.

Autodesk has self-certified and we are officially part of the new Data Privacy Framework.
The EU-U.S. DPF, UK Extension to the EU-U.S. DPF, and Swiss-U.S. DPF were respectively developed by the U.S. Department of Commerce and the European Commission, UK Government, and Swiss Federal Administration to provide U.S. organizations with reliable mechanisms for personal data transfers to the United States from the European Union, United Kingdom, and Switzerland while ensuring data protection that is consistent with EU, UK, and Swiss law.

Subprocessors

Autodesk can provide a list of all the subprocessors it uses when it acts as a processor to customers on request. Requests for our subprocessor list can be made via the contact details below. All subprocessors are subject to rigorous security and privacy checks before being onboarded by Autodesk. Once these privacy and security checks are carried out, and Autodesk has assessed the risk, the sub processor is required to enter into data protection contract terms with Autodesk.

Government Requests for Data

Autodesk products that may permit customers to process and store business data in the cloud, such as sales and spending data, and a variety of other commercial information, may technically qualify as a "Remote Computing Service", and therefore Autodesk may be considered an "Electronic Communication Service Provider" ("ECSP") under Section 702 of the Foreign Intelligence Surveillance Act ("FISA"). However, companies like Autodesk that offer ordinary commercial products or services, and whose data transfers involve ordinary commercial information like employee, customer, or sales records, have no basis to believe U.S. intelligence agencies would seek to collect that data through FISA Section 702. Executive Order 12333, also discussed in the Schrems II judgment, authorizes parts of the U.S. government to conduct certain surveillance activities, but it does not grant the U.S. government any powers to compel companies like Autodesk to assist in those efforts. Therefore, Autodesk would be under no obligation to assist the U.S. government in conducting surveillance if the government sought to rely on Executive Order 12333 to request customer data. As documented in our Transparency Report, before complying with any Government Request we will:

- Narrowly construe each request and disclose customer data only when required to do so by law.
- Review each request for valid legal process.
- Provide the same level of protection to all our customers, no matter where they are located or the origin of the request, to the extent that the governing law allows.
- Commit to maintaining customer privacy and confidentiality.
- Delay notice to our customers only (1) when legally obligated to do so such as, for example, when we receive a delayed notice order (DNO) issued by a court or (2) in the case of emergencies (e.g., regarding imminent threat to life, child sexual exploitation, terrorism).
- Notify our customers of the government request for their data after the DNO expires or the emergency exception no longer applies. Autodesk does not comply with informal requests for delayed notice or indefinite DNO's.

Storage of data

Autodesk does offer data localization for certain products. However, identity, logging, and other pertinent personal data may be stored, processed and accessed from other global locations for all global services offered by Autodesk. This includes support and maintenance, availability and reliability, certain services (for example, translation), account management, product entitlements, email, and collaboration. There are purposes for which Covered Content may need to be stored or processed on servers outside the region the customer selects; for example when users or their collaborators access our Services using a client outside the region, temporarily when using certain high-performance compute applications (such as translation services), and for logging, support, maintenance, or security purposes, or in connection with legal obligations or proceedings. Further information on the data we store in our EU Data Centers can be found on our website. As a global company, Autodesk does transfer data across national border, but has implemented appropriate safeguards as already described in this document.

Conclusion

We are committed to providing and continuing to advance technical, legal, and organizational safeguards to ensure that Autodesk can carry out cross border data transfers in a way that prevents your data from being accessed by third parties.

Contact

For all Data Protection Agreement, and Subprocessor related requests, please email autodesk.dpa@autodesk.com. For any other matter discussed in this whitepaper, please email privacy.questions@autodesk.com