Microsoft

#AzureEvent
#BuildWithAzure

Azure Workshop

GDPR, Security and Privacy features for cloud applications

Ben Roscorla, Mike Ormond, Robin Lester

vipazure@microsoft.com

The security imperative

Security Imperative | Securing Investment | Securing Infrastructure | Securing Data | Securing Applications | Monitoring & Ops

What imperative?

- ❑ Proliferation of bad actors
- ❑ Increasingly sophisticated threats
- ❑ Increasingly diverse users
- ❑ Dynamic cloud environment
- ❑ Compliance and legislation

- ❑ Financial & Reputation Risk

Sobering statistics

200+

The average number of days that attackers reside within a victim's network before detection

75%

of all network intrusions are due to compromised user credentials

£350B

The total potential cost of cybercrime to the global economy

£2.4M

The average cost of a data breach to a company

The frequency and sophistication of cybersecurity attacks are getting worse.

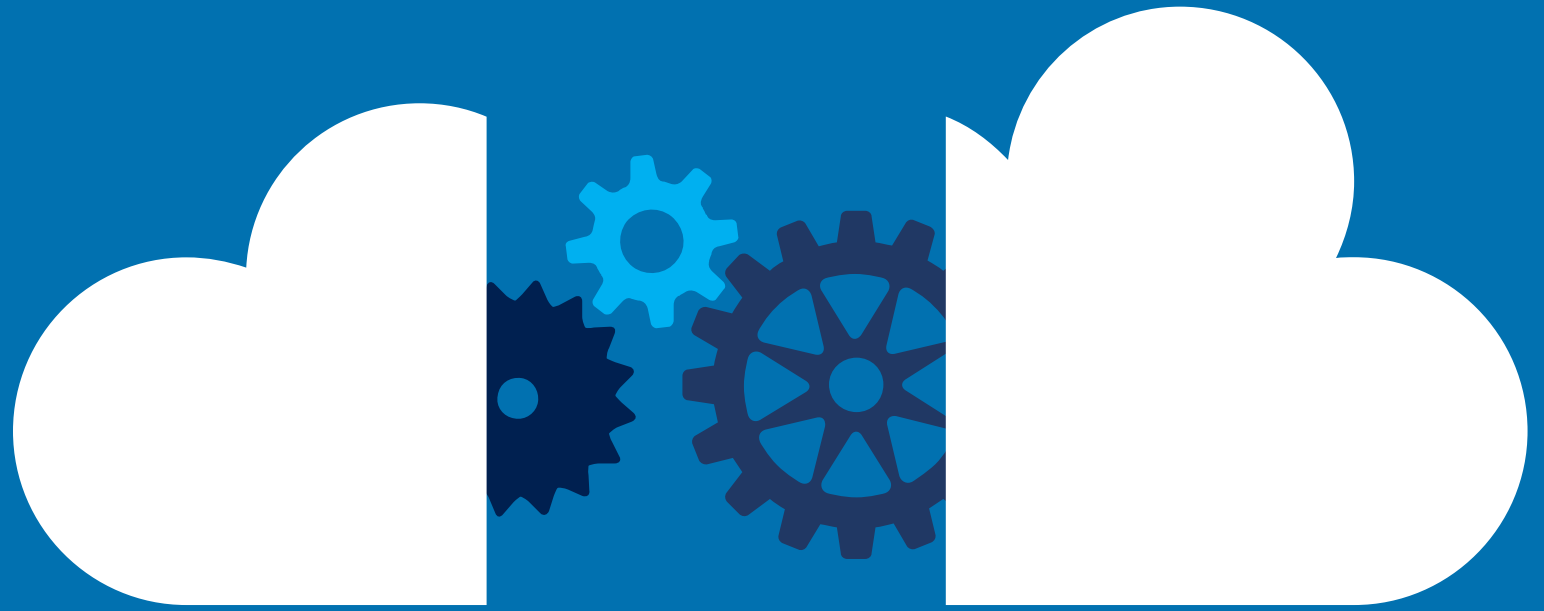
Security Imperative | Securing Investment | Securing Infrastructure | Securing Data | Securing Applications | Monitoring & Ops

What imperative?

- The cloud can be harnessed to defend against threats
- Massive investment in cloud security
- Cloud security is a shared responsibility

Demo

I’m under attack



The Microsoft Cloud -A Cloud You Can Trust

Security

The confidentiality, integrity, and availability of your data is protected.

Privacy & Control

No one is able to use your data in a way that you do not approve.

Compliance

You have visibility into how your data is being handled and used.

Transparency

Your content is stored and managed in compliance with applicable laws, regulations and standards.

https://azure.microsoft.com/en-gb/support/trust-center/

Security Imperative | Securing Investment | Securing Infrastructure | Securing Data | Securing Applications | Monitoring & Ops

Investing in your security

You have a right to expect:

- Your content should be safeguarded using state-of-the industry security technology and processes.
- Your content should be encrypted in transit and at rest.

What we're doing about it:

- Our datacenters are equipped with state-of-the-art physical security measures.
- We operate a 24x7 incident response team to mitigate threats and attacks.
- We encrypt data between you and our data centers.
- We protect your stored data with built-in tools and provide access to further encryption capabilities.

Securing the Platform – How we do it

Security Development Lifecycle (SDL)

- ✓ Security Embedded in Planning, Design, Development, & Deployment

Infrastructure security controls

- ✓ Datacenter Security
- ✓ Secure Multi-tenancy
- ✓ Network Protection
- ✓ DDoS Defense
- ✓ Data Segregation
- ✓ Data Protection

Operational security controls

- ✓ Prevent & Assume Breach Strategy
- ✓ Incident Response
- ✓ Access Policy & Controls
- ✓ Threat Detection
- ✓ Forensics

Compliance

- ✓ Strategy
- ✓ Certifications

Security Imperative | Securing Investment | Securing Infrastructure | Securing Data | Securing Applications | Monitoring & Ops

Protecting your data privacy

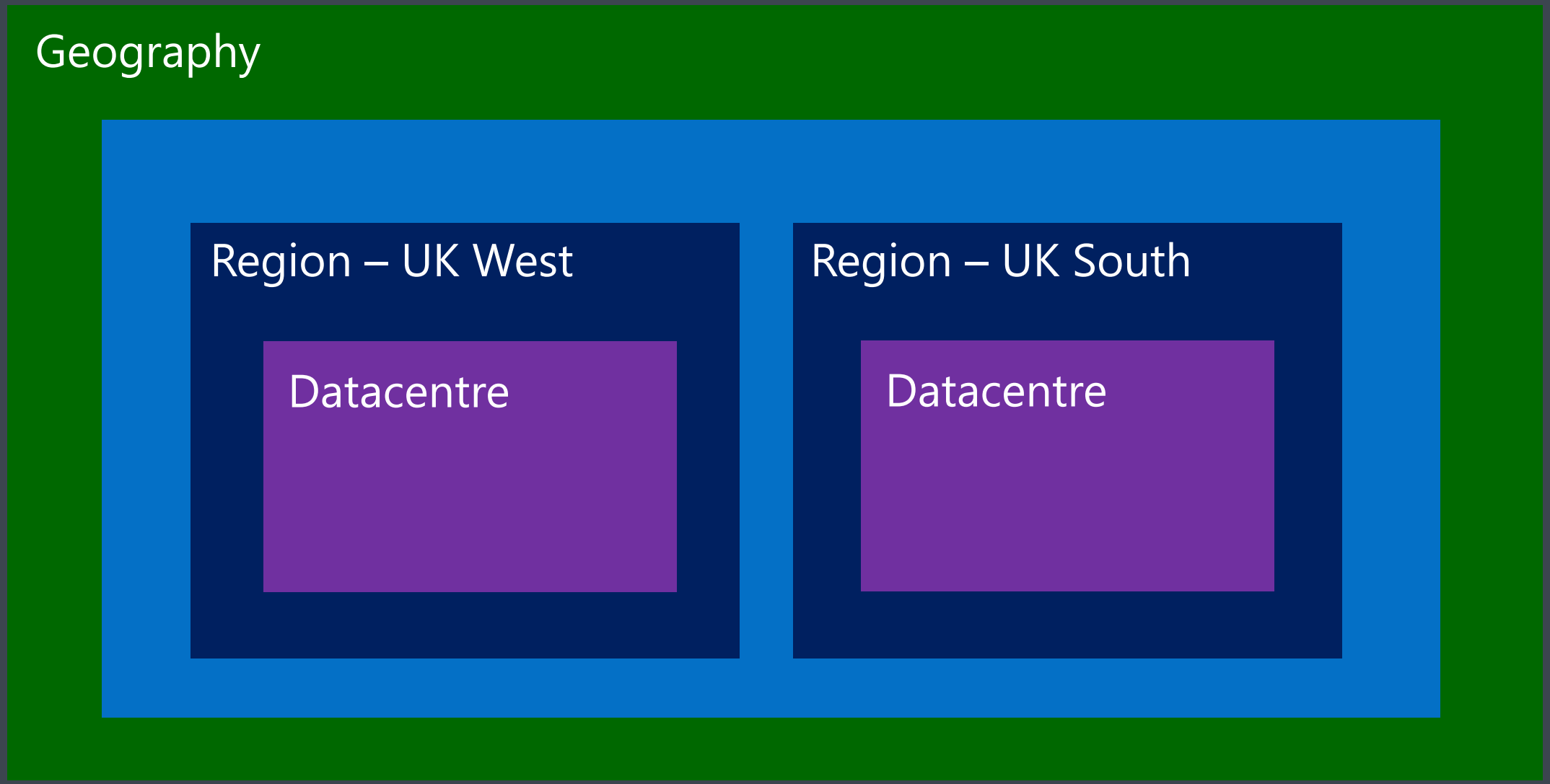
You have a right to expect:

- Your content should only be accessed as permitted by you, and should not be shared with third parties unless permitted by you.
- You should always have access to your content, and should be able to delete it or take it with you if you leave.

What we're doing about it:

- We allow you to keep the data you upload in the region you specify.
- We will not use your data for advertising or commercial purposes.
- We will not disclose your information outside of Microsoft except with your consent or when required by law.
- We provide a variety of tools to extract your data.
- Azure will fully delete your data within 180 days after expiration or termination.

UK Datacenters



Enabling your compliance

You have a right to expect:

- Your content should be stored and managed in compliance with applicable laws, regulations and key international standards
- You should have the ability to see the certifications for each Microsoft service.

What we're doing about it:

- We lead the industry in meeting the latest standards for data privacy and security, such as ISO 27018.
- We regularly undergo independent audits to certify our compliance.
- We achieved Pan Government Accreditation and meet the 14 Cloud Security Principles for HMG.
- O365 received ISB 1596 compliance.
- We enable our customers to be PSN compliant

Azure covers 62 compliance offerings

Azure has the deepest and most comprehensive compliance coverage in the industry

Global

- ☑ ISO 27001:2013
- ☑ ISO 27017:2015
- ☑ ISO 27018:2014
- ☑ ISO 22301:2012
- ☑ ISO 9001:2015
- ☑ ISO 20000-1:2011
- ☑ SOC 1 Type 2
- ☑ SOC 2 Type 2
- ☑ SOC 3
- ☑ CSA STAR Certification
- ☑ CSA STAR Attestation
- ☑ CSA STAR Self-Assessment

US Gov

- ☑ FedRAMP High
- ☑ FedRAMP Moderate
- ☑ DoD DISA SRG Level 5
- ☑ DoD DISA SRG Level 4
- ☑ DoD DISA SRG Level 2
- ☑ DFARS
- ☑ DoE 10 CFR Part 810
- ☑ NIST SP 800-171
- ☑ NIST CSF
- ☑ Section 508 VPATs
- ☑ FIPS 140-2
- ☑ ITAR
- ☑ CJIS
- ☑ IRS 1075

Industry

- ☑ PCI DSS Level 1
- ☑ GLBA
- ☑ FFIEC
- ☑ Shared Assessments
- ☑ FISC (Japan)
- ☑ HIPAA BAA
- ☑ HITRUST
- ☑ 21 CFR Part 11 (GxP)
- ☑ MARS-E
- ☑ IG Toolkit (UK)
- ☑ NEN 7510:2011 (Netherlands)
- ☑ FERPA
- ☑ CDSA
- ☑ MPAA
- ☑ FACT (UK)

Regional

- ☑ Argentina PDPA
- ☑ Australia CCSL / IRAP
- ☑ Canada Privacy Laws
- ☑ China GB 18030:2005
- ☑ China DJCP (MLPS) Level 3
- ☑ China TRUCS / CCCPPF
- ☑ EU ENISA IAF
- ☑ EU Model Clauses
- ☑ EU – US Privacy Shield
- ☑ Germany C5
- ☑ Germany IT-Grundschutz workbook
- ☑ India MeitY
- ☑ Japan CS Mark Gold
- ☑ Japan My Number Act
- ☑ Netherlands BIR 2012
- ☑ New Zealand Gov CIO Fwk
- ☑ Singapore MTCS Level 3
- ☑ Spain ENS
- ☑ Spain DPA
- ☑ UK G-Cloud
- ☑ UK Cyber Essentials Plus

Maintaining transparency

You have a right to expect:

- You should have a clear, plain-language explanation of how your cloud provider uses, manages and protects your organization's content.
- You should be told how your cloud provider will respond to law enforcement requests to access your organization's content.

What we're doing about it:

- We provide understandable and strict policy of what we will—and will NOT—use your content for.
- When responding to law enforcement requests, we strive to defend your rights and privacy, and ensure due process is followed.
- For each of our services, we provide you with information on where your content may be stored and processed.

Compliance and legislation

- Payment Industry - PCI DSS
- National Cyber Security Centre - Cloud Security Principles
- Legislative Requirement - GDPR

PCI DSS

Build and Maintain a Secure Network and Systems

1. Install and maintain a firewall configuration to protect cardholder data

2. Do not use vendor-supplied defaults for system passwords and other security parameter

Protect Cardholder Data

3. Protect stored cardholder data

4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Protect all systems against malware and regularly update anti-virus software or programs

6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need to know

8. Identify and authenticate access to system components

9. Restrict physical access to cardholder data

Regularly monitor and test networks

10. Track and monitor all access to network resources and cardholder data

11. Regularly test security systems and processes

Maintain an Information Security Policy

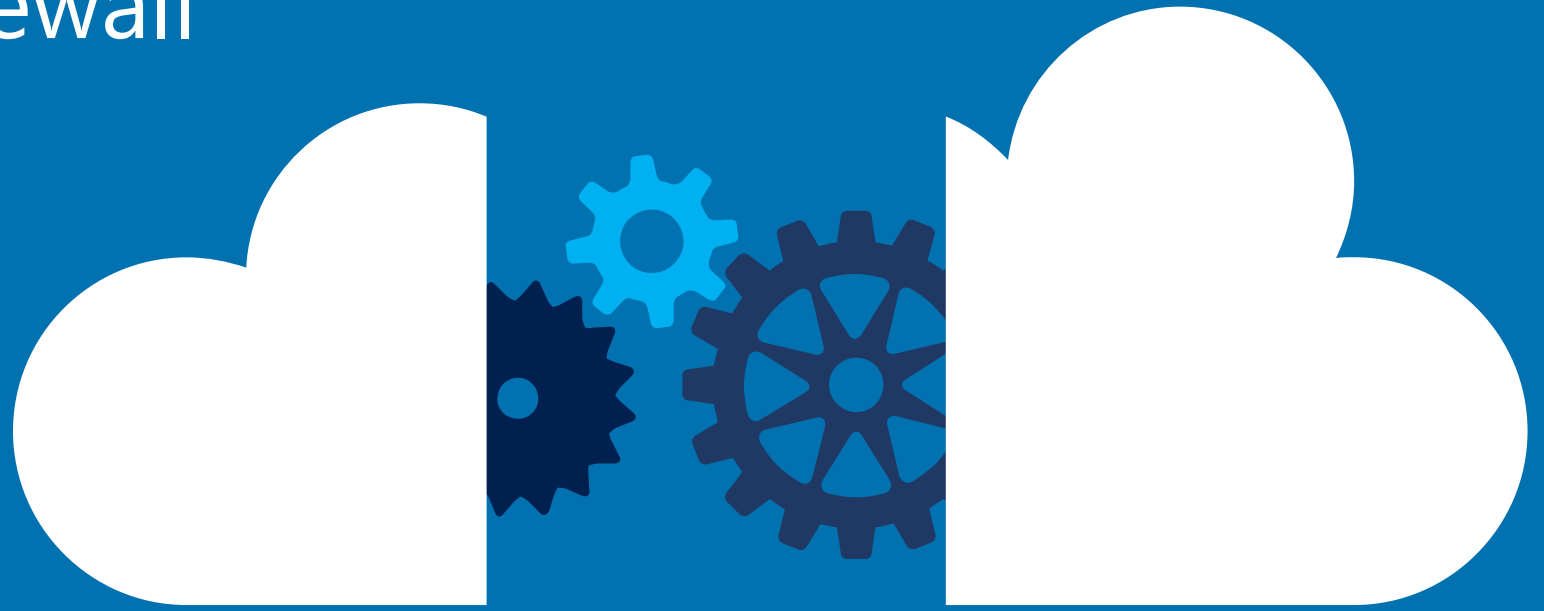
12. Maintain a policy that addresses information security for all personnel

Cloud Security Principles

1. Data in transit protection
2. Asset protection and resilience
3. Separation between users
4. Governance framework
5. Operational security
6. Personnel security
7. Secure development
8. Supply chain security
9. Secure user management
10. Identity and authentication
11. External interface protection
12. Secure service administration
13. Audit information for users
14. Secure use of the service

Demo

Web Application Firewall



Providing clarity and consistency for the protection of personal data

The **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 they are located.

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

Microsoft believes the GDPR is an important step forward for clarifying and enabling individual privacy rights

What are the key changes to address the GDPR?

Personal privacy

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 will need to:

- Protect personal data using appropriate security
- Notify authorities of personal data breaches
- Obtain appropriate consents for processing data
- Keep records detailing data processing

Transparent policies

Organizations required to:

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

IT and training

Organizations will need to:

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

Security Imperative | Securing Investment | Securing Infrastructure | Securing Data | Securing Applications | Monitoring & Ops

How do I get started?

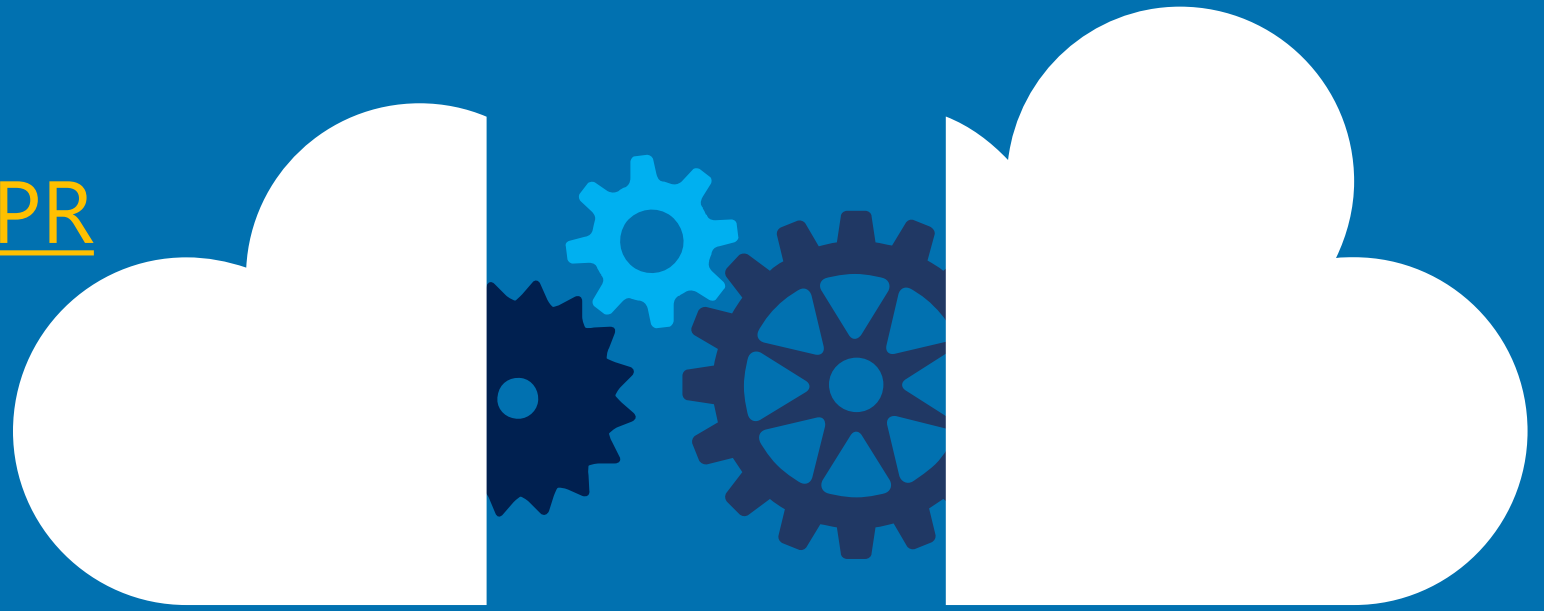
1. **Discover** — Identify what personal data you have and where it resides
2. **Manage** — Govern how personal data is used and accessed
3. **Protect** — Establish security controls to prevent, detect, and respond to vulnerabilities & data breaches
4. **Report** — Keep required documentation, manage data requests and breach notifications

Demo

GDPR Resources

Trust Center – GDPR

Partner Network - GDPR



Azure - GDPR Product Mapping

Discover Which type of data , Where data resides	Manage Access Control , Privacy by Design	Protect Data Security at rest and in transit	Report Documentation, Breach Response
Azure Security Center provides you with visibility and control over the security of your Azure resources. It continuously monitors your resources, provides helpful security recommendations, and helps you prevent, detect, and respond to threats. Azure Security Center's embedded advanced analytics help you identify attacks that might otherwise go undetected.			
Azure Data Catalog Discover, understand, and consume data from different sources and databases.	**Azure AD RBAC & Dynamic groups** Grant access to appropriate content for appropriate personnel. Revoke access instantly	**Azure Key Vault** Securely store and access secrets using hardware security modules to streamline key management.	**Log Analytics** Azure provides configurable security auditing and logging options that can help you identify and repair gaps in your security policies to prevent breaches
Log Analytics Log Analytics helps you collect and analyze data generated by resources in either your cloud or on-premises environments. It provides real-time insights using integrated search and custom dashboards to readily analyze millions of records across all workloads and servers regardless of their physical location.	**AAD Privileged identity management** Grant admin access for selective persons for specific amount of time	**Data Encryption in Azure Storage** Automatically encrypt your data when it is written to Azure Storage using Storage Service Encryption. Additionally, you can use Azure Disk Encryption to encrypt operating systems and data disks used by virtual machines, also in transit	**Azure AD Advanced Reports** Sign-in attempts , Sign-in locations , application access logging, account maintenance logging
Azure AD Application Catalog Discover and maintain What type of applications users are accessing , cloud or LOB	**Azure Information Protection** Enforcing access control policies on mails and documents	**Azure MFA** Add another layer of authentication to ensure securing identities, works with SaaS, LOB or on-premise apps	**Azure Information Protection** Reporting on documents consumption anywhere around the world
Azure Information Protection Identify information types using automatic classification capabilities		**Azure Identity Protection** Advanced risk based identity protection with alerts, analysis, & remediation.	
		Azure Information Protection Encrypted sensitive data across you environment from unwarranted access or use, at rest and in transit	

Security Imperative | Securing Investment | Securing Infrastructure | Securing Data | Securing Applications | Monitoring & Ops

Resources

Microsoft Trust Center
Compliance Offerings
Trust Center – GDPR
Partner Network - GDPR