Beginning your General Data Protection Regulation (GDPR) Journey

Accelerate GDPR compliance with the Microsoft Cloud

Table of Contents

Introduction 4

Microsoft's GDPR commitment 4

Understanding the GDPR—a primer 5

What is the GDPR? 5

Does the GDPR apply to my organization? 5

When does the GDPR take effect? 5

What are the key concepts in the GDPR? 5

What are examples of requirements of the GDPR related to these principles? 6

Partnering with Microsoft on your journey to the GDPR 6

Getting started with the GDPR 7

A platform approach to the GDPR 7

Taking action today 10

Discover: Identify what personal data you have and where it resides 10

Does the GDPR apply to my data? 10

Building your inventory 10

Manage: Govern how personal data is used and accessed 13

Data governance 13

Data classification 14

Protect: Establish security controls to prevent, detect, and respond to vulnerabilities and data breaches 17

Protecting your data 17

Detecting and responding to data breaches 23

Report: Execute on data requests, report data breaches, and keep required documentation 27

Record-keeping 27

Reporting tools and documentation of cloud services 29

Notifying data subjects 30

Handling data subject requests 30

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

Published May 2017

Version 1.1

Introduction

On May 25, 2018, a European privacy law is due to take effect that sets a new global bar for privacy rights, security, and compliance.

The General Data Protection Regulation, or GDPR, is fundamentally about protecting and enabling the privacy rights of individuals. The GDPR establishes strict global privacy requirements governing how you manage and protect personal data while respecting individual choice—no matter where data is sent, processed, or stored.

Microsoft and our customers are now on a journey to achieve the privacy goals of the GDPR. At Microsoft, we believe privacy is a fundamental right, and we believe that the GDPR is an important step forward for clarifying and enabling individual privacy rights. But we also recognize that the GDPR will require significant changes by organizations all over the world.

Although your journey to GDPR may seem challenging, we are here to help you.

Microsoft's GDPR commitment

Trust is central to our mission to empower every person and every organization on the planet to achieve more. We take a principled approach to building trust, with strong commitments to privacy, security, compliance, and transparency. We are applying those principles as we prepare for the GDPR.

We understand that GDPR compliance is a shared responsibility. That is why we are committed to be GDPR compliant across our cloud services when enforcement begins on May 25, 2018.

We are also committed to share our experience complying with complex regulations to help you craft the best path forward for your organization to meet the privacy requirements of the GDPR. With the most comprehensive set of compliance and security offerings of any cloud provider and a vast partner ecosystem, we are prepared to support your privacy and security initiatives now and in the future.

As part of our commitment to partner with you on your journey to the GDPR, we have developed this white paper to help with your preparations. The paper provides an overview of the GDPR, describes what we are doing to prepare for the GDPR, and shares examples of steps you can take today with Microsoft to start your own journey to GDPR compliance.

We look forward to sharing additional updates about how we can help you comply with this important new law and, in the process, advance personal privacy protections. Please visit our GDPR section of the Microsoft Trust Center to find additional resources and to learn more about how Microsoft can help you fulfill specific GDPR requirements.

Understanding the GDPR—a primer

Before describing the specific ways that Microsoft can help you prepare for the GDPR, we'd like to address some of the most fundamental and critical questions about the regulation and what it might mean for you. A fuller overview can be found here.

What is the GDPR?

The General Data Protection Regulation is a new privacy regulation across the European Union. It provides individuals with more control over their personal data, ensures transparency about the use of data, and requires security and controls to protect data.

Does the GDPR apply to my organization?

The GDPR applies more broadly than might be apparent at first glance. The law imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents. The GDPR applies no matter where you are located.

Unlike privacy laws in some other jurisdictions, the GDPR is applicable to organizations of all sizes and all industries. The EU is often viewed as a role model on privacy issues internationally, so we also expect to see the concepts in the GDPR adopted in other parts of the world over time.

When does the GDPR take effect?

The GDPR takes effect on May 25, 2018. It will replace the existing Data Protection Directive (Directive 95/46/EC), which has been in force since 1995. The GDPR actually became law in the EU in April 2016, but given the significant changes some organizations will need to make to align with the regulation, a two-year transition period was included.

What are the key concepts in the GDPR?

The GDPR is structured around six principles:

- Requiring transparency on the handling and use of personal data.
- Limiting personal data processing to specified, legitimate purposes.
- Limiting personal data collection and storage to intended purposes.
- Enabling individuals to correct or request deletion of their personal data.
- Limiting the storage of personally identifiable data for only as long as necessary for its intended purpose.
- Ensuring personal data is protected using appropriate security practices.

What are examples of requirements of the GDPR related to these principles?

- Under the GDPR, individuals have a right to know if an organization is processing their personal data and to understand the purposes of that processing. An individual has the rights to have their data deleted or corrected, to ask that it no longer be processed, to object to direct marketing, and to revoke consent for certain uses of their data. The right to data portability gives individuals the right to move their data elsewhere and to receive assistance in doing so.
- The GDPR requires organizations to secure personal data in accordance with its sensitivity. In the event of a data breach, data controllers must generally notify the appropriate authorities within 72 hours. Additionally, if the breach is likely to result in a high risk to the rights and freedoms of individuals, organizations will also need to notify affected individuals without undue delay.
- There must be a legal basis for the processing of personal data. Any consent for the processing of personal data must be "freely given, specific, informed, and unambiguous." There are unique consent requirements to protect children under the GDPR.
- Organizations must conduct data protection impact assessments to predict the privacy impacts of projects and employ mitigations as needed. Records of processing activities, consents to process data, and compliance with the GDPR must be maintained.
- GDPR compliance is not a one-time activity, but is an ongoing process. Non-compliance with the GDPR can result in significant fines. To ensure compliance with the GDPR, organizations are encouraged to embrace a culture of privacy to protect the interests of individuals in their personal data.

For a more detailed GDPR overview and to better understand terms like pseudonymization, processing, controllers, processors, data subjects, and personal data, please visit Microsoft.com/GDPR. We are committed to help you meet the GDPR requirements and to further support the privacy rights of individuals.

Partnering with Microsoft on your journey to the GDPR

Complying with the GDPR is a business-wide challenge that will take time, tools, processes, and expertise, and may require significant changes in your privacy and data management practices. Your journey to comply with the GDPR will go more smoothly if you are operating in a well architected cloud services model and have an effective data governance program in place. When it comes to successfully complying with the GDPR, you can count on Microsoft and our extensive partner ecosystem to help you.

Microsoft has a long history of providing cloud services you can trust. We take a principled approach to privacy, security, compliance, and transparency with strong commitments to ensure you can trust the digital technology you rely on. We have the most extensive compliance portfolio in the industry, and we were the first to adopt key standards such as the ISO/IEC 27018 cloud privacy standard. Our customers and partners benefit from our experienced leadership in privacy, security, compliance, and transparency.

As you prepare to comply with the GDPR, here is what else you can expect from us:

- **Technology that meets your needs**. You can take advantage of our broad portfolio of enterprise cloud services to meet your GDPR obligations for areas including deletion, rectification, transfer of, access to, and objection to processing of personal data. Furthermore, you can count on our extensive global partner ecosystem for expert support as you use Microsoft technologies.
- **Contractual commitments**. We are standing behind you through contractual commitments for our cloud services, including timely security support and notifications in accordance with the new GDPR requirements. In March 2017, our customer licensing agreements for Microsoft cloud services will include commitments to be GDPR compliant when enforcement begins.
- **Sharing our experience**. We will share our GDPR compliance journey so you can adapt what we have learned to help you craft the best path forward for your organization.

Getting started with the GDPR

A platform approach to the GDPR

The systems you use to create, store, analyze, and manage data can be spread across a wide array of IT environments—personal devices, on-premises servers, cloud services, even the Internet of Things. This means that most of your IT landscape could be subject to the requirements of the GDPR.

Your efforts to meet the GDPR's requirements will be best served by looking at the requirements holistically and within the context of all your regulatory and legal privacy obligations. For instance, many of the security controls to prevent, detect, and respond to vulnerabilities and data breaches required by the GDPR are similar to the controls expected by other data protection standards, such as the ISO 27018 cloud privacy standard.

Rather than track the controls required by individual standards or regulations on a case-by-case basis, a best practice is to identify an overall set of controls and capabilities to meet these requirements. Likewise, rather than assessing individual technologies and solutions against a comprehensive regulation such as the GDPR, taking a platform view—such as one encompassing

Windows, Microsoft SQL Server, SharePoint, Exchange, Office 365, Azure, and Dynamics 365—can provide a clearer path to ensure you comply not only with the GDPR, but also with other requirements important to you as well.

We recommend you begin your journey to GDPR compliance by focusing on four key steps:

- **Discover**—identify what personal data you have and where it resides.
- **Manage**—govern how personal data is used and accessed.
- **Protect**—establish security controls to prevent, detect, and respond to vulnerabilities and data breaches.
- **Report**—execute on data requests, report data breaches, and keep required documentation.

For each of the steps, we have outlined example tools, resources, and features in various Microsoft solutions that can be used to help you address the requirements of that step. While this document is not a comprehensive "how to," we have included links for you to find out more details, and more information is available at Microsoft.com/GDPR.

Given how much is involved, you should not wait until GDPR enforcement begins to prepare. You should review your privacy and data management practices now.

The following sections outline the specific elements of each component of the GDPR and describe ways that you can use products and services available from Microsoft today to get started.

Taking action today

Discover: Identify what personal data you have and where it resides

The first step towards GDPR compliance is to assess whether the GDPR applies to your organization, and, if so, to what extent. This analysis starts with understanding what data you have and where it resides.

Does the GDPR apply to my data?

The GDPR regulates the collection, storage, use, and sharing of "personal data." Personal data is defined very broadly under the GDPR as *any* data that relates to an identified or identifiable natural person.

If your organization has such data—in customer databases, in feedback forms filled out by your customers, in email content, in photos, in CCTV footage, in loyalty program records, in HR databases, or anywhere else—or wishes to collect it, and if the data belongs or relates to EU residents, then you need to comply with the GDPR. Note that personal data doesn't need to be stored in the EU to be subject to the GDPR—the GDPR applies to data collected, processed, or stored outside the EU if the data is tied to EU residents.

Building your inventory

To understand whether the GDPR *does* apply to your organization and, if it does, what obligations it imposes, it is important to inventory your organization's data. This will help you to understand what data is personal, and to identify the systems where that data is collected and stored, understand why it was collected, how it is processed and shared, and how long it is retained.

Here are examples of specific ways that that our cloud and on-premises offerings can help you with the GDPR's first step.

Azure

As Azure is an open and flexible cloud platform, it includes a service to help make data sources easily discoverable and identifiable. The Microsoft Azure Data Catalog is a fully managed cloud service that serves as a system of registration and system of discovery for your organization's data sources. In other words, Azure Data Catalog is all about helping you discover, understand, and use data sources to get more value from your existing data. Once a data source has been registered with Azure Data Catalog, its metadata is indexed by the service so that you can easily search to discover the data you need.

Dynamics 365

Dynamics 365 provides several visibility and auditing capabilities that can be used through the Reporting & Analytics dashboards of Dynamics 365 to identify personal data:

- Dynamics 365 includes a Report Wizard that you can use to easily create reports without using XML or SQL-based queries.
- Dashboards in Dynamics 365 provide an overview of business data—actionable information that's viewable across your organization.
- Microsoft Power BI is a self-service business intelligence (BI) platform you can use to discover, analyze, and visualize data, and share or collaborate on these insights with colleagues.

Enterprise Mobility + Security (EMS) Suite

Enterprise Mobility + Security features identity-driven security technologies that help you discover, control, and safeguard personal data held by your organization, as well as reveal potential blind spots and detect when data breaches occur.

Microsoft Cloud App Security is a comprehensive service that provides deeper visibility, comprehensive controls, and improved protection for your data in your cloud applications. You can have visibility to which cloud apps are in use in your network—identifying over 13,000 apps from all devices—and get risk assessments and ongoing analytics.

Microsoft Azure Information Protection helps you identify what your sensitive data is and where it resides. You can either query for data marked with a particular sensitivity or intelligently identify sensitive data when a file or email is created. Once identified, you can automatically classify and label the data—all based on the company's desired policy.

Office 365

There are several specific Office 365 solutions that can help you identify or manage access to personal data:

- Data Loss Prevention (DLP) in Office and Office 365 can identify over 80 common sensitive data types including financial, medical, and personally identifiable information.
- Content search in the Office 365 Security & Compliance Center can search across mailboxes, public folders, Office 365 Groups, Microsoft Teams, SharePoint Online sites, One Drive for Business locations, and Skype for Business conversations.

- Office 365 eDiscovery search can be used to find text and metadata in content across your Office 365 assets—SharePoint Online, OneDrive for Business, Skype for Business Online, and Exchange Online.
- Office 365 Advanced eDiscovery, powered by machine learning technologies, can help you identify documents that are relevant to a particular subject (for example, a compliance investigation) quickly and with better precision than traditional keyword searches or manual reviews of vast quantities of documents. Advanced eDiscovery can significantly reduce cost and effort to identify relevant documents and data relationships by using machine learning to train the system to intelligently explore large datasets and quickly zero in on what's relevant—reducing the data prior to review.
- Advanced Data Governance uses intelligence and machine-assisted insights to help you find, classify, set policies on, and take action to manage the lifecycle of the data that is most important to your organization.

SharePoint

You can utilize the SharePoint Search Service, and search functionality within the application, to trace personal data. To identify and search for sensitive content, SharePoint Server 2016 provides the same data loss prevention capabilities as Office 365.

SQL Server and Azure SQL Database

The SQL language can be used to query databases and to customize tools or services that may help enable this requirement. Search is fully supported through queries, although full trace logging should be done at the application level. The Script task provides code to perform custom functions, such as complex data queries that are not available in the built-in tasks and transformations that SQL Server Integration Services provides. The Script task can also combine functions in one script instead of using multiple tasks and transformations. This product suite also includes powerful business intelligence functionality providing end-user access to data insights.

Windows and Windows Server

To find data within Windows, you can utilize Windows Search to trace and locate personal data on your local machine and any connected devices that you have adequate permissions to access. To enhance the capabilities of Windows Search to locate the target data, you can configure Indexing Options in the Control Panel to customize the capabilities of Windows Search (for example, indexing file contents).

Manage: Govern how personal data is used and accessed

The GDPR provides data subjects—individuals to whom data relates—with more control of how their personal data is captured and used. Data subjects can, for example, request that your organization shares data that relates to them, transfer their data to other services, correct mistakes in their data, or restrict certain data from further processing in certain cases. In some cases, these requests must be addressed within fixed time periods.

Data governance

In order to satisfy your obligations to data subjects, you will need to understand what types of personal data your organization processes, how, and for what purposes. The data inventory discussed previously is a first step to achieving this understanding. Once that inventory is complete, it is also important to develop and implement a data governance plan. A data governance plan can help you define policies, roles, and responsibilities for the access, management, and use of personal data, and can help you ensure your data handling practices comply with the GDPR. For example, a data governance plan can give your organization confidence that it effectively respects data subject demands to delete or transfer data.

Microsoft Cloud Services

To support your data governance strategy, the Microsoft cloud services are developed using the Microsoft Privacy-by-Design and Privacy-by-Default methodology. When you entrust your data to Azure, Office 365, or Dynamics 365, you remain the sole owner: you retain the rights, title, and interest in the data you store in the services.

Microsoft cloud services take strong measures to help protect your customer data from inappropriate access or use by unauthorized persons, as detailed in the Microsoft Trust Center. These measures include restricting access by Microsoft personnel and subcontractors, and carefully defining requirements for responding to government requests for customer data.

However, you can access your own customer data at any time and for any reason.

In addition, we redirect government requests for your data to be made directly to you unless legally prohibited, and we have challenged government attempts to prohibit disclosure of such requests in court.

To help ensure Microsoft cloud services are managed correctly and to provide assurances to our customers, the cloud services are audited at least annually against several global data privacy standards, including HIPAA and HITECH, CSA Star Registry, and several ISO standards. These reports are accessible at https://servicetrust.microsoft.com/Documents/ComplianceReports.

Beyond these commitments, we provide you with the necessary control to ensure how data is managed and who has access to what data within your organization.

Azure

Azure Active Directory is an identity and access management solution in the cloud. It manages identities and controls access to Azure, on-premises, and other cloud resources, data, and applications. With Azure Active Directory Privileged Identity Management, you can assign temporary, Just-In-Time (JIT) administrative rights to eligible users to manage Azure resources.

Azure Role-Based Access Control (RBAC) helps you manage access to your Azure resources. This enables you to grant access based on the user's assigned role, making it easier to grant only the required permissions that users need to perform their jobs. You can customize RBAC per your organization's business model and risk tolerance.

Office 365

Office 365 solutions have several features that can help you manage personal data:

- Data governance features in the Office 365 Security & Compliance Center help you archive and preserve content in Exchange Online mailboxes, SharePoint Online sites, and OneDrive for Business locations, and import data into your Office 365 organization.
- The Retention feature in Office 365 can help you manage the lifecycle of email and documents by keeping the content you need and removing content after it's no longer required.
- Advanced Data Governance uses intelligence and machine-assisted insights to help you find, classify, set policies on, and take action to manage the lifecycle of the data that is most important to your organization.
- Information management policies in SharePoint Online enable you to control how long to retain content, to audit what people do with content, and to add barcodes or labels to documents.
- Journaling in Exchange Online can help you respond to legal, regulatory, and organizational compliance requirements by recording inbound and outbound email communications.

Data classification

Data classification is an important part of any data governance plan. Adopting a classification scheme that applies throughout your organization can be particularly helpful for responding to data subject requests, because it enables you to identify more readily and process personal data requests.

Today, we provide guidance and tools to help you work through the complexities of data classification.

Azure

The Data Classification whitepaper provides specific guidance for data classification for Azure and walks you through the principles behind data classification techniques, the process, terminology, and implementation. The documentation contains a wealth of other information and links.

Dynamics 365

The Dynamics 365 (online) security and compliance planning guide provides comprehensive guidance on understanding the key compliance and security considerations associated with planning for a deployment of Dynamics 365 (online) in environments that include enterprise directory integration services such as directory synchronization and single sign-on. It includes information on data privacy and confidentiality policies, data classification, and impact.

Enterprise Mobility + Security (EMS)

Azure Information Protection can help you classify and label your data at the time of creation or modification. Protection (encryption plus authentication plus use rights) or visual markings can then be applied to sensitive data. Classification labels and protection are persistent, traveling with the data so that it's identifiable and protected at all times—regardless of where it's stored or with whom it's shared.

Office and Office 365

- Data Loss Prevention (DLP) in Office and Office 365 can identify over 80 common sensitive data types including financial, medical, and personally identifiable information. In addition, DLP allows organizations to configure actions to be taken upon identification to protect sensitive information and prevent its accidental disclosure.
- Advanced Data Governance uses intelligence and machine-assisted insights to help you find, classify, set policies on, and take action to manage the lifecycle of the data that is most important to your organization. Classify data based on automatic analysis and policy recommendations, then apply actions to preserve data in-place or purge what's necessary. In-place data as well as third-party data sources can be ingested into Office 365 and classified by message type. Message type classification allows for the search,

sort, and export of the various data sources, which eases the process of performing ediscovery reviews.

Windows and Windows Server

The Microsoft Data Classification Toolkit for Windows Server 2012 R2 provides sample search expressions and rules that you can use to assist compliance activities conducted by your organization's IT professionals, auditors, accountants, attorneys, and other compliance professionals.

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

Organizations increasingly understand the importance of information security—but the GDPR raises the bar. It requires that organizations take appropriate technical and organizational measures to protect personal data from loss or unauthorized access or disclosure.

Protecting your data

Data security is a complex area. There are many types of risk to identify and consider—ranging from physical intrusion or rogue employees to accidental loss or hackers. Building risk management plans and taking risk mitigation steps, such as password protection, audit logs, and encryption, can help you ensure compliance.

The Microsoft cloud is specifically built to help you understand risks and to defend against them, and is more secure than on-premises computing environments in many ways. For example, our datacenters are certified to internationally recognized security standards; protected by 24-hour physical surveillance; and have strict access controls.

How we secure our cloud infrastructure is only part of a comprehensive security solution and each of our products, either in the cloud or on-premises, have security features to help you secure your data.

Azure

The following Azure services and tools will help you protect personal data in your cloud environment:

- Azure Security Center provides you with visibility and control over the security of your Azure resources. It continuously monitors your resources and provides helpful security recommendations. It enables you to define policies for your Azure subscriptions and resource groups based on your company's security requirements, the types of applications that you use, and the sensitivity of your data. It also uses policy-driven security recommendations to guide service owners through the process of implementing needed controls—for example, enabling antimalware or disk encryption for your resources. Security Center also helps you rapidly deploy security services and appliances from Microsoft and partners to strengthen the protection of your cloud environment.
- Data encryption in Azure secures your data at rest and in transit. You can, for example, 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 Windows and Linux virtual machines. Data is protected in transit between an application and Azure so that it always remains highly secure.

- Azure Key Vault enables you to safeguard your cryptographic keys, certificates, and passwords that help protect your data. Key Vault uses hardware security modules (HSMs) and is designed so that you maintain control of your keys and therefore your data, including ensuring that Microsoft cannot see or extract your keys. You can monitor and audit use of your stored keys with Azure logging, and import your logs into Azure HDInsight or your security information and event management (SIEM) system for additional analysis and threat detection.
- Microsoft Antimalware for Azure Cloud Services and Virtual Machines is a free real-time protection capability that helps you identify and remove viruses, spyware, and other malicious software that target data theft, with configurable alerts that let you know when known malicious or unwanted software attempts to install itself or run on your Azure systems.

Dynamics 365

You can use the security concepts for Dynamics 365 to protect the data integrity and privacy in a Dynamics 365 organization. You can combine business units, role-based security, record-based security, and field-based security to define the overall access to information that users have in your Dynamics 365 organization.

- Role-based security in Dynamics 365 allows you to group together a set of privileges that limit the tasks that can be performed by a given user. This is an important capability, especially when people change roles within an organization.
- Record-based security in Dynamics 365 allows you to restrict access to specific records.
- Field-level security in Dynamics 365 allows you to restrict access to specific high-impact fields, such as personally identifiable information.

Enterprise Mobility + Security (EMS)

In the majority of data breaches, attackers gain corporate network access through weak, default, or stolen user credentials. Our security approach starts with identity protection at the front door with risk-based conditional access.

- Azure Active Directory (Azure AD) in Enterprise Mobility + Security helps you protect your organization at the access level by managing and protecting your identities—including your privileged and non-privileged identities. Azure AD provides one protected common identity for accessing thousands of apps. Azure AD Premium features MultiFactor Authentication (MFA), which is access control based on device health, user location, identity and sign-in risk, and holistic security reports, audits, and alerts. Azure

AD Privileged Identity Management (PIM) helps discover, restrict, and monitor privileged identities and their access to resources through a security wizard, reviews, and alerts. This enables scenarios such as time-limited "just in time" and "just enough administration" access.

Enterprise Mobility + Security provides deep visibility into user, device, and data activity onpremises and in the cloud and helps you protect your data with strong controls and enforcement.

- Azure Information Protection helps extend control over your data throughout the complete data lifecycle—from creation to storage on-premises and in cloud services, to sharing internally or externally, to monitoring the distribution of files, and finally to responding to unexpected activities.
- Cloud App Security provides deep visibility and strong data controls for the software as a service (SaaS) and cloud apps your employees are using, so you can gain complete context and start controlling data with granular-level policies.
- Microsoft Intune provides mobile device management, mobile application management, and PC management capabilities from the cloud. Using Intune, you can provide your employees with access to corporate applications, data, and resources from virtually anywhere on almost any device, while helping to keep corporate information highly secure.

Office and Office 365

The Office 365 platform incorporates security at every level, from application development to physical datacenters to end-user access. Office 365 applications include both built-in security features that simplify the process of protecting data and the flexibility for you to configure, manage, and integrate security in ways that make sense for your unique business needs. The Office 365 compliance framework has over 1,000 controls that enable us to keep Office 365 up to date with evolving industry standards, including over 50 certifications or attestations.

Many security controls are available by default. SharePoint and OneDrive for Business, for instance, both use encryption for data in transit and at rest. In addition, you may configure and deploy digital certificates to obfuscate personal data, and you can use Office Access controls to grant and restrict access to personal data.

Office 365 offers other features that help you safeguard data and identify when a data breach occurs:

- Secure Score gives you insights into your security position and what features are available to reduce risk while balancing productivity and security.

- Advanced Threat Protection (ATP) for Exchange Online helps protect your email against new, sophisticated malware attacks in real time. It also allows you to create policies that help prevent your users from accessing malicious attachments or malicious websites linked through email. ATP for Exchange Online includes protection against unknown malware and viruses, time-of-click protection against malicious URLs, and rich reporting and URL trace capabilities.
- Information Rights Management (IRM) helps you and your users prevent sensitive information from being printed, forwarded, saved, edited, or copied by unauthorized individuals. With IRM in SharePoint Online, you can limit the actions that users can take on files that have been downloaded from lists or libraries, such as printing copies of the files or copying text from them. With IRM in Exchange Online, you can help prevent sensitive information in email messages and attachments from leaking via email, online and offline.
- Mobile Device Management (MDM) for Office 365 lets you set up policies and rules to help secure and manage your users' enrolled iPhones, iPads, Android devices, and Windows phones. For example, you can remotely wipe a device and view detailed device reports. Office 365 also uses multi-factor authentication to help provide extra security.

SQL Server and Azure SQL Database

SQL Server and Azure SQL Database provide controls for managing database access and authorization at several levels:

- Azure SQL Database firewall limits access to individual databases within your Azure SQL Database server by restricting access exclusively to authorized connections. You can create firewall rules at the server and database levels, specifying IP ranges that are approved to connect.
- SQL Server authentication helps you ensure that only authorized users with valid credentials can access your database server. SQL Server supports both Windows authentication and SQL Server logins. Windows authentication offers integrated security, and is recommended as the more secure option, where the authentication process is entirely encrypted. Azure SQL Database supports Azure Active Directory authentication, which offers a single sign-on capability and is supported for managed and integrated domains.
- SQL Server authorization enables you to manage permissions according to the principle of least privilege. SQL Server and SQL Database use role-based security, which supports granular control of data permissions via the management of role memberships and object-level permissions.

- Dynamic data masking (DDM) is a built-in capability that can be used to limit sensitive data exposure by masking the data when accessed by non-privileged users or applications. Designated data fields are masked in query results on the fly, while the data in the database remains unchanged. DDM is simple to configure and requires no changes to the application. For users of Azure SQL Database, dynamic data masking can automatically discover potentially sensitive data and suggest the appropriate masks to be applied.
- Row-level security (RLS) is an additional built-in capability that enables SQL Server and SQL Database customers to implement restrictions on data row access. RLS can be used to enable fine-grained access over rows in a database table, for greater control over which users can access which data. Since the access restriction logic is located in the database tier, this capability greatly simplifies the design and implementation of application security.

SQL Server and SQL Database provide a powerful set of built-in capabilities that safeguard data and identify when a data breach occurs:

- Transparent data encryption protects data at rest by encrypting the database, associated backups, and transaction log files at the physical storage layer. This encryption is transparent to the application, and uses hardware acceleration to improve performance.
- Transport Layer Security (TLS) provides protection of data in transit on SQL Database connections.
- Always Encrypted is an industry-first feature that is designed to protect highly sensitive data in SQL Server and SQL Database. Always Encrypted allows clients to encrypt sensitive data inside client applications and never reveal the encryption keys to the database engine. The mechanism is transparent to applications, as encryption and decryption of data is done transparently in an Always Encrypted–enabled client driver.
- Auditing for SQL Database and SQL Server audit track database events and write them to an audit log. Auditing enables you to understand ongoing database activities, as well as analyze and investigate historical activity to identify potential threats or suspected abuse and security violations.
- SQL Database Threat Detection detects anomalous database activities indicating potential security threats to the database. Threat Detection uses an advanced set of algorithms to continuously learn and profile application behavior, and notifies immediately upon detection of an unusual or suspicious activity. Threat Detection can help you meet the data breach notification requirement of the GDPR.

Windows and Windows Server

Windows 10 and Windows Server 2016 include industry-leading encryption, antimalware technologies, and identity and access solutions that enable you to move from passwords to more secure forms of authentication:

- Windows Hello is a convenient, enterprise-grade alternative to passwords that uses a natural (biometrics) or familiar (PIN) method to validate identity, providing the security benefits of smartcards without the need for additional peripherals.
- Windows Defender Antivirus is a robust antimalware solution that works right out of the box to help you stay protected. Windows Defender Antivirus is quick to detect and protect against emerging malware, and it can immediately help protect your devices when a threat is first observed in any part of your environment.
- Device Guard allows you to lock down your devices and servers to protect against new and unknown malware variants and advanced persistent threats. Unlike detection-based solutions such as antivirus programs that need constant updating to detect the latest threats, Device Guard locks down devices so they can only run the authorized applications you choose, which is an effective way to combat malware.
- Credential Guard is a feature that isolates your secrets on a device, like your single signon tokens, from access even in the event of a full Windows operating system compromise. This solution fundamentally prevents the use of hard-to-defend attacks such as "pass the hash."
- BitLocker Drive Encryption in Windows 10 and Windows Server 2016 provides enterprisegrade encryption to help protect your data when a device is lost or stolen. BitLocker fully encrypts your computer's disk and flash drives to prevent unauthorized users from accessing your data.
- Windows Information Protection picks up where BitLocker leaves off. While BitLocker protects the entire disk of a device, Windows Information Protection protects your data from unauthorized users and applications running on a machine. It also helps you prevent data from leaking from business to non-business documents or to locations on the web.
- Shielded Virtual Machines allow you to use BitLocker to encrypt disks and virtual machines (VMs) running on Hyper-V, to prevent compromised or malicious administrators from attacking the contents of protected VMs.
- Just Enough Administration and Just in Time Administration allows administrators to perform their regular jobs and actions, while enabling you to limit the scope of capabilities and time that administrators can run. If a privileged credential is compromised, the scope of damage is severely limited. This technique provides

administrators with only the level of access they require during the time they are working on the project.

Detecting and responding to data breaches

In certain cases, the GDPR requires that if a data breach occurs, organizations need to rapidly notify regulators. In some cases, organizations will also need to notify the affected data subjects. In order to meet this requirement, organizations will benefit from being able to monitor for and detect system intrusions.

For incidents where we hold some or all of the responsibility to respond, we have established detailed Security Incident Response Management processes such as outlined for Azure and Office 365.

In addition, we outline how we work collaboratively with our customers under a Shared Responsibility Model outlined in the Shared Responsibilities in Cloud Computing white paper.

Once you have detected a potential breach, we recommend, and use for our own incident response program, a four-step process:

- Assess the impact and severity of the event. Based on evidence, the assessment may or may not result in further escalation to a Cybersecurity / Data Protection response team.
- Conduct a technical or forensic investigation, and identify containment, mitigation, and workaround strategies. If the Cybersecurity / Data Protection team believes that personal data may have become exposed to an unlawful or unauthorized individual, a notification process begins in parallel as called for in the GDPR.
- Create a recovery plan to mitigate the issue. Crisis containment steps such as quarantining affected systems should occur immediately and in parallel with diagnosis. Longer term mitigations may be planned which occur after the immediate risk has passed.
- Create a post-mortem that outlines the details of the incident, with the intention to revise policies, procedures, and processes to prevent a reoccurrence of the event. This stage is in line with Article 31 of the GDPR to record the facts surrounding the breach, its effects, and the remedial action taken.

Azure

Protecting personal data in your systems and reporting on and reviewing for compliance are key requirements of the GDPR. The following Azure services and tools will help you meet these GDPR obligations:

- Integrated services with Azure enable you to more quickly and easily understand the overall security posture as well as detect and investigate threats to your cloud environment. Azure Security Center employs advanced security analytics. Breakthroughs in big data and machine learning technologies are used to evaluate events across the entire cloud fabric—detecting threats that would be impossible to identify using manual approaches, and predicting the evolution of attacks. These security analytics include:
    - Integrated threat intelligence, which looks for known bad actors by using global threat intelligence from Microsoft products and services, the Microsoft Digital Crimes Unit (DCU), the Microsoft Security Response Center (MSRC), and external feeds.
    - Behavioral analytics, which applies known patterns to discover malicious behavior.
    - Anomaly detection, which uses statistical profiling to build a historical baseline. It alerts on deviations from established baselines that conform to a potential attack vector.

  Additionally, Security Center provides prioritized security alerts that give you insights into the attack campaign, including related events and impacted resources.

    - Azure Log Analytics provides configurable security auditing and logging options that can help 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. It helps facilitate quick response and thorough investigation for any security events.

Dynamics 365

We regularly maintain and update Dynamics 365 (online) to ensure security, performance, and availability, and to provide new features and functionality. From time to time, we also respond to service incidents. For each of these activities, the Dynamics 365 administrator for your organization receives email notifications. During a service incident, a Dynamics 365 (online) customer service representative may also call and follow up with an email. See the full details of our policies and communications for Dynamics 365 on TechNet.

Enterprise Mobility +Security (EMS)

Our comprehensive threat intelligence uses cutting-edge behavioral analytics and anomaly detection technologies to uncover suspicious activity and pinpoint threats—both on-premises

and in the cloud. That includes known malicious attacks (such as Pass the Hash, Pass the Ticket) and security vulnerabilities in your system. You can take immediate action against detected attacks and streamline recovery with powerful support. Our threat intelligence is enhanced with the Microsoft Intelligent Security Graph, driven by a vast number of datasets and machine learning in the cloud:

- Microsoft Advanced Threat Analytics (ATA) is an on-premises product to help IT security professionals protect their organization from advanced targeted attacks by automatically analyzing, learning, and identifying normal and abnormal entity (user, devices, and resources) behavior. ATA identifies advanced persistent threats (APTs) on- premises by detecting suspicious user and entity behavior (devices and resources), using machine learning and information in on-premises Active Directory, SIEM systems, and Windows Events logs. It also detects known malicious attacks (such as Pass the Hash). Finally, it provides a simple attack timeline with clear and relevant attack information, so you can quickly focus on what is important.
- Cloud App Security provides threat protection for your cloud applications that's enhanced with vast Microsoft threat intelligence and research. You can identify high-risk usage, security incidents, and detect abnormal user behavior to prevent threats. Cloud App Security advanced machine learning heuristics learn how each user interacts with each SaaS application and, through behavioral analysis, assesses the risks in each transaction. This includes simultaneous logins from two countries, the sudden download of terabytes of data, or multiple failed login attempts that may signify a brute force attack.
- Azure Active Directory (Azure AD) Premium provides identity-level threat detection in the cloud. Azure AD monitors application usage and protects your business from advanced threats with security reporting and monitoring. Access and usage reports provide visibility into the integrity and security of your organization's directory. Also, Azure AD provides identity protection with notifications, analysis, and recommended remediation.

Office and Office 365

Office 365 features several capabilities that help you identify and respond when a data breach occurs:

- Threat Intelligence helps you proactively uncover and protect against advanced threats in Office 365. Deep insights into threats—available in part because of Microsoft's global presence, the Intelligent Security Graph, and input from cyber threat hunters—help you quickly and effectively enable alerts, dynamic policies, and security solutions.
- Advanced Security Management enables you to identify high-risk and abnormal usage, alerting you to potential breaches. In addition, it allows you to set up activity policies to

track and respond to high-risk actions and suspicious activity. And you can also get productivity app discovery, which lets you use the information from your organization's log files to understand and act on your users' app usage in Office 365 and other cloud apps.

- Advanced Threat Protection for Exchange Online helps protect your email against new, sophisticated malware attacks in real time. It also allows you to create policies that help prevent your users from accessing malicious attachments or malicious websites linked through email.

SQL Server and Azure SQL Database

SQL Server and SQL Database provide a powerful set of built-in capabilities that identify when a data breach occurs:

- Auditing for SQL Database and SQL Server audit track database events and write them to an audit log. Auditing enables you to understand ongoing database activities, as well as analyze and investigate historical activity to identify potential threats or suspected abuse and security violations.
- SQL Database Threat Detection detects anomalous database activities indicating potential security threats to the database. Threat Detection uses an advanced set of algorithms to continuously learn and profile application behavior, and notifies immediately upon detection of an unusual or suspicious activity. Threat Detection can help you meet the data breach notification requirement of the GDPR.

Windows and Windows Server

Windows Defender Advanced Threat Protection (ATP) enables your security operations teams to detect, investigate, contain, and respond to data breaches on your network. With Windows Defender ATP, you gain advanced breach detection, investigation, and response capabilities across all your endpoints with up to 6 months of historical data, even when endpoints are offline, outside of the network domain, have been reimaged, or no longer exist. Windows Defender ATP helps you fulfill a key requirement of the GDPR, which is having clear procedures for detecting, investigating, and reporting data breaches.

Report: Execute on data requests, report data breaches, and keep required documentation

The GDPR sets new standards in transparency, accountability, and record-keeping. You will need to be more transparent about not only how you handle personal data, but also how you actively maintain documentation defining your processes and use of personal data.

Record-keeping

Organizations processing personal data will need to keep records about the purposes of processing; the categories of personal data processed; the identity of third parties with whom data is shared; whether (and which) third countries receive personal data, and the legal basis of such transfers; organizational and technical security measures; and data retention times applicable to various datasets. One way to achieve this is using auditing tools, which can help to ensure that any processing of data—whether it be collection, use, sharing, or otherwise—is tracked and recorded.

Microsoft cloud services offer embedded auditing services that can help you meet this standard.

Azure, Office 365, and Dynamics 365

In the Service Trust Portal, you can find comprehensive information about the various Azure, Office 365, and Dynamics 365 compliance, security, privacy, and trust offerings, including reports and attestations. Third-party independent audit and GRC (governance, risk management, and compliance) assessment reports help you to stay up to date on how Microsoft cloud services comply with global standards that matter to your organization. Trust documents can help you understand how Microsoft cloud services protect your data and how you can manage data security and compliance for your cloud services.

Azure

Auditing and logging of security-related events, and related alerts, are important components in an effective data protection strategy.

Azure logging and auditing capabilities enable you to:

- Create an audit trail for applications deployed in Azure and virtual machines created from the Azure Virtual Machines Gallery.
- Perform centralized analysis of large data sets by collecting security events from Azure infrastructure as a service (IaaS) and platform as a service (PaaS). You can then use Azure HDInsight to aggregate and analyze these events, and export them to on-premises SIEM systems for ongoing monitoring.

- Monitor access and usage reporting by taking advantage of Azure logging of administrative operations, including system access, to create an audit trail in case of unauthorized or accidental changes. You can retrieve audit logs for your Azure Active Directory tenant, and view access and usage reports.
- Export security alerts to on-premises SIEM systems by using Azure Diagnostics, which can be configured to collect Windows security event logs and other security-specific logs.
- Get third-party security monitoring, reporting, and alert tools from the Azure Marketplace.

Microsoft Azure Monitor enables organizations to easily view and manage all their data monitoring tasks from a central dashboard. You get detailed, up-to-date performance and utilization data, access to the activity log that tracks every API call, and diagnostic logs that help you trace issues in your Azure resources. In addition, you can set up alerts and take automated actions. Azure Monitor integrates with your existing tools, so you get rich end-to-end monitoring and analytics by combining Azure Monitor with the analysis tools you are already familiar with.

Office and Office 365

- Service Assurance in the Office 365 Security & Compliance Center gives you deep insights for conducting risk assessments, with details on Microsoft Compliance reports and transparent status of audited controls, including:
- Microsoft security practices for customer data that is stored in Office 365.
- Independent third-party audit reports of Office 365.
- Implementation and testing details for security, privacy, and compliance controls that help customers comply with standards, laws, and regulations across industries, such as ISO 27001 and ISO 27018, as well as the Health Insurance Portability and Accountability Act (HIPAA).
- Office 365 audit logs allow you to monitor and track user and administrator activities across workloads in Office 365, which help with early detection and investigation of security and compliance issues. Use the Office 365 Audit log search page to start recording user and admin activity in your organization. After Office 365 prepares the audit log, you can search it for a broad range of activities, including uploads to OneDrive or SharePoint Online or user password resets. Exchange Online can be set up to track changes that are made by administrators, and track whenever a mailbox is accessed by someone other than the person who owns the mailbox.

- Customer Lockbox gives you authority over how a Microsoft support engineer may access your data during a help session. In cases where the engineer requires access to your data to troubleshoot and fix an issue, Customer Lockbox allows you to approve or reject the access request. If you approve it, the engineer is able to access the data. Each request has an expiration time, and once the issue is resolved, the request is closed, and access is revoked.

Enterprise Mobility + Security (EMS)

Azure Information Protection provides rich logging and reporting to analyze how sensitive data is distributed. Document tracking allows users and admins to monitor activities on shared data and revoke access in unexpected events. Azure Information Protection also provides capabilities to analyze unstructured data residing in file shares, SharePoint sites and libraries, online repositories, and desktop or laptop drives. With access to the files, you can scan the contents of each file and determine whether certain classes of personal data exist in the file. You can then classify and tag with a label each file based on the kind of data present. Additionally, you can generate reports of this process, with information about the files scanned, classification policies that matched, and the label that was applied.

Windows and Windows Server

Windows Event Log provides rich event logging capabilities that enable administrators to view logged information about operating system, application, and user activities. This log system can be configured to audit detailed user and application actions including access to files, application usage, and policies changes, just to name a few. The Windows Event Log also enables administrators to forward events from clients and servers to a central location for reporting and auditing purposes.

Reporting tools and documentation of cloud services

As with any other database or system handling personal data, your use of cloud services should be well recorded and well understood by your organization. For example, your organization will need to understand the personal data held by service providers on your organization's behalf; the contractual relationship governing those service providers; and what happens to the data when a service relationship ends.

We help you manage this information by maintaining simple and clear reporting tools about your account in the Microsoft cloud, along with extensive documentation about our cloud services, how they work, and our contractual relationship with you.

Notifying data subjects

The GDPR will change data protection requirements and employ stricter obligations for data processors and data controllers regarding notice of personal data breaches that result in a risk to individual rights and freedoms. Under the new regulation, as defined in Articles 17, 31, and 32, the Data Processor must notify the Data Controller of any such personal data breach after having become aware of it without undue delay.

Once aware of a breach, the Data Controller must notify the relevant data protection authority within 72 hours. If the breach is likely to result in a high risk to the rights and freedoms of individuals, controllers will also need to notify affected individuals without undue delay. This means that if you are using a Data Processor in your role as Data Controller, you need to make sure you have a clear set of expectations built into your contracts around potential breach notifications.

For incidents where Microsoft holds some or all of the responsibility to respond, we have established detailed Incident Security Incident Response Management processes such as outlined for Azure, Office 365, and Dynamics 365. We also back up our GDPR commitments in our contract language.

Microsoft products and services—such as Azure, Dynamics 365, Enterprise Mobility + Security, Office 365, and Windows 10—have solutions available today to help you detect and assess security threats and breaches and meet the GDPR's breach notification obligations.

Handling data subject requests

Among the most significant elements of the GDPR are the rights of the "data subject" stipulated in the Articles under Section 2: Information and Access to Data, Section 3: Rectification and Erasure, and Section 4: Right to Object and Automated Individual Decision Making.

These obligations may have implications on your IT environment and operations as a Data Controller, and the IT environment and operations of any service providers you engage as Data Processors.

Proper data governance has been a key element of privacy laws and is advocated in most data protection and privacy laws and regulations. One key element of governance under the GDPR is the establishment of a Data Protection Officer (DPO) in specific circumstances outlined in Articles 35, 36, and 37. The DPO needs to be involved in all issues which relate to the protection of personal data.

A second important element of GDPR governance is the completion of the Data Protection Compliance Review generating a Data Protection Impact Assessment (DPIA) under the direction of a DPO. Article 35-*11: Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.*.

The Microsoft Trust Center provides information about the ways in which we can support your journey, including a special section on Microsoft's views and commitments around the GDPR.