Building Customer Trust Through Privacy and Security

Richard Greene, Senior EU Data Protection Counsel, Autodesk

Deanna Brock, Senior Manager, Sr. Corporate Counsel, Autodesk

Safe Harbor Statement

We may make forward-looking statements regarding planned or future development efforts for our existing or new products and services and statements regarding our strategic priorities. These statements are not intended to be a promise or guarantee of business results, future availability of products, services or features but merely reflect our current plans and are based on factors currently known to us. These planned and future development efforts may change without notice. Purchasing and investment decisions should not be made based upon reliance on these statements.

A discussion of factors that may affect future results is contained in our most recent Form 10-K and Form 10-Q filings available at www.sec.gov, including descriptions of the risk factors that may impact us and the forward-looking statements made in these presentations. Autodesk assumes no obligation to update these forward-looking statements to reflect events that occur or circumstances that exist or change after the date on which they were made. If this presentation is reviewed after the date the statements are made, these statements may no longer contain current or accurate information.

This presentation also contains information, opinions and data supplied by third parties and Autodesk assumes no responsibility for the accuracy or completeness of such information, opinions or data, and shall not be liable for any decisions made based upon reliance on any such information, opinions or data.

Autodesk's partners frequently compete against each other in the marketplace, and it is critically important that all participants in this meeting observe all requirements of antitrust laws and other laws regarding unfair competition. Autodesk's long insistence upon full compliance with all legal requirements in the antitrust field has not been based solely on the desire to stay within the bounds of the law, but also on the conviction that the preservation of a free and vigorous competitive economy is essential to the welfare of our business and that of our partners, the markets they serve, and the countries in which they operate. It is against the policy of Autodesk to sponsor, encourage or tolerate any discussion or communication among any of its partners concerning past, present or future prices, pricing policies, bids, discounts, promotions, terms or conditions of sale, choice of customers, territorial markets, quotas, inventory, allocation of markets, products or services, boycotts and refusals to deal, or any proprietary or confidential information. Communication of this type should not occur, whether written, oral, formal, informal, or "off the record." All discussion at this meeting should be strictly limited to presentation topics.

PLEASE NOTE: AU content is proprietary. Do Not Copy, Post or Distribute without expressed permission.

- 'Celebgate'
- Open Letter

Agenda

- ✓ **Why trust is important**

- ✓ **Laws & Regulations: moving target**

- ✓ **Security Resiliency**

- ✓ **Why trust is important to Autodesk**

- ✓ **What Autodesk is doing to gain and maintain customer trust**
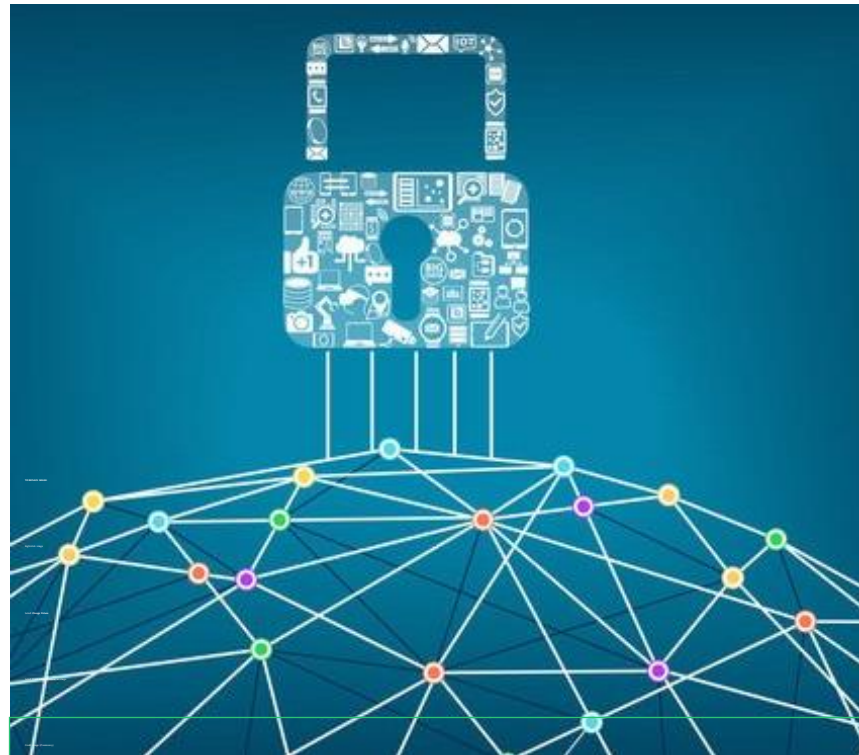
- ✓ **Q&A**

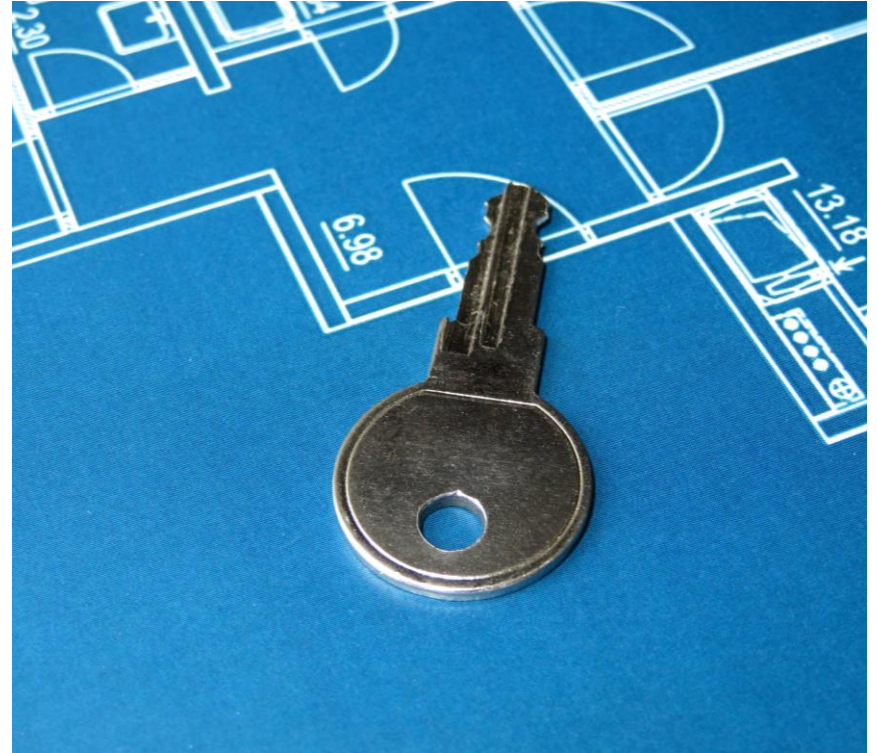# Why Trust is Important

Laws & Regulations: A Moving Target

Increased Privacy & Security Obligations for Companies

- **2018: GDPR** (EU)

- **2020: CCPA** (California)

- **2021: PIPL** (China)

- **2023: CPRA** (California)

- **TBC: ADPPA** (United States Federal Law)

- **Data Localization & Data Transfer restrictions trends** (export controls, data privacy laws, sensitive IP

Security Resiliency

- Gartner predicts by 2025, 45% of organisations will have experienced a cyber attack perpetrated by external actors

- **GAO Report of estimate of the financial loss of cyber attacks:**

  - ✓ Cost in 2016 ($470 million)

  - ✓ Cost in 2021 ($2.6 Billion)

- **Loss of IP and confidential Data**

- **Damage to brand reputation**

- **Threat to National Security**

Why Trust is Important to Autodesk

Autodesk's Data Trust Journey

| 1982 | 2012 | 2018 | 2021 |

AutoCAD

✓ Computer-aided design software

✓ Radically disrupted the design industry

Autodesk 360

✓ Autodesk moves to the cloud

✓ Additional Security & Privacy Controls
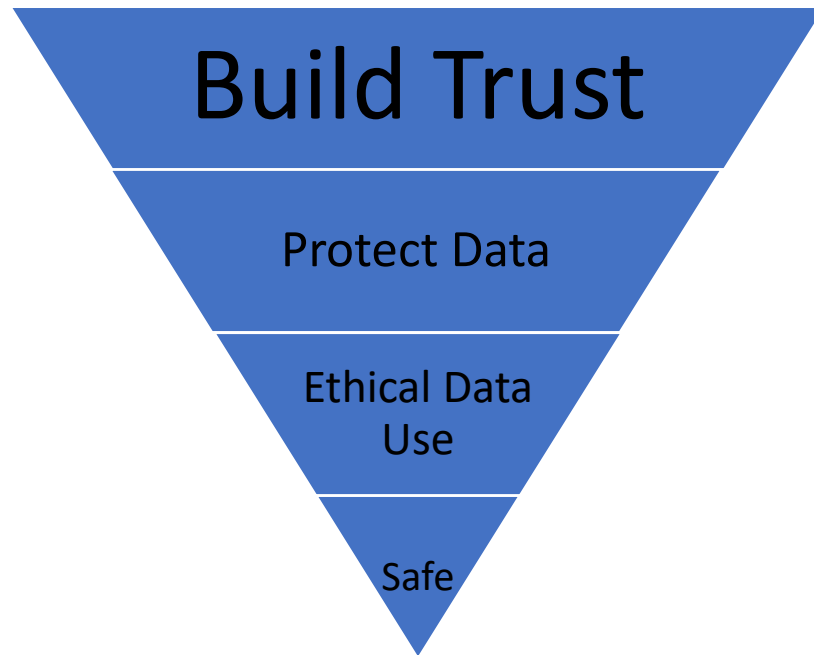
The GDPR

✓ Monumental compliance shift

Autodesk Trust Initiative

✓ Launched in 2021

Autodesk 2021 Strategic Objective:

"Build operational excellence in data protection, platform resilience & ethical data practices"

- Ben Cochran, VP Developer Enablement

Build Trust

Protect Data

Ethical Data Use

Safe

Building Customer Trust

Legal & Industry Led initiatives

- Security certifications

- Robust supplier onboarding and vendor management programs

- Company policies

What Autodesk is Doing to Gain/Maintain Customer Trust

Trust Building Blocks

- **Transparency**

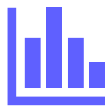- **User Control**

- **Keeping Data Secure**

- **Accountability**

Transparency

Leveraging the Trust Center

Privacy Statement

Transparency Report

External ISO/SOC II Associations (ISO 27001 cert)

Privacy & security settings are embedded into our products

Incident Reporting Information

TRUST CENTER   OVERVIEW   SECURITY   INCIDENT RESPONSE   PRIVACY   COMPLIANCE   AVAILABILITY   ADVISORIES   CONTACT US

Our security framework

The Autodesk Security framework was designed around industry standards to ensure consistent security practices, enabling us to build secure, run secure, and stay secure.

Build secure

Embedding security into our products is a critical part of securing our customers' investment in Autodesk products and services.

We build security into our products and services from the ground up. We integrate security activities into all phases of the development effort to ensure issues are identified and corrected early and throughout the build process.

Run secure

Securing our infrastructure is another critical way that we protect the

Stay secure

Gaining visibility into our environment offers us valuable insight into persistent suspicious activity, active security incidents, and ongoing exploits impacting Autodesk and our customers.

We take proactive steps to defend against these threats with the appropriate incident response. We work closely with all teams and personnel involved in a given situation to ensure that an appropriate response is managed for the issue.

User Control

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.

Desktop products

Desktop products

☑ **Help develop our products and services**
Allows us to optimize performance and quality based on usage patterns, and provide new and improved offerings.

☑ **Customize our messaging**
Allows us to create customized offers and promotional content for you based on your usage.

Save

Cancel

‹ UNIVERSITY

Keeping Data Secure

Autodesk adheres to the industry standards and latest practices

Accountability

- Autodesk Trust Center

- Contractual commitments with Customers

- Internal security and data privacy standard our product teams are held to

- Risk-based supplier onboarding and ongoing due diligence including systematic tracking of suppliers that have access to customer information

Privacy by Design (PBD)　　Transparency & Choice　　Vendor Management　　Encryption　　Data Lifecycle Management

Continuing to Build Trust

- Autodesk continues to invest in programs that builds trust

- A journey not a destination