

GDPR and the Cloud

Jennifer Koo
Corporate, External and Legal Affairs



Agenda



A Primer



Processor Obligations



Partnering with your
Cloud Provider

GDPR – a primer

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 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 will need to:

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

What does this mean for my data?





25 May 2018

Cloud – a primer

Fourth industrial revolution

**All powered
by the cloud**



Preparing for the GDPR



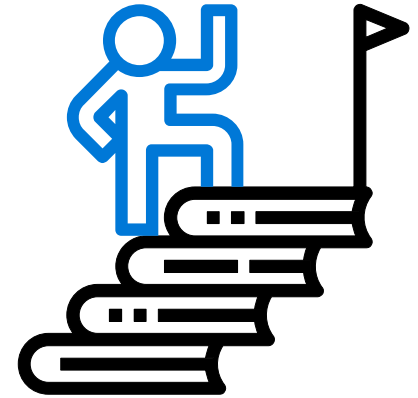
Simplify your privacy journey

Elevate your privacy practices with our cloud



Uncover risk & take action

Use our solutions to expose areas of risk and respond with agility and confidence



Leverage guidance from experts

Use our partner network to help you meet your privacy, security, and compliance goals

What is the Cloud?

Characteristics of cloud computing

On-demand self service

Delivers capacity in seconds or minutes through a specialized web interface

Broad network access

Supports many devices such as mobile phones, tablets, laptops, and workstations

Resource pooling

Provides immediate access to thousands, and potentially hundreds of thousands, of servers

Rapid elasticity

Allows you to effect changes immediately to save money with two scenarios:
Outside in: Threshold-based scaling (up and down) with limits
Inside out: API-based scaling (up and down) with limits

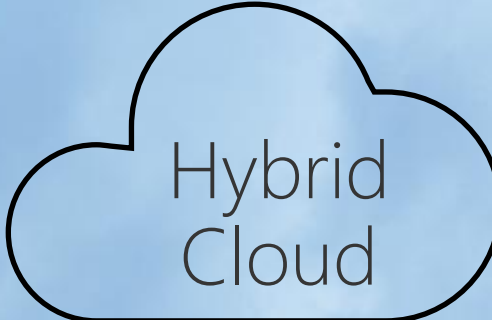
Measured service

Provides you with the means to improve CPU utilization and save money with pay by the minute, which improves operational metrics and cost accounting

Cloud deployment options

A black outline of a cloud shape containing the text "Private Cloud".

Private
Cloud

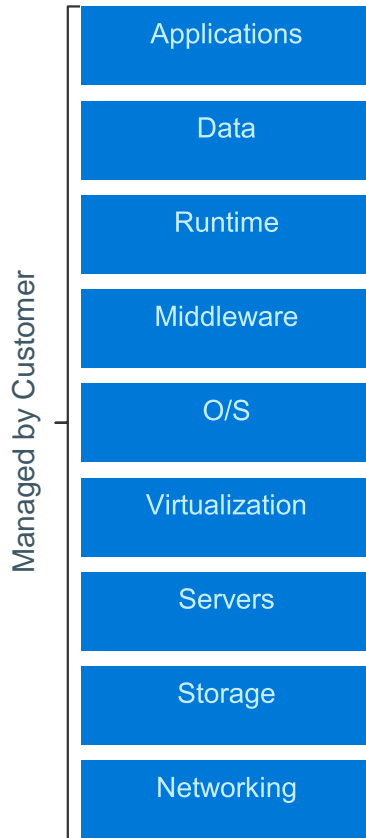
A black outline of a cloud shape containing the text "Hybrid Cloud".

Hybrid
Cloud

A black outline of a cloud shape containing the text "Public Cloud".

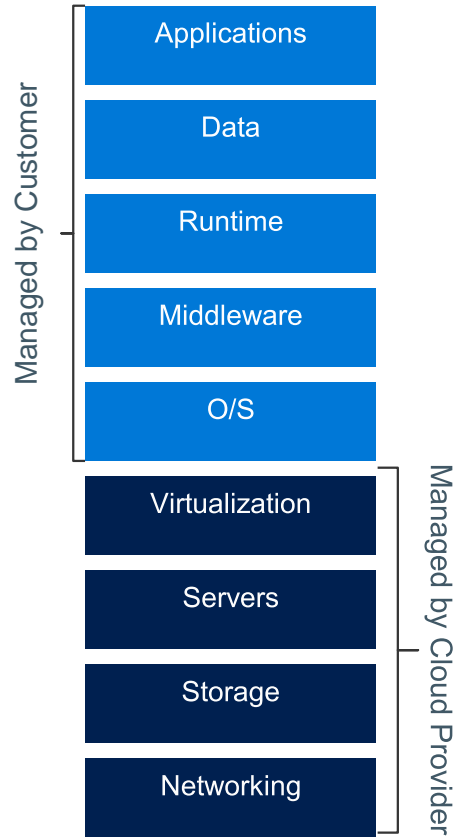
Public
Cloud

On Premises



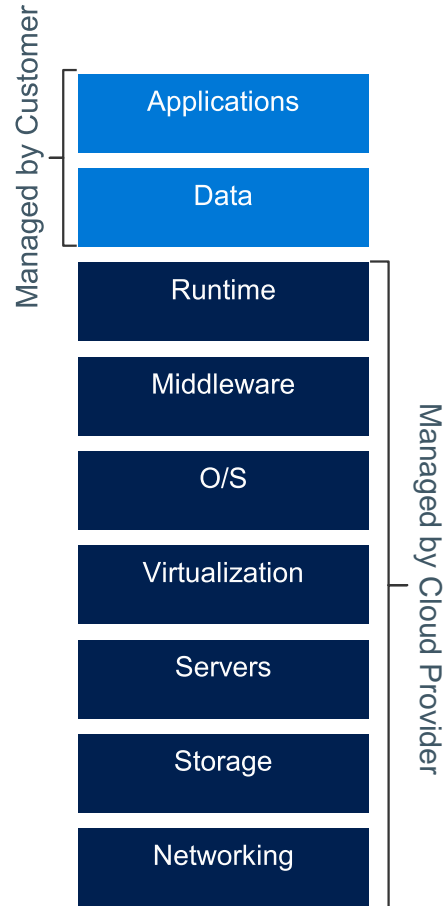
e.g. Windows Server

Infrastructure (as a Service)



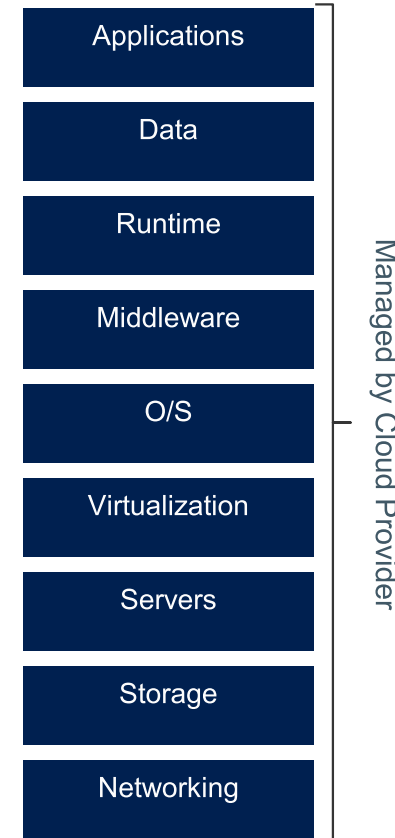
e.g. Microsoft Azure

Platform (as a Service)



e.g. Microsoft Azure

Software (as a Service)



e.g. Office 365

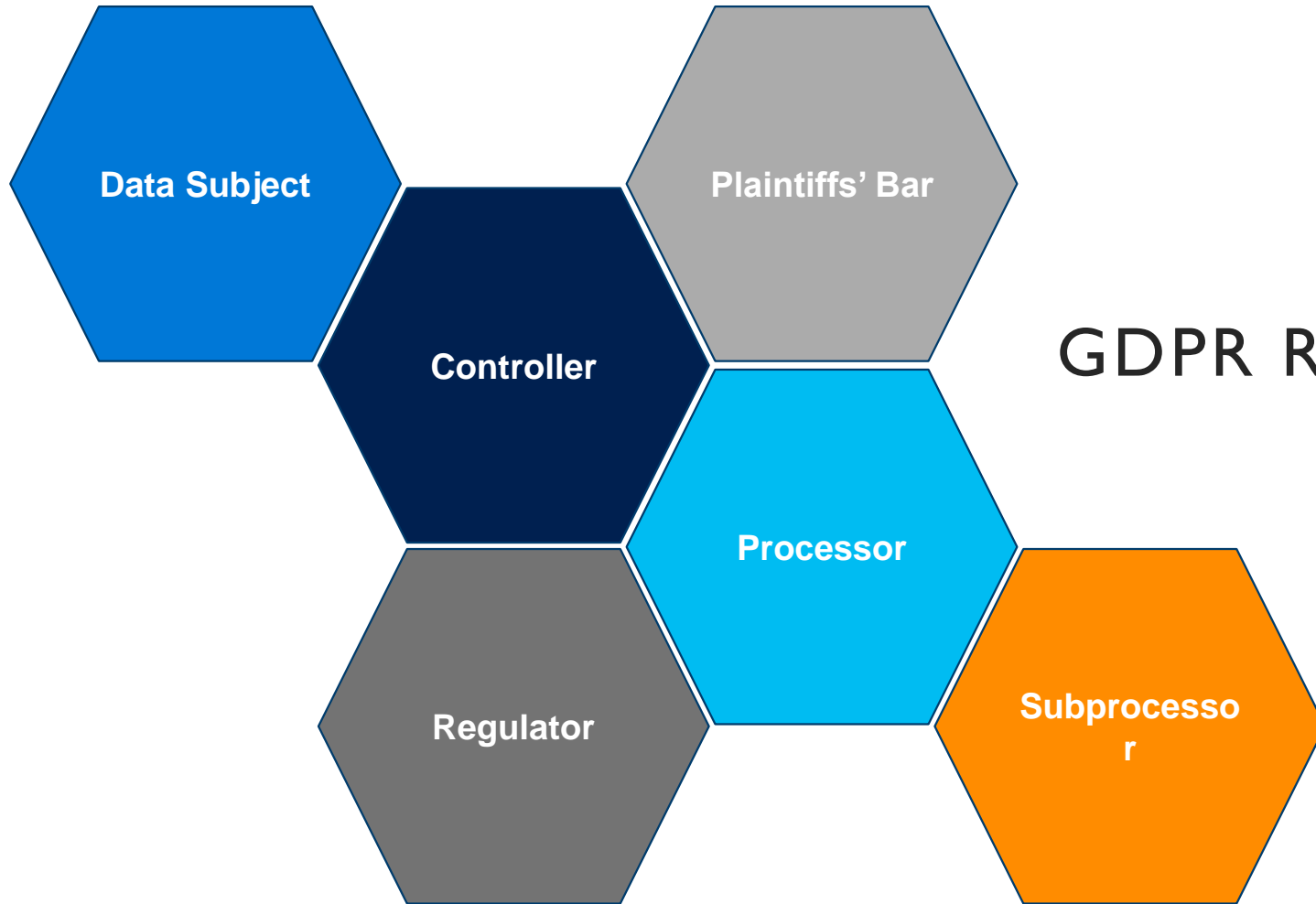
Freeing you up to work on the important things

Traditional on-premises	Infrastructure as a Service	Platform as a Service	Software as a Service
DRINKS	DRINKS	DRINKS	DRINKS
DINNER	DINNER	DINNER	DINNER
CLEANING	CLEANING	CLEANING	CLEANING
BREAKFAST	BREAKFAST	BREAKFAST	BREAKFAST
HEATING/AC	HEATING/AC	HEATING/AC	HEATING/AC
BEDDING	BEDDING	BEDDING	BEDDING
ROOM	ROOM	ROOM	ROOM
<i>House</i>	<i>Vacation rental</i>	<i>Hotel</i>	<i>All-inclusive resort</i>

 YOU MANAGE

 YOU NO LONGER HAVE TO MANAGE

GDPR Processor Requirements (Article 28 GDPR)



GDPR RELATIONSHIPS

Some definitions:

01

Controller – “natural or legal person ... which, determines the purposes and means of the processing of personal data...” (Art 4 (7), GDPR)

02

Processor – “natural or legal person... which processes the data on behalf of the Controller...” (Art 4 (8), GDPR)

03

Processing – “any operation... which is performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction” (Art 4(2), GDPR)

“Appropriate Technical and Organizational Measures”

- ... the controller shall use **only processors providing sufficient guarantees to implement appropriate technical and organizational measures** in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject. (GDPR, Art 28(1))

Prescribed Contractual Clauses under Art. 28

1

General
Requirements

2

Data Transfers

3

Authorized
Persons

4

Sub-processors

5

Controller
Assistance

6

End of Services

7

Documentation
and Audits

(1) General
Requirements
(Art 28(3),
GDPR)

Processing by a processor shall be governed by a contract... that is binding on the processor with regard to the controller and that sets out the **subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.**

(2) Data
Transfers (Art
28(3)(a),
GDPR)

The contract... shall stipulate...that the processor processes the personal data only on documented instructions from the controller...**including with regard to transfers of personal data to a third country or an international organization...**

(3) Authorized
Persons (Art
28(3) (b),
GDPR)

...that persons authorized to process the personal data have committed themselves to **confidentiality** or are under an appropriate statutory obligation of confidentiality;

(4) Sub-
processors
(Art 28(2),
GDPR)

The processor shall not engage another processor without prior specific or general written authorization of the controller...

...the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

(4) Sub-
processors
(Art 28(4),
GDPR)

... the same data protection obligations as set out in the contract ..between the controller and processor...shall be imposed on that other processor by way of a contract...

Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations

(5) (a)
Controller
Assistance –
Data Subject
Rights

“the contract...shall stipulate...that the processor:...assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the controller’s obligation to respond to requests for exercising the data subject’s rights laid down in Chapter III”
(GDPR, Art 28 (3)(e))

Chapter III (Rights of Data Subject) covers transparency and modalities; information and access to personal data; rectification and erasure; right to object and automated individual decision-making; and restrictions

(5) Controller Assistance

“the contract...shall stipulate...that the processor assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor” (GDPR, Art 28(3)(f))

(5) Controller Assistance

Art. 32: Security of Processing

Art. 33: Notification of a personal data breach to the supervisory authority

Art. 34: Communication of a personal data breach to the data subject

Art. 35: Data protection impact assessment

Art. 36: Prior consultation

(5) Controller Assistance – Data Security (Art 32, GDPR)

+ “the contract... shall stipulate...that the processor takes all measures required pursuant to Article 32...”

Controller and processor to implement **“appropriate technical and organizational measures** to ensure **a level of security appropriate to the risk...**”

Adherence to approved code of conduct/certification mechanism to demonstrate compliance

(5) Controller Assistance – Data Breach (Art 33, 34, GDPR)

Controller's obligations to notify supervisory authority under Article 33

Controller's obligations to communicate to data subject under Article 34

The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

(5) Controller
Assistance –
Data
Protection
Impact
Assessment
(Art 35, GDPR)

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

(6) End of
Services (Art
28(3)(g),
GDPR)

At the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to the processing, and deletes existing copies..

(6)

Documentation
and audits (Art
28(3)(h), GDPR)

Makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller

Earning your trust with contractual commitments to the General Data Protection Regulation

Apr 17, 2017 | Rich Sauer - Microsoft Corporate Vice President & Deputy General Counsel



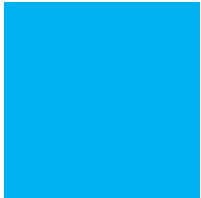
Trust is central to Microsoft's mission to empower every person and every organization on the planet to achieve more. So that you can trust the Microsoft products and services you use, we take a principled approach with strong commitments to privacy, security, compliance and transparency. This approach includes helping you on your journey to meet the requirements of the European Union's General Data Protection regulation (GDPR), a privacy regulation which goes into effect on May 25, 2018.

If your organization collects, hosts or analyzes personal data of EU residents, GDPR provisions require you to use third-party data processors who guarantee their ability to implement the technical and organizational requirements of the GDPR. To further earn your trust, we are making contractual commitments available to you that provide key GDPR-related assurances about our services. Our contractual commitments guarantee that you can:

- Respond to requests to correct, amend or delete personal data.
- Detect and report personal data breaches.
- Demonstrate your compliance with the GDPR.

Microsoft is the first global cloud services provider to publicly offer you these contractual commitments. We believe privacy is a fundamental right. The GDPR is an important step forward to further clarify and enable individual privacy rights and look forward to sharing additional updates how we can help you comply with this new regulation and, in the process, advance personal privacy protections.

Your Cloud Provider is Your Partner



Risk customers must manage

Data Classification | End Point Devices



Shared risks

Identity & access management



Risks a provider can help reduce

Physical | Networking

Responsibility

On-Prem IaaS PaaS SaaS

Data classification and accountability



Client & end-point protection



Identity & access management



Application level controls



Network controls



Host Security



Physical Security



Cloud Customer Cloud Provider

Partnering with your Cloud Provider

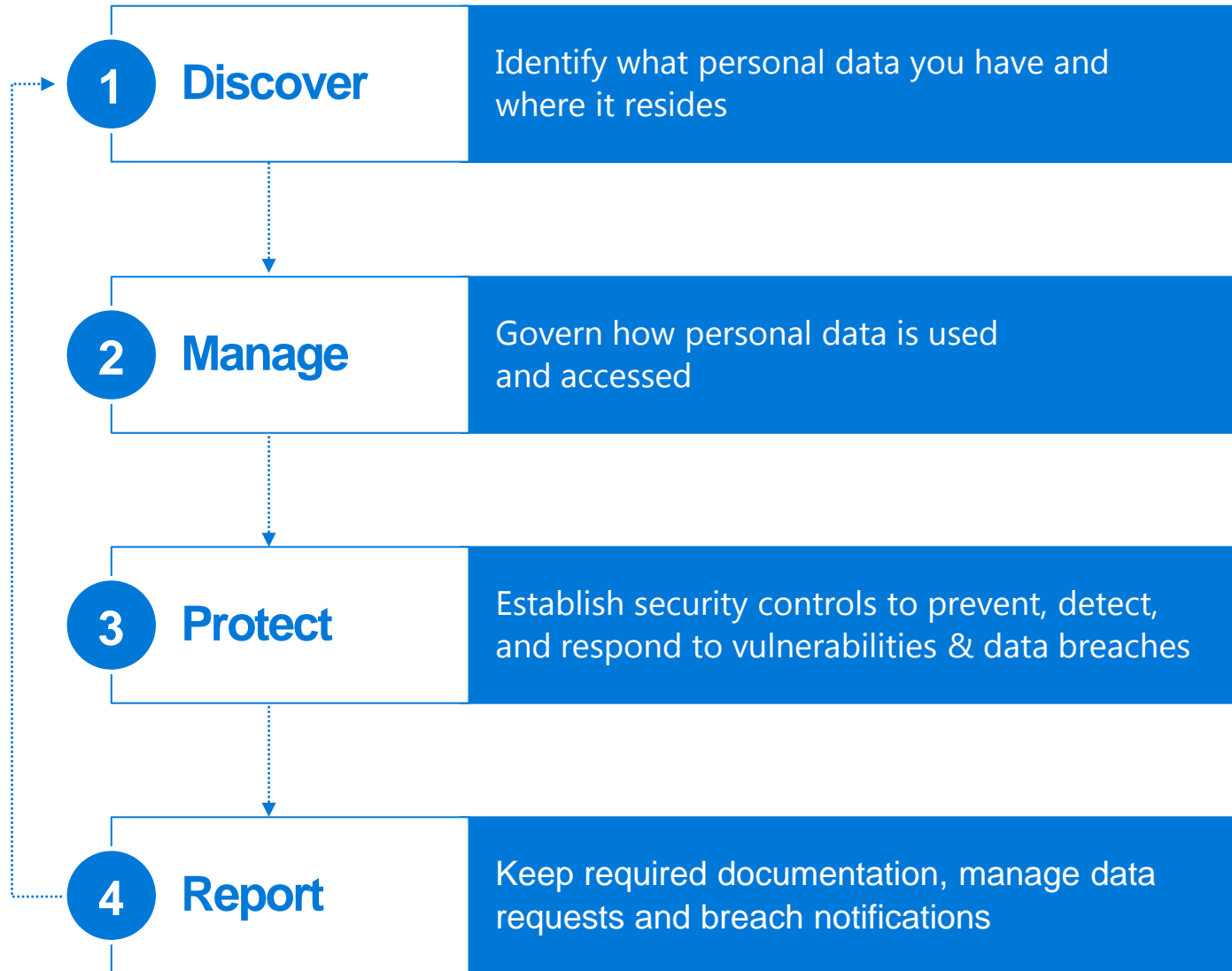
“Make no mistake, the GDPR sets a new and higher bar for privacy rights, for security, and for compliance.

And while your journey to GDPR may seem challenging, Microsoft is here to help all of our customers around the world.”

Brad Smith
President & Chief Legal Officer
Microsoft Corporation



How do I get started?



SOLUTIONS TO HELP YOU PREPARE FOR THE GDPR



1 Discover:

Identify what personal data you have and where it resides

In-scope:

Any data that helps you identify a person

- Name
- Email address
- Social media posts
- Physical, physiological, or genetic information
- Medical information
- Location
- Bank details
- IP address
- Cookies
- Cultural identity

Inventory:

Identifying where personal data is collected and stored

- Emails
- Documents
- Databases
- Removable media
- Metadata
- Log files
- Backups

Example solutions

Microsoft Azure

Microsoft Azure Data Catalog

Enterprise Mobility + Security (EMS)

Microsoft Cloud App Security

Dynamics 365

Audit Data & User Activity
Reporting & Analytics

Office & Office 365

Data Loss Prevention
Advanced Data Governance
Office 365 eDiscovery

SQL Server and Azure SQL Database

SQL Query Language

Windows & Windows Server

Windows Search

2 Manage:

Govern how personal data is used and accessed within your organization

Data governance:

Defining policies, roles and responsibilities for the management and use of personal data

- At rest
- In process
- In transit
- Storing
- Recovery
- Archiving
- Retaining
- Disposal

Data classification:

Organizing and labeling data to ensure proper handling

- Types
- Sensitivity
- Context / use
- Ownership
- Custodians
- Administrators
- Users

Example solutions

Microsoft Azure

Azure Active Directory
Azure Information Protection
Azure Role-Based Access Control (RBAC)

Enterprise Mobility + Security (EMS)

Azure Information Protection

Dynamics 365

Security Concepts

Office & Office 365

Advanced Data Governance
Journaling (Exchange Online)

Windows & Windows Server

Microsoft Data Classification Toolkit

3 Protect:

Establish security controls to prevent, detect, and respond to vulnerabilities and data breaches

Preventing data attacks:

Protecting your data

- Physical datacenter protection
- Network security
- Storage security
- Compute security
- Identity management
- Access control
- Encryption
- Risk mitigation

Detecting & responding to breaches:

Monitoring for and detecting system intrusions

- System monitoring
- Breach identification
- Calculating impact
- Planned response
- Disaster recovery
- Notifying DPA & customers

Example solutions

Microsoft Azure

Azure Key Vault
Azure Security Center
Azure Storage Services Encryption

Enterprise Mobility + Security (EMS)

Azure Active Directory Premium
Microsoft Intune

Office & Office 365

Advanced Threat Protection
Threat Intelligence

SQL Server and Azure SQL Database

Transparent data encryption
Always Encrypted

Windows & Windows Server

Windows Defender Advanced Threat Protection
Windows Hello
Device Guard

4 Report:

Keep required documentation, manage data requests and breach notifications

Record-keeping:

Enterprises will need to record the:

- Purposes of processing
- Classifications of personal data
- Third-parties with access to the data
- Organizational and technical security measures
- Data retention times

Reporting tools:

Implement reporting capabilities

- Cloud services (processor) documentation
- Audit logs
- Breach notifications
- Handling Data Subject Requests
- Governance reporting
- Compliance reviews

Example solutions

Microsoft Trust Center
Service Trust Portal

Microsoft Azure
Azure Auditing & Logging
Azure Data Lake
Azure Monitor

Enterprise Mobility + Security (EMS)
Azure Information Protection

Dynamics 365
Reporting & Analytics

Office & Office 365
Service Assurance
Office 365 Audit Logs
Customer Lockbox

Windows & Windows Server
Windows Defender Advanced Threat Protection

Compliance manager

Manage your compliance from one place

- **Real-time risk assessment**

An intelligent score shows your compliance posture against evolving regulations

- **Actionable insights**

Recommended actions to improve your data protection capabilities

- **Simplified compliance**

Streamlined workflow and audit-ready reports

The screenshot displays the Microsoft Compliance Manager interface for Office 365 in-Scope Cloud Services against the ISO 27001:2013 framework. The top section shows a compliance score of 2/174, with 1% of controls assessed. A progress bar indicates the assessment status, and a 'Last Modified' date of 9/13/2017 is shown. Below this, a table lists various controls, including 'Microsoft Managed Controls' and 'Office 365 Access Control Control Family'. A detailed view of a specific control (AR-0112) is shown, including its description, status (Implemented), test date (10/19/2016), and test result (Passed). The interface also provides implementation details, test plan details, and management responses for the selected control.

MS Control	Certification Control(s)	Description	Status	Test Date	Test Result
AR-0112	ISO 27001:2013:- C.07.03.a, C.07.03.b, C.07.03.c	Information security policy awareness...Office 365 personnel awareness around contribution to the effectiveness of the information security management system...Personnel awareness of the implications of non-conformance...Awareness education and training	Implemented	10/19/2016	Passed

Resources

[Microsoft.com/GDPR](https://www.microsoft.com/GDPR)

- [GDPR Assessment Tool](#)
- [Guidance](#)
- [Whitepapers](#)
- [GDPR F.A.Q.](#)
- [Solutions](#)



Last Words



25 May 2018



Cloud computing as a tool both for digital transformation and compliance



Controllers and processors have shared compliance responsibilities.



Work with your cloud providers for commitments and assurances of compliance.



Watch this space! Guidance, Codes of Conduct and GDPR Certification!

