



Privacy, Trust, and the General Data Protection Regulation (GDPR)

JP Clementi, Microsoft: Azure Global Privacy

"Businesses and users are going to embrace technology only if they can trust it."

Satya Nadella
Chief Executive Officer
Microsoft Corporation



- We take a principled approach with strong commitments to privacy, security, compliance and transparency.
- Moving to the cloud makes it easier for you to become compliant with privacy regulations by managing and protecting personal data in a centralized location.
- Microsoft is the industry leader in privacy and security with extensive expertise complying with complex regulations.

Overview

Privacy - Microsoft understands that when you, our customer, use our business cloud services, you are entrusting us with your most valuable asset—your data. You trust that its privacy will be protected and that it will be used only in a way that is consistent with your expectations.

General Data Protection Regulation (GDPR) - imposes new rules on organizations in the European Union (EU) and those that offer goods and services to people in the EU, or that collect and analyze data tied to EU residents, no matter where those organizations are located

- **Enhanced** personal privacy rights
- **Increased** duty for protecting data
- **Mandatory** breach reporting
- **Significant** penalties for noncompliance



General Data Protection Regulation

Art. 15 Right of access by the data subject	Art. 16 Right of rectification	Art. 17 Right to erasure (right to be forgotten)	Art. 18 Right to restriction of processing
Art. 20 Right to data portability	Art. 25 Data protection by design and by default	Art. 30 Records of processing activities	Art. 32 Security of processing
Art. 33 Notification of a personal data breach to the supervisory authority	Art. 35 Data protection impact assessment	Art. 46 Transfers subject to appropriate safeguards	Art. 84 Penalties






People

Process

Technology


What key changes result from the GDPR?



Data Subject Rights

Individuals have the right to:


- Access their personal data
- Correct errors in their personal data
- Erase their personal data
- Object to processing of their personal data
- Export personal data



Controls and notifications

Organizations are required to:


- Protect personal data by implementing appropriate security
- Notify authorities of personal data breaches
- Obtain appropriate consent for processing data
- Keep records detailing data processing



Transparent policies

Organizations are required to:

- Provide clear notice of data collection
- Outline processing purposes and use cases
- Define data retention and deletion policies




IT and training

Organizations are required to:


- Train privacy personnel and employees
- Audit and update data policies
- Employ a Data Protection Officer (if required)
- Create and manage compliant vendor contracts

Microsoft Confidential – for internal only use by partners.

GDPR is.....

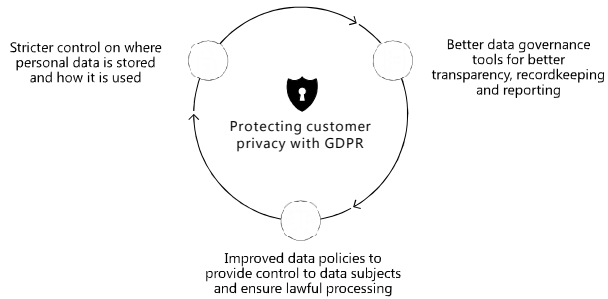


Privacy by Design



Security by Design

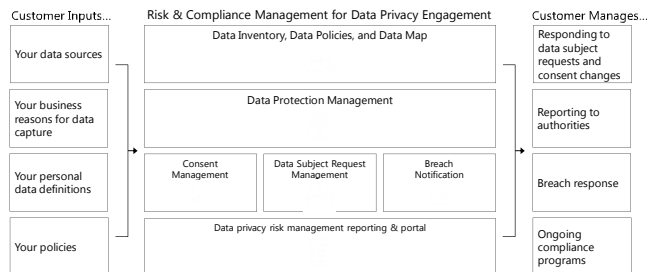
What does this mean for my data?

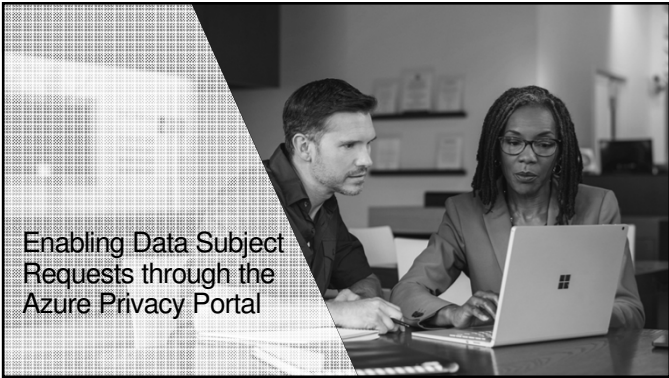


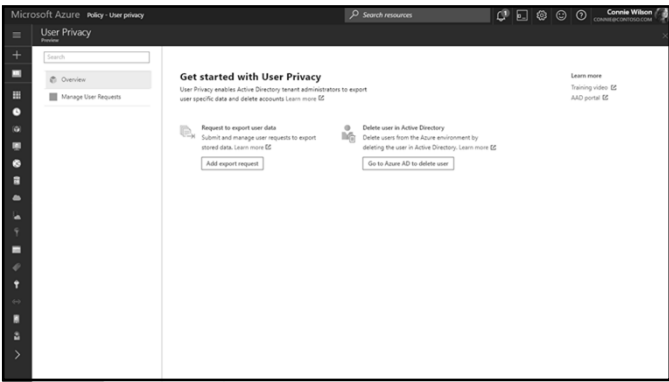
Our commitment to you

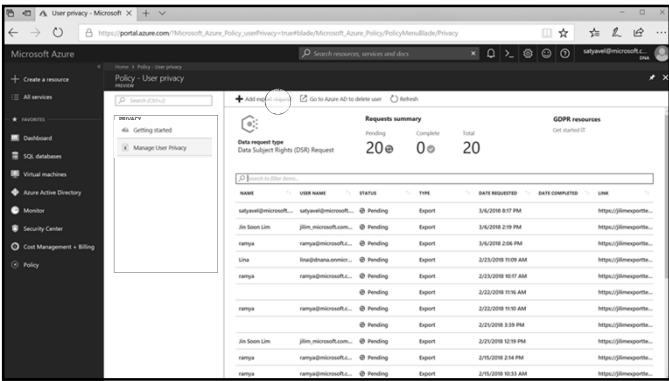
- ✓ To simplify your path to compliance, we are GDPR compliance ready across our cloud services beginning on May 25, 2018.
- ✓ We will share our experience in complying with complex regulations such as the GDPR.
- ✓ Together with our partners, we are prepared to help you meet your policy, people, process, and technology goals on your journey to GDPR.

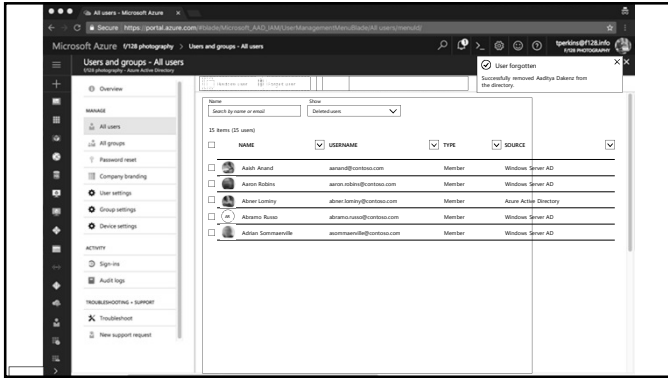
GDPR Overview











Trusted Platform

Built-in compliance and security to manage and control access to personal data

Transparency & Privacy

Data Residency

Operational Security

Breach Notification

Transparency - Compliance Manager

- View your compliance posture against evolving regulations in real-time.
- Take recommended actions to improve your data protection capabilities.
- Conduct pre-audits to prepare for external audits.

Compliance Manager is a dashboard that provides a summary of your data protection and compliance posture and recommendations to improve data protection and compliance. This is a recommendation, it is up to you to evaluate its effectiveness in your regulatory environment prior to implementation. Recommendations from Compliance Manager should not be interpreted as a guarantee of compliance.

Azure covers 79 compliance offerings

Global	<input checked="" type="checkbox"/> ISO 27001:2013	<input checked="" type="checkbox"/> ISO 9001:2015	<input checked="" type="checkbox"/> CDS Benchmark	<input checked="" type="checkbox"/> CSA STAR Self-Assessment
	<input checked="" type="checkbox"/> ISO 27017:2015	<input checked="" type="checkbox"/> ISO 20000-1:2011	<input checked="" type="checkbox"/> CSA STAR Certification	<input checked="" type="checkbox"/> WCAG 2.0 (ISO 40500:2012)
	<input checked="" type="checkbox"/> ISO 27018:2014	<input checked="" type="checkbox"/> SOC 1 Type 2	<input checked="" type="checkbox"/> CSA STAR Certification	
	<input checked="" type="checkbox"/> ISO 22301:2012	<input checked="" type="checkbox"/> SOC 2 Type 2	<input checked="" type="checkbox"/> CSA STAR Attestation	
U.S. Government	<input checked="" type="checkbox"/> FedRAMP High	<input checked="" type="checkbox"/> DoD DISA SRG Level 4	<input checked="" type="checkbox"/> NIST SP 800-171	<input checked="" type="checkbox"/> ITAR
	<input checked="" type="checkbox"/> FedRAMP Moderate	<input checked="" type="checkbox"/> DoD DISA SRG Level 2	<input checked="" type="checkbox"/> NIST CSF	<input checked="" type="checkbox"/> CDS
	<input checked="" type="checkbox"/> EAR	<input checked="" type="checkbox"/> DFARS	<input checked="" type="checkbox"/> Section 508 VPATs	<input checked="" type="checkbox"/> IRS 1075
	<input checked="" type="checkbox"/> DoD DISA SRG Level 5	<input checked="" type="checkbox"/> DoE 10 CFR Part 810	<input checked="" type="checkbox"/> FIPS 140-2	
Industry	<input checked="" type="checkbox"/> PCI DSS Level 1	<input checked="" type="checkbox"/> FCA + PRA (UK)	<input checked="" type="checkbox"/> HIPAA BAA	<input checked="" type="checkbox"/> CDSA
	<input checked="" type="checkbox"/> GLBA	<input checked="" type="checkbox"/> MAS + ABS (SG)	<input checked="" type="checkbox"/> HITECH	<input checked="" type="checkbox"/> MPAA
	<input checked="" type="checkbox"/> FFIEC	<input checked="" type="checkbox"/> 23 NYCRR 500	<input checked="" type="checkbox"/> 21 CFR Part 11 (GxP)	<input checked="" type="checkbox"/> DPP (UK)
	<input checked="" type="checkbox"/> Shared Assessments	<input checked="" type="checkbox"/> SEC 17a-4	<input checked="" type="checkbox"/> MARS-E	<input checked="" type="checkbox"/> FACT (UK)
Regional	<input checked="" type="checkbox"/> TSC (JP)	<input checked="" type="checkbox"/> CTC 1.31	<input checked="" type="checkbox"/> NHS IG Toolkit (UK)	
	<input checked="" type="checkbox"/> APRA (AU)	<input checked="" type="checkbox"/> 2FINRA 4511	<input checked="" type="checkbox"/> NEN 7510:2011 (NL)	
	<input checked="" type="checkbox"/> OSFI (CA)	<input checked="" type="checkbox"/> SOX	<input checked="" type="checkbox"/> FERPA	
	<input checked="" type="checkbox"/> Argentina PDPA	<input checked="" type="checkbox"/> EN 301 549	<input checked="" type="checkbox"/> India MeitY	<input checked="" type="checkbox"/> Spain DPA
	<input checked="" type="checkbox"/> Australia BRAP Unclassified	<input checked="" type="checkbox"/> EU ENSA IAF	<input checked="" type="checkbox"/> Japan CS Mark Gold	<input checked="" type="checkbox"/> UK Cyber Essentials Plus
	<input checked="" type="checkbox"/> Australia BRAP Protected	<input checked="" type="checkbox"/> EU Model Clauses	<input checked="" type="checkbox"/> Japan My Number Act	<input checked="" type="checkbox"/> UK G-Cloud
	<input checked="" type="checkbox"/> Canada Privacy Laws	<input checked="" type="checkbox"/> EU - US Privacy Shield	<input checked="" type="checkbox"/> Netherlands BBR 2012	<input checked="" type="checkbox"/> UK PASP
	<input checked="" type="checkbox"/> China GB 18030:2010	<input checked="" type="checkbox"/> GDPR	<input checked="" type="checkbox"/> New Zealand Gov CIO Fwk	
	<input checked="" type="checkbox"/> China DICI (MLPS) Level 3	<input checked="" type="checkbox"/> Germany CS	<input checked="" type="checkbox"/> Singapore MTCS Level 3	
	<input checked="" type="checkbox"/> China TRUCS / CCCPP	<input checked="" type="checkbox"/> Germany IT-Grundschutz	<input checked="" type="checkbox"/> Spain ENS	

Resources

- ☒ Azure sales guide, playbook, and customizable presentation for GDPR
<https://aka.ms/GDPR-Partners>
- ☒ GDPR on the Microsoft Trust Center
<https://microsoft.com/gdpr>
- ☒ Compliance Manager
<https://aka.ms/compliancemanager>
- ☒ Azure Blueprints
<https://aka.ms/Azure-Blueprints>



Thank you!