Building Customer Trust Through Privacy and Security

Richard Greene Senior EU Privacy Counsel
Autodesk

Deanna Brock Senior Manager, Senior Corporate Counsel
Autodesk

Learning Objectives

- Get a baseline understanding of the latest global security and regulatory developments.
- Gain an overview of new security initiatives such as FedRAMP and C5
- Learn where to find resources and materials that describe Autodesk's Privacy and Security Practices.
- Learn about the privacy and security features of Autodesk products.

Description

The Privacy and Security framework of an organization has become increasingly important when it comes to building brand trust. This importance is being driven by increased global regulation around data privacy, and the enhanced threat faced as a result of external bad actors. In this presentation, we will explore why Trust is important to Autodesk. We'll guide participants through the latest global, regulatory, and security requirements that organizations now need to comply with. Beyond regulatory compliance, we'll look at the latest security and privacy industry-led initiatives and trends that can help build customer trust. We'll look at Autodesk's own approach to privacy and security and explain what we've done in this area to foster customer trust.

Speakers

Richard Greene, Senior EU Privacy Counsel

I have worked in the area of data privacy, and the intersection between the 'law and technology' for over a decade. I am a qualified barrister in Dublin, Ireland and have worked in a number of privacy centric roles before joining Autodesk in 2020. As part of my role in Autodesk, I advise Autodesk's internal teams on EU data protection compliance matters.

Deanna Brock, Senior Manager, Senior Corporate Counsel

I have 20 years of experience as a transactional attorney working on large complex contract negotiations on both the "buy" side and "sale" side. I am a California licensed attorney and hold a LL.M in Taxation. At Autodesk, I am responsible for the Entertainment & Media agreements, the awesome team that supports direct sales for the Americas and global procurement/sourcing.

Why is Trust Important to Autodesk

Companies such as Apple and IBM have successfully positioned their data privacy and security practices as a competitive advantage over their closest rivals. Since the EU passed their significant data protection law the GDPR in 2018 coupled with the enhanced threat from nefarious third-party actors' face means that privacy and security is now more than ever important when it comes to building trust.

Autodesk recognises that by strengthening its own privacy and security programs, it can help Autodesk foster enhanced trust with their customers, which is why the goal of building customer trust through data protection and security practices is a key strategic goal for Autodesk

Compliance with Global Data Protection Laws

Global Laws & Regulations

In 2018, the EU implemented the General Data Protection Regulation (GDPR) which placed additional compliance obligations on companies in relation to data privacy and security. Since 2018, the GDPR has become a model for other privacy and regulatory frameworks which have been subsequently passed such as Brazil's General Data Protection Law (LGPD), California's California Consumer Privacy Act (CCPA) which is to be amended again in 2023 and most significantly the China Personal Information Protection Law (PIPL) which was passed in 2021. A consequence of these emerging laws means that companies must have in place strong and robust privacy programs that ensure compliance with increasing global regulations. Now that these emerging laws are in place means that trust is now an important consideration.

In the United States, there is also a draft federal bill, the American Data Privacy & Protection Act which is the first bipartisan, bicameral federal privacy law. It remains to be seen whether this law will be passed.

This chart shows which countries have implemented comprehensive data 'GDPR type' laws:
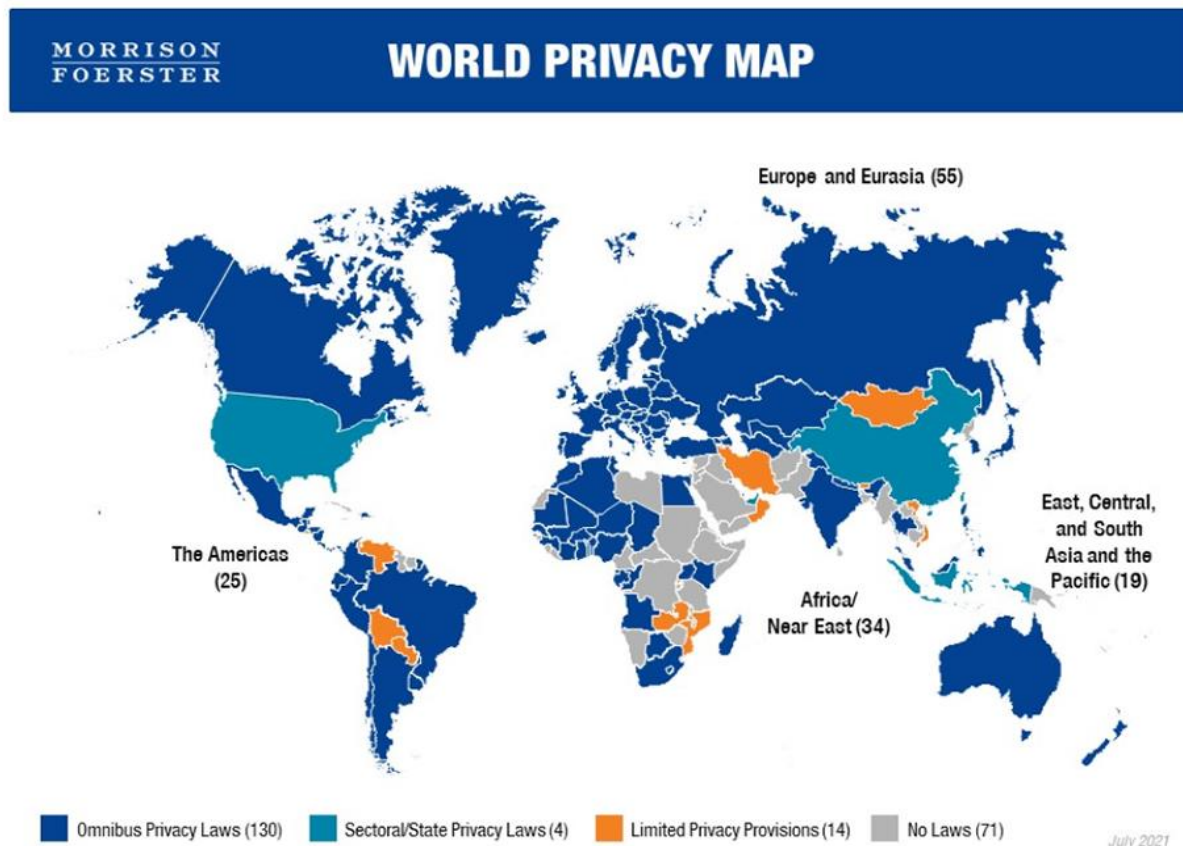
<u>Data Transfer & Data Regionalization Trends</u>

Increasingly there has been a shift globally towards data localisation. Data localisation refers to a mandatory legal or administrative requirement directly or indirectly stipulating that data be stored or processed, exclusively or non-exclusively, within a specified jurisdiction. Data Localization can be overt such as is the case with certain authoritarian regimes such as Russia. However, Data Localization can also be driven by other factors. For example, in the EU context there has been an increasing trend towards data localization as a consequence of restrictions being placed on the transfer of personal data from the European Union to the United States

Security Resiliency

In 2022, the average number of cyberattacks and data breaches increased by 15.1% from 2021. Over the next two years, the security executives polled by ThoughtLab will see a rise in attacks from social engineering and ransomware as nation-states and cybercriminals grow more sophisticated. The main causes of these attacks will come from misconfigurations, human error, poor maintenance, and unknown assets.

Autodesk understands the importance of having a robust security program which is why it pursues the latest security certifications and accreditations as outlined below.

How Autodesk is Fostering Customer Trust

In 2021, Autodesk launched the Trust Initiative with the objective of building operational excellence in data protection, platform resilience & ethical data practices.

The concept of Trust can be quite broad and includes a number of factors. However, in the context of data privacy and security, the following are common metrics of strong privacy and security programs:

- Transparency
- User Control
- Keeping Data Secure
- Accountability

We will examine these metrics in the context of Autodesk's own privacy & Security practices:

Transparency. Transparency is a fundamental principle of data privacy and relates to the information that an organisation provides to users' information around the collection, use and storage of personal data. Autodesk launched the [Trust Center](#) which it uses to communicate its privacy program to customers. Autodesk continuously updates the Trust Center and is committed to strengthening this as a one stop resource for our customers on Autodesk's privacy program which is constantly evolving in response to regulatory changes. The common features of the Trust Center include our Privacy Statement, Information on our Data Protection Agreements, and the publication of our Transparency Report which documents the number and type of law enforcement and government requests Autodesk receives annually.

User Controller. Control refers to what oversight the user has over their data. Autodesk has embedded a number of privacy options in the settings of its products which provides control to users at the individual level.

My profile and settings

Personal information

Security

Settings

Electronic — Yes

Phone calls — Set your preferences

Product privacy

The usage data we collect helps us understand how you use our products, what information you might be interested in, and what we can improve to make your engagement with Autodesk more rewarding. To learn more, see our analytics programs page and Privacy Statement.

Data Security. Keeping Data Secure is one of the most important metrics of any data program and is arguably the most crucial metric when it comes to building Trust in the modern digital economy. As noted above, the threat from non-actors is increasing year on year which means that companies need to increasingly stay ahead of cyber attackers. Autodesk endeavours to invest in data security, and has in place industry standards, and accreditations such as SSAE-16 AT 101 SOC 2 attestation ISO 27001, ISO 27017, ISO 27018 certifications. We are also pursuing other accreditations such FedRAMP which is a U.S. government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. To allow U.S Federal agencies or their commercial suppliers of design and construction services to use cloud technology on Federal projects software, vendors must go through a rigorous security authorization process. In the German context, Autodesk is also pursuing the Cloud Computing Compliance Controls Catalog (C5). C5 is an audited standard that establishes a mandatory minimum baseline for cloud security and the adoption of public cloud solutions by German government agencies and organizations that work with the government. C5 is also being increasingly adopted by the private sector.

Accountability. The final component of Trust in the context of Privacy and Security is accountability. This is one of the main principles that underpins most global privacy programs. This principle requires that organisations take a proactive and structured approach to privacy management through the implementation of appropriate and demonstrable privacy and data protection measures. Autodesk achieves this through its Privacy management program which governs the processing of information worldwide. This program is based on the principles found in the GDPR and covers the processing and the security of information across the organisation. It covers the threat of data in relation to the vendors we use, our collection of information and how we secure that information

Summary:

The concept of Trust is an evolving concept as new laws and external cyber threats increase. Autodesk is committed to continuing to build trust with customers through enhanced security and privacy protections.

Useful Links:

➢ Articles on Data Trust
- "Privacy is a Competitive Advantage" The Financial Times
- The Trust Factor And Why It's Critical For Data Privacy

➢ Articles on Global Data Protection Laws
- Global Data Laws Map from the International Association of Privacy Practitioners (IAPP)
- OECD Report on Global Data Protection Trends

➢ Autodesk Resources on Data Privacy & Security
- Autodesk Trust Center
- Autodesk's Privacy Statement
- Autodesk's Transparency Report