How Microsoft Azure Can Help Organizations Become Compliant with the EU General Data Protection Regulation (GDPR)

Published May 2017

Microsoft

Disclaimer

This white paper is a commentary on the GDPR, as Microsoft interprets it, as of the date of publication. We've spent a lot of time with GDPR and like to think we've been thoughtful about its intent and meaning. But the application of GDPR is highly fact-specific, and not all aspects and interpretations of GDPR are well-settled.

As a result, this white paper is provided for informational purposes only and should not be relied upon as legal advice or to determine how GDPR might apply to you and your organization. We encourage you to work with a legally qualified professional to discuss GDPR, how it applies specifically to your organization, and how best to ensure compliance.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS WHITE PAPER. This white paper is provided "as-is". Information and views expressed in this white paper, including URL and other Internet website references, may change without notice.

This white paper does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this paper for your internal, reference purposes only.

Published May 2017

Version 1.4

Acknowledgements

Author
Eric Tierling

Contributors and Reviewers
Rich Hagemeyer
Alan Ross
Frank Simorjay
Andreas Ebert
Markus Feichtner
Scott Schnoll
Adwait Joshi
Mike Wickstrand
Shont Miller
Afsaneh Karami
John Payseno
Steve Wacker (Wadeware LLC)

Table of contents

Introduction

On May 25 2018, a revised European data protection law is due to take effect, refreshing the former rules of the European Union (EU) that were defined in 1995. This new data protection law, which is designed to protect individuals in their data, is known as the General Data Protection Regulation (GDPR). Substantial changes are required by organizations throughout the world to achieve compliance with the GDPR.

The following definitions are relevant in this context:

- According to the GDPR, "personal data means any information relating to an identified or identifiable natural person," which is called a *data subject*.
- As a provider of cloud services and products such as Azure, Microsoft serves as a *data processor* – an entity that processes data on behalf of its customers.
- Another party in this relationship is the *controller*. This is the entity that determines the purposes, conditions, and means for the processing of personal data that is carried out by a processor.

For Azure cloud services, a customer usually is the controller and Microsoft acts as the processor.

> **Note:** This paper does not address aspects of Microsoft as a controller.

The goals of the GDPR are consistent with our long-standing commitments to security, privacy, transparency, and compliance. The Microsoft Trust Center allows you to view compliance by service, location, or industry, or by the certifications and attestations Microsoft has achieved for its cloud services. Microsoft also leads the industry in engagements with customers, regulatory bodies, and standards boards.

This white paper is designed to help you understand how Microsoft Azure can support you in your preparation for GDPR. Additional details about the GDPR in general and what you can also do to prepare for it is available in two additional Microsoft GDPR documents: "Beginning your General Data Protection Regulation journey" and "An Overview of the General Data Protection Regulation (GDPR)."

Overview

Microsoft cloud services such as Azure (as well as other cloud services and on-premises solutions that are out of scope for this paper) help organizations identify and catalog personal data in systems, build more secure environments, and simplify management of GDPR compliance. This white paper is written for decision makers, privacy officers, security and compliance personnel, and other stakeholders who like to learn more about useful actions to prepare for GDPR compliance by using Microsoft Azure. It is divided into the following sections:

- Section 1 discusses the GDPR in general, its importance, and what approach Microsoft suggests for addressing GDPR requirements.
- Section 2 discusses how you can use Azure today to prepare for GDPR compliance.
- Section 3 discusses related topics such as Azure Cloud Germany.
- Section 4 provides additional recommendations that may be useful for your organization's journey toward GDPR compliance.

Shared responsibilities between Microsoft and customers

Understanding how a cloud service provider such as Microsoft shares responsibility with customers to meet security, privacy, and compliance requirements is an essential part of cloud computing. When adopting Microsoft cloud services and products, it is important to remember that some security, privacy, and compliance needs are the responsibility of the customer, some are the responsibility of Microsoft, and some are shared. The white paper "Shared responsibility in cloud computing" can help you learn more about each party's responsibilities in cloud-based solutions.

1. GDPR: A new era for the protection of personal data

Since the mid-1990s, data privacy for individuals in the 28 member states of the EU (European Union) and some non-EU countries (Iceland, Liechtenstein, and Norway) that are collectively referred to as the EEA (European Economic Area) was mainly based on the EU Directive 95/46/EC (also known as the Data Protection Directive), adopted in 1995. This directive outlined the minimum standards for data protection in Europe.

Although the Data Protection Directive applied to 31 countries in the EEA, it was by definition a *directive*, which required each country to transpose the requirements into their own local data protection law. The result has been local laws that differ in detail (for example, with regard to the consent that is required by an individual for processing his or her personal data).

In late 2010, the EU initiated an approach to reform these data protection rules to modernize and align them with the Internet and other digital transformation technologies. The first draft of this new law was presented in January 2012. It was finalized four years later and adopted as Regulation (EU) 2016/679 or simply the *General Data Protection Regulation*, abbreviated *GDPR*.

In total, this personal data protection law of the EU consists of 99 articles. It is supplemented by a number of elucidations in the form of 173 recitals (a recital can contain additional explanations of an article; the English PDF file version of the GDPR law is 88 pages long). Because the GDPR is a regulation, no transposition into local laws is required. Instead, the GDPR applies to all EU and EEA member states, and will be implemented by May 25, 2018.

The GDPR replaces individual local data protection laws based on the transposition of the former Data Protection Directive, and is valid in each of the 31 countries of the EU and the EEA. Each EU and EEA member state has the freedom to define additional personal data protection laws that further extend the provisions defined in the GDPR. Thus, the GDPR serves as the lowest common denominator for new data protection rules implemented in the 28 EU countries as well as in Iceland, Lichtenstein, and Norway.

> **Note:** An important fact to highlight is that the GDPR applies not just to organizations located in the EU, but to any organization – whether in the EU or not – that offers goods and services to EU individuals, or monitors the behavior of people in the EU.

What organizations can do today to prepare for the GDPR

Microsoft has products and services available that can help you in your preparation for meeting GDPR requirements. We have developed a four-step process that we recommend you follow on your journey to GDPR compliance. The four steps are:

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 and data breaches.
4. **Report:** Keep required documentation, manage data requests, and provide breach notifications.

2. GDPR compliance preparation

Existing functionality in Microsoft cloud services such as Azure[1] can pave the way for you and serve as enablers for your GDPR compliance. The following tables illustrate how the four steps relate to specific requirements in the GDPR, and how your organization can use features in Azure that are available today to start preparing for your GDPR compliance.

Step 1: Discover

The goals for the first step are to identify personal data and where it resides.

Topic	Categorization – categorizing and tagging of data sets
GDPR citation: Art. 9	Azure Information Protection can help you automate the process of classifying categories of data. Azure Information Protection labels are available to apply classification to documents and email. The classification is identifiable always, regardless of where the data is stored or with whom it is shared. The persistent labels include visual markings such as a header, footer, or watermark. Metadata is added to files and email headers in clear text so that other services (such as data loss prevention solutions) can identify the classification and take appropriate action. In addition to tagging personal data in Azure Information Protection, you can use Azure Data Factory and Azure HDInsight for this purpose. Azure Data Factory has capabilities to help trace and locate personal data, including visualization and monitoring tools to identify when data arrived and where it came from. There are also capabilities for automating data pipelines with on-demand cloud resource management. Azure HDInsight helps by providing a platform to deploy various software frameworks that can trace and search for personal data. In addition, you can import Azure HDInsight data into Excel and query for personal data using the power query functionality. Azure Data Catalog is also an essential element in this step. This service helps with the management of data (the metadata, not the data itself) and can provide your organization with a strategic platform functionality to become and stay compliant with the GDPR.

[1] Although most of the Azure services are sold on a consumption basis, certain services are sold separately on a per-seat basis. Please see the Azure pricing page for details.

Topic	Consent – provide mechanism for data subjects to withdraw consent
GDPR citation: Art. 7, Sec. 3	As an Azure customer, you have full access to your data at all times and can always search for, export, and delete portions of that data that relate to an individual data subject at any time. More information about what happens to your data if you leave the service by ending your subscription is available at the Microsoft Trust Center – How we manage your data.

Step 2: Manage

The goal of the second step is to govern how personal data is used and accessed within your organization.

Topic	Data security – segregation of duties
GDPR citation: Art. 25, Sec. 2	Azure services include the segregation of role functionality: • You can use Azure Role-Based Access Control (RBAC) to enforce separation of duties. This Azure service enables you to define fine-grained access permissions to grant only the amount of access that users need to perform their jobs. Instead of giving everybody unrestricted permissions for Azure resources, you can allow only certain actions for accessing personal data. • You can use Azure Key Vault for web applications to support separation of duties. This service allows you to implement a segregation of role functionality in the management of keys and data. • To minimize the number of people who have access to certain information such as personal data, you can also use Azure Active Directory Privileged Identity Management. This functionality allows you to discover, restrict, and monitor privileged identities and their access to resources. You can also enforce on-demand, just-in-time administrative access when needed.

Topic	Data security – provide mechanism to grant and restrict access to personal data
GDPR citation: Art. 25, Sec. 2	Azure Information Protection helps you to classify, label, and protect your documents and email. This can be done automatically by administrators who define rules and conditions, manually by users, or a combination in which users are given recommendations. For example, if a user saves a Word document that contains personal data such as credit card information (after an administrator has created and applied a rule to automatically recognize this kind of information), the user receives a notice that recommends applying a specific label to the document.

Topic	Data security – provide mechanism to grant and restrict access to personal data
	In addition, Azure is audited at least annually against global data privacy standards, such as ISO 27018. Reports of these audits can be downloaded from the Service Trust Preview, along with other compliance, privacy, and security-related information.

Step 3: Protect

The goal of the third step is to establish security controls to prevent, detect, and respond to vulnerabilities and data breaches.

Topic	Data protection – provide mechanism to grant and restrict access to personal data
GDPR citation: Art. 25, Sec. 2	Azure Key Vault, a cloud-hosted service for managing cryptographic keys and other secrets used in cloud applications, provides capabilities to help you with the protection of data and access to data. This Azure service enables you to safeguard your cryptographic keys, certificates, and passwords. Azure Key Vault uses specialized hardware security modules (HSMs) for maximum protection and is designed in a way that allows you to maintain control of keys and data. Also, there is a bring-your-own-key (BYOK) capability provided by Azure Key Vault and its various related options; this white paper provides more information about this capability. You can monitor and audit the usage of your stored keys in different ways, from Azure logging and the import of these logs into Azure HDInsight to the ability to incorporate this information into your existing security information and event management (SIEM) system for additional analysis, such as threat detection. Azure is developed using the Microsoft Security Development Lifecycle, which includes privacy-by-design and privacy-by-default methodologies. These methodologies define the privacy principles and standard privacy features that inform product development. Principles that govern these methodologies include: • Microsoft uses your data only to provide you the online services, including purposes compatible with providing those services. • Microsoft does not mine your data for advertising purposes. • If you ever choose to leave the service, you may take your data with you with full fidelity. • Microsoft tells the customer where the data resides, who has access, and under what circumstances.

Topic	Data security – provide mechanism to pseudonymize, encrypt, or otherwise secure personal data
GDPR citation: Art. 32, Sec. 1, Sub. (a)	Azure offers a variety of options to support pseudonymization, encryption and security. • Azure Storage Services Encryption helps you to protect and safeguard your data, including personal data, in support of organizational security commitments and compliance requirements defined by frameworks and regulations such as the GDPR. Azure Storage Service Encryption allows you to request that the storage service automatically encrypt the data when writing it to Azure Storage. Microsoft handles all the encryption, decryption, and key management in a fully transparent fashion. All data is encrypted using 256-bit AES (Advanced Encryption Standard) encryption, also known as AES-256, one of the strongest block ciphers available. You can enable this feature on all available redundancy types of Azure File Storage, since both options – LRS (locally redundant storage) and GRS (geo-redundant storage) – are included. • You can also use Azure Disk Encryption for virtual machines that are hosted in Azure and have Windows or Linux running as a local operating system. By doing so, all data inside these virtual machines is encrypted automatically as well. • Transparent Data Encryption with Azure SQL Database helps protect against the threat of malicious activity by performing real-time encryption and decryption of the database, associated backups, and transaction log files at rest. All of this takes place without requiring changes to the applications.

Topic	Data security – implement appropriate technical security measures in the product to confirm the ongoing confidentiality, integrity, and availability of personal data and processing systems

GDPR citation:
Art. 32, Sec. 1, Sub. (b)
	All Azure services are developed using the Microsoft Security Development Lifecycle. As a foundation, Microsoft uses many service-level security measures to assure the ongoing confidentiality, integrity, and availability of processing systems and the data they process. These service-level security measures use a defense-in-depth strategy that includes protections at the physical, logical, and data layers. These security measures include but are not limited to:
	• Physical - Datacenters
	  ○ 24-hour restricted access
	  ○ Multiple authentication processes (such as badges, smart cards, and biometric scanners)
	  ○ On-premises security guards

Topic	Data security – implement appropriate technical security measures in the product to confirm the ongoing confidentiality, integrity, and availability of personal data and processing systems

- Monitoring using video surveillance, motion sensors, and security breach alarms
- Automated fire prevention and extinguishing systems

- Physical - Network
  - Access control lists
  - IPsec policies on hosts
  - Restrictive firewall rules and host-based firewall rules
  - Edge router security
  - Network segmentation to provide physical separation of critical back-end servers and storage devices from public-facing interfaces
- Logical
  - Strict control of admin access to customer data
  - Use of the Microsoft Security Development Lifecycle for all products
  - Antimalware software
  - Pretested standard configurations
- Data
  - Data isolation using Azure Active Directory authorization, role-based access controls, and workload-specific isolation mechanisms
  - Use of encryption and other cryptographic security measures

As a result, Microsoft Azure provides confidentiality, integrity, and availability of data while also enabling transparent accountability. To help you better understand the collection of security controls implemented within Azure from both customer and Microsoft perspectives, Introduction to Azure Security provides a comprehensive overview of the security measures.

Also, many organizations have chosen hybrid IT configurations in which some of the organization's information assets are in Azure while others remain on-premises. In such hybrid IT scenarios, there is usually some type of cross-premises connectivity between the organization's on-premises networks and Azure Virtual Networks. For the confidentiality, integrity, and availability of information that is exchanged, including personal data, Azure offers different options:

- By implementing a Site-to-Site VPN with Azure you can create a virtual private connection between your on-premises network and an Azure Virtual Network. This connection takes place over the Internet and allows you to securely "tunnel" information inside an encrypted link between your network and Azure. Site-to-Site VPN is a secure, mature technology that has been

Topic	Data security – implement appropriate technical security measures in the product to confirm the ongoing confidentiality, integrity, and availability of personal data and processing systems
	deployed by enterprises of all sizes for decades. The IPsec tunnel mode is used in this option as an encryption mechanism. • Because traffic within the tunnel does traverse the Internet with a site-to-site VPN, Microsoft offers another, even more secure connection option for cross-premises connectivity. Azure ExpressRoute is a dedicated WAN link between Azure and an on-premises location or an Exchange hosting provider. Because this is a direct connection of your telecommunication provider, your data does not travel over the Internet and therefore is not exposed to it. Best practices for implementing a secure hybrid network that extends an on-premises network to Azure is available at the Azure Architecture website.

Topic	Data security – provide mechanism to restore the availability and access to personal data
GDPR citation: Art. 32, Sec. 1, Sub. (c)	With Microsoft Azure, you can choose between different options to restore the availability of and access to personal data. • Azure Backup is a simple, secure, and reliable cloud-integrated backup service offering to back up and restore your data. The instant restore functionality of Azure Backup provides you with a restore service for recovering individual files and folders backed up from sources in the cloud or on-premises. • Azure Site Recovery replicates, fails over, and recovers workloads so that they remain available when failure occurs. Designed as an automated protection and disaster recovery in the cloud solution, it coordinates and manages the ongoing replication of data. Azure Site Recovery can protect both Microsoft and VMware virtual servers as well as physical servers located in your datacenter, so you can use Azure or your secondary datacenter as your recovery site. • In general, Azure geo-redundant storage (GRS) replicates your data, including personal data, to a secondary region that is hundreds of miles away from the primary region. When you create a storage account, you select the primary region for the account. The secondary region is determined based on the primary region and cannot be changed. If your Azure storage account has GRS enabled, your data is durable even in the case of a complete regional outage or a disaster in which the primary region is not recoverable.

Topic	Data security – facilitate regular testing of security measures
GDPR citation: Art. 32, Sec. 1, Sub. (d)	Microsoft conducts tests of Azure security measures on a regular basis. We have decades-long experience building enterprise software and running some of the largest online services in the world. This experience is used to implement and continuously improve security-aware software development, operational management, and threat-mitigation practices that are essential to the strong protection of services and data. The guiding principle of the Microsoft security strategy is to "assume breach." The Microsoft global incident response team works around the clock to mitigate the effects of any attack against Microsoft cloud services. Highly specialized groups of security experts working in what is known as the Microsoft Red Team use their expertise to strengthen threat detection, response, and defense for Microsoft enterprise cloud services such as Azure. They simulate real-world breaches, conduct continuous security monitoring, and practice security incident response to validate and improve the security of our services and your data. Rigorous third-party audits verify that Azure adheres to strict security controls such as the ones contained in the ISO/IEC 27001 standard mandate. Currently, both the Azure public cloud and Azure Cloud Germany are audited once a year for ISO/IEC 27001 compliance by a third-party accredited certification body, which provides independent validation that security controls are in place and operating effectively. Also, as part of the annual ISO/IEC 27001 recertification process for our cloud infrastructure, Microsoft runs annual tests for infrastructure failures.

Topic	Breach response and notification – processor shall notify the controller without undue delay after becoming aware of a personal data breach
GDPR citation: Art. 33	This requirement is fulfilled by all Azure services. Microsoft will promptly notify you of any security incident, investigate the incident, and provide you with detailed information about it. Also, Microsoft takes reasonable steps to mitigate the effects and to minimize any damage resulting from security incidents. In general, we use a Shared Responsibility Model for our Azure cloud services. There are areas that fall under your area of responsibility (for example, within your Azure Virtual Machine) in which Microsoft does not monitor for security incidents. However, in these instances we provide tools for this purpose (such as Azure Security Center). Apart from that, Microsoft holds the responsibility to notify you of security incidents that affect the infrastructure. For incidents in which Microsoft holds some or all of the responsibility to respond, we have established a detailed Security Incident Response Management process specific for Azure. We will also notify affected Microsoft customers with enough details to investigate on their end, and to meet any commitments they have made to their users

Topic	Breach response and notification – processor shall notify the controller without undue delay after becoming aware of a personal data breach
	while not unduly delaying the notification process. Customers, as controllers, are responsible for notifying affected third-party data subjects. Additional information about Azure Incident Response and Notification is described in Microsoft Azure Security Response in the Cloud. In addition, you can set designated emergency contacts in the Azure Security Center. General information on this topic is also available at the Microsoft Trust Center.

Step 4: Report

The goal of the fourth and final step is to retain the required documentation and to manage data subject requests and breach notifications.

Topic	Documentation – maintain auditable trails that record processing activities
GDPR citation: Art. 30	Azure features comprehensive logs to audit actions on resources. For example, through the Activity Log, you can determine who initiated an operation, when it occurred, and what the status of the operation was. You can use the Activity Log to determine the what, who, and when for any write operations (PUT, POST, DELETE) made for the resources in your Azure subscription. You can also become aware of the status of the operations and other relevant properties.

Topic	Data transfer – provide lawful mechanism for data transfers in and out of the EU
GDPR citation: Art. 46, Sec. 1	Most Azure services enable you to specify the region (for example, West Europe) where your data will be stored. Microsoft may replicate to other regions for data resiliency but will not replicate data outside the broader geographic area (for example, Europe). Additional information is available at http://azuredatacentermap.azurewebsites.net.

Topic	Data transfer – maintain inventory of data transfer contracts with third parties
GDPR citation: Art. 46, Sec. 1	This requirement applies to all Microsoft cloud services. We maintain an inventory of third-party service providers who may have access to data. The Microsoft Online Services Subcontractor List covers the subcontractors for all the online services offered under the Data Processing Terms section of the Online Services Terms. Microsoft Commercial Support Contractors is a separate list that covers the

Topic	Data transfer – maintain inventory of data transfer contracts with third parties
	subcontractors used by the Microsoft global support organization for all Microsoft products, including Microsoft Online Services. Additional information is available at the Microsoft Trust Center.

Topic	Data transfer – provide appropriate safeguards, enforceable data subject rights, and effective legal remedies
GDPR citation: Art. 46, Sec. 2-3	Microsoft offers industry-leading contractual commitments for all of its enterprise cloud services, including Azure. The commitments include detailed data protection terms and the EU Model Clauses. Microsoft also complies with the EU-U.S. Privacy Shield Framework regarding the collection, use, and retention of personal information transferred from the European Union to the United States. Microsoft has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. Finally, Microsoft was the first cloud service provider to receive compliance attestation with ISO/IEC 27018. For details, see the Online Services Terms.

Topic	Privacy by Design – embed privacy controls in the product / service and its development lifecycle that are designed to implement data protection principles and to minimize the amount of data subject personal data collected
GDPR citation: Art. 25, Sec. 1; Art. 25, Sec. 2	This requirement is fulfilled by all Microsoft cloud services (such as Azure) that are developed using the Microsoft Security Development Lifecycle (SDL). Among other things, SDL includes privacy-by-design and privacy-by-default methodologies that define the privacy principles and standard privacy features that inform product development. Principles that govern these methodologies include: • Microsoft uses data only to provide its customers with online services, including purposes compatible with providing those services. • Microsoft does not mine data of its customers for advertising purposes. • If customers choose to leave the service, they can take their data with them with full fidelity. • Microsoft transparently tells customers where their data resides, who has access, and under what circumstances. In addition, Microsoft has integrated several contractual commitments that enable data subject privacy. Microsoft cloud products, including Azure, are audited at least annually against several global data privacy standards, including ISO 27018. These compliance reports are accessible at the Microsoft Trust Center.

Topic	Rights to access and to data portability – access and export the personal data to data subjects in structured, machine-readable formats
GDPR citation: Art. 15 & 20	All Azure data is accessible and exportable at any time. For example, you can export a virtual machine (VM) in a virtual hard disk (VHD) and SQL databases into various database formats. In general, all Azure Storage content is fully exportable. Also, Azure BizTalk Services and Azure Data Lake are helpful in this context. Azure BizTalk Services may help enable application integration to facilitate data portability requests by enabling you to integrate data from disparate sources. Azure Data Lake has capabilities that enable the extraction and conversion of data. Azure Data Lake Analytics jobs are written in the U-SQL language that is easily adaptable to specific needs. To learn more about U-SQL, see Get started with U-SQL language.

3. GDPR and a national cloud such as Microsoft Azure Germany

Since September 2016, Azure Germany has been available via Microsoft Cloud Germany – a first-of-its-kind model in Europe developed in response to customer needs. With your data remaining in Germany under the control of a data trustee, Microsoft Cloud Germany provides a differentiated option to the Microsoft cloud services already available across Europe, thereby creating increased opportunities for innovation and economic growth for highly regulated partners and customers in Germany, the European Union (EU), the European Free Trade Association (EFTA), and the United Kingdom (UK). Infrastructure and platform services that enable a broad range of solutions from the Internet of Things (IoT) to Machine Learning are made available via locally deployed datacenters in Magdeburg and Frankfurt, Germany.

Your data stored in these datacenters is managed under the control of a data trustee, T-Systems International, an independent German company and subsidiary of Deutsche Telekom. Your data processed in Microsoft Cloud Germany remains in Germany under the control of T-Systems International. The incorporation of such a data trustee model provides additional controls for your data, as access is provided only with the permission of the customer or the data trustee. Microsoft Cloud Germany adheres to German data handling regulations and gives customers additional choices of how and where data is processed.

For details, see the white papers Microsoft Cloud Germany – Compliance in the cloud for organizations in EU/EFTA and Microsoft Azure Germany - IT Grundschutz Compliance Workbook.

Organizations that use or are interested in Microsoft Cloud Germany and that want to know about the GDPR compliance of this unique cloud implementation can build on the trust and transparency that characterize all Microsoft compliance and certification activities:

- Like the Microsoft Azure public cloud, Microsoft Azure Germany is both ISO/IEC 27001 certified and compliant with ISO/IEC 27018. This is an important milestone for the GDPR compliance of Microsoft Azure Germany.
- In general, Microsoft Azure Germany uses the same underlying systems and operations procedures as other Microsoft cloud services, such as Azure. Thus, compliance options that apply to the Microsoft cloud also apply to Microsoft Azure Germany.

4. Final recommendations

The GDPR will affect how you use and manage data across a variety of systems – from devices and the IoT to on-premises systems and cloud services. Therefore, the GDPR has broad implications for organizations that use personal data in their business.

We are here to help you to start your journey to GDPR compliance today:

- Microsoft cloud services, such as Azure, Dynamics 365, and Office 365 enable you to ease the processes you have to implement for GDPR compliance through smart technology, innovation, and collaboration.
- Through our cloud services and on-premises solutions, Microsoft helps you locate and catalog the personal data in your systems, build a more secure environment, and simplify the management and monitoring of personal data.
- To help organizations to meet their GDPR requirements, Microsoft is investing in additional features and functionality.
- Finally, we are sharing best practices from our own privacy experts.

As with many standards and regulations, GDPR compliance is not a one-time state, but rather a continuous process. By working with a hyperscale cloud service provider such as Microsoft and using services such as Azure, you can benefit from the "economics of compliance." Microsoft cloud services enable you to reduce the programming efforts and administrative burdens required to become GDPR compliant.

Microsoft has a long tradition of compliance in the cloud. Additional information about how Microsoft is working to help organizations become GDPR compliant is available at:

- GDPR on the Microsoft Trust Center
  https://microsoft.com/gdpr
- Get GDPR compliant with the Microsoft Cloud
  https://aka.ms/GDPRBlogPost
- Microsoft white paper "Journey to GDPR"
  https://aka.ms/gdprwhitepaper
- Microsoft white paper "An Overview of the General Data Protection Regulation (GDPR)"
  https://aka.ms/gdproverview
- Microsoft National Clouds
  https://www.microsoft.com/en-us/TrustCenter/CloudServices/NationalCloud
- Create your free Azure account today
  https://azure.microsoft.com/free