Microsoft Trust Center

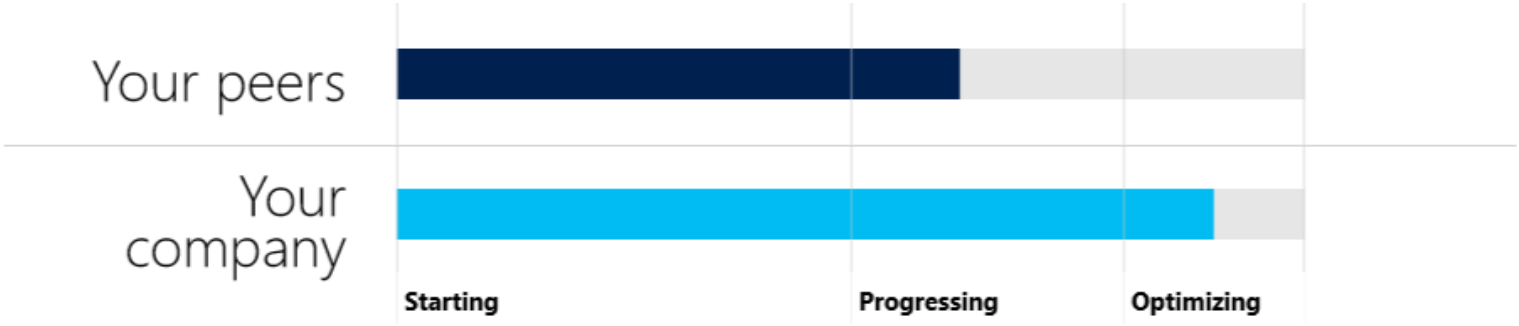
Microsoft GDPR ASSESSMENT TOOL

Results

The General Data Protection Regulation (GDPR) strengthens the right of individuals in the European Union (EU) to control their personal data and requires organizations to bolster their privacy and data protection measures. It applies to organizations established in the European Union (EU) as well as organizations-wherever they are located-that offer goods and services to the EU or monitor the behavior of individuals in the EU. Enforcement of the regulation begins May 25, 2018. The following questions are meant to assist organizations by identifying technologies and steps that can be implemented to simplify their GDPR compliance efforts.

Discover

Detailed Results and Resources



Question 1/2

Search for and identify personal data. The GDPR has many requirements about how you collect, store, and use personal data, making it necessary to first identify the personal data you hold about data subjects.How much of the personal data about data subjects under your organization's control have you identified?

Your answers : All/Nearly All

Offering	How it helps you become GDPR compliant
Azure	Azure provides you with several tools for search in Azure. Azure Data Catalog provides a service in which many common data sources can be registered, tagged, and searched for personal data. Azure Search allows you to locate data across user-defined indexes. You can also search for user accounts in Azure Active Directory. Create a free Azure account
Dynamics 365	Dynamics 365 provides multiple methods for you to search for personal data within records such as: Advanced Find, Quick Find, Relevance Search, and Filters. These functions all enable you to identify personal data. See plans and pricing for Dynamics 365
EMS	Enterprise Mobility + Security (EMS) provides you with multiple tools that enable you to identify personal data. Azure Information Protection (AIP) helps you identify, classify, and label personal data at the time of creation or modification. Cloud App Security offers Cloud Discovery functionality that can use your traffic logs to discover and analyze the cloud apps in use in your organization. Getting started with Enterprise Mobility + Security
Office 365	Office 365 includes powerful tools to identify personal data across Exchange Online, SharePoint Online, OneDrive for Business, and Skype for Business environments.Content Search allows you to query for personal data using relevant keywords, file properties, or built-in templates. Advanced eDiscovery lets you identify relevant data faster and with better precision than traditional keyword searches by finding near-duplicate files, reconstructing email threads, and identifying key themes and data relationships. See plans and pricing for Office 365 Business
SQL	The SQL Server family of products and services enables you to use queries, customized tools or services, and metadata views to search for and identify stored personal data in databases. Full-Text Search allows you to run full-text queries against character-based data in SQL Server tables.Free trial evaluation of SQL Server
Windows 10/Windows Server	Windows 10 and Windows Server 2016 have tools to locate personal data, including PowerShell, which can help you find data housed in local and connected storage as well as search for files and items by file name, properties, and full-text contents for some common file types and data types. Try Windows Server 2016 Try Windows 10 Enterprise edition for free

Question 2/2

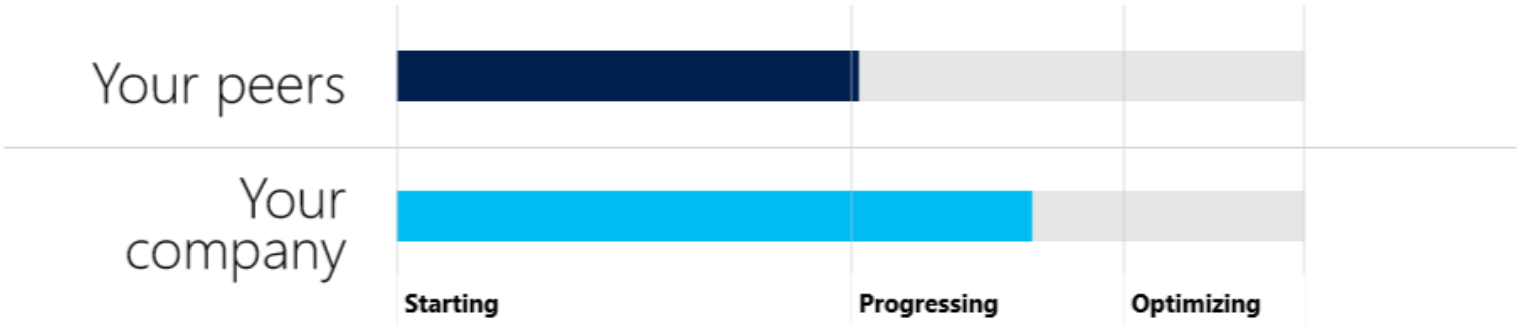
Classify personal data. The GDPR has many requirements to enable the rights of data subjects. This makes it necessary to classify personal data.How confident are you in the tools your organization currently has to classify personal data?

Your answers : Mostly confident

Offering	How it helps you become GDPR compliant
Azure	Azure provides tools that can be used to classify data. Customer applications or services built on Azure infrastructure may be able to use Azure Information Protection labels to apply classifications to sensitive data. Azure data sources can be registered with Azure Data catalog, and then annotated manually or with a REST API in accordance with your classification standard. Create a free Azure account
Dynamics 365	Dynamics 365 offers flexibility to build out an application extension around data classification. Using the Entity and Field levels, customers can configure Forms and Views to look for personal information based on GDPR requests. At the Row level, data classification can be implemented using solution customization. See plans and pricing for Dynamics 365
EMS	Enterprise Mobility + Security (EMS) offers you a variety of tools to facilitate data classification, as well as services to trace and locate data. Azure Information Protection helps you classify and label data so that persistent protection can be applied to sensitive data. You can configure policies to trigger some actions based on sensitivity labels - these actions can be automatic encryption of data or adding visual markings such as a headers, footers, or watermarks. Cloud App Security lets you investigate files and set policies based on Azure Information Protection classification labels, enabling greater visibility and control of personal data in the cloud.Getting started with Enterprise Mobility + Security
Office 365	Office 365 has multiple tools to classify data and assign protections such as: access restrictions, encryption, and policies to enforce deletion and retention policies. Advanced Data Governance helps you identify, classify, and manage data and sensitive data, as well as apply retention and deletion policies to help protect data. Office 365 data loss prevention (DLP) policies can automatically apply restrictions on access to and sharing of data.See plans and pricing for Office 365 Business
SQL	The SQL Server family of products and services includes the Extended Properties feature that lets you create custom classification labels and apply them to sensitive data housed in SQL Server databases. Using Extended Properties, you can add custom properties to database objects that denote classification levels for sensitive data. Free trial evaluation of SQL Server
Windows 10/Windows Server	Windows 10 and Windows Server 2016 both support Azure Information Protection, which lets you classify and label data so that persistent protection can be applied to sensitive data. You may also deploy automatic file classification in Active Directory, creating personal data classification rules, and then assigning values to the resource properties for files on a file server. Try Windows Server 2016 Try Windows 10 Enterprise edition for free

Manage

Detailed Results and Resources



Question 1/9

Data Governance. To manage data and support the rights of data subjects under the GDPR, organizations should implement a data governance program.Would you say that your organization has a data governance program in place that meets the demands of the GDPR?

Your answers : Agree

Offering	How it helps you become GDPR compliant
Azure	Azure includes features that can help you enable data governance. Azure Active Directory is a solution that manages identities and controls access to Azure as well as on-premises and other cloud resources, data, and applications. Azure Active Directory Privileged Identity Management enables you to minimize the number of people who have access to certain information such as personal data. Azure Role-Based Access Control helps you manage access to Azure resources by enabling access based on a userâ€™s assigned role. Create a free Azure account
Dynamics 365	Dynamics 365 provides you with a set of features to manage the access of both users and groups to personal data. Role-based security allows you to group together a set of privileges that limits the tasks a user can perform. Record-based security lets you restrict access to specific records. Field-level security lets you restrict access to specific high-impact fields, such as those containing personally identifiable information. See plans and pricing for Dynamics 365
EMS	Enterprise Mobility + Security (EMS) provides several features that can be used as part of a data governance plan, including: Azure Information Protection, which helps you classify and label data so that persistent protection and governance policies can be applied for sensitive or personal data; and Cloud App Security, which can leverage the classification labels set by AIP to enforce automatic governance actions such as quarantining files and revoking the ability to share files.Getting started with Enterprise Mobility + Security
Office 365	Office 365 gives you multiple tools to enable data governance by classifying, labeling, and placing restrictions on data. Advanced Data Governance provides proactive policy recommendations and automatic data classifications that enable you to identify, classify, and manage personal data and sensitive data as well as set and enforce retention and deletion policies. The Labels function lets you automatically classify personal data and sensitive data across the organization for governance, and enforce retention and deletion rules based on that classification. Information Rights Management can help prevent unauthorized persons from accessing personal data in Office 365.See plans and pricing for Office 365 Business
SQL	The SQL Server family of products and services provides you with tools that can help enable a data governance program. SQL Server Authentication and Azure Active Directory (AAD) Authentication help you ensure that only authorized users with valid credentials can access the database server. Individuals or groups can be mapped to roles in the database, and assigned permissions related to specific functions, such as connecting from an application. Row-Level Security enables you to control access to rows in a database table based on user settings, and Dynamic Data Masking limits exposure of sensitive data by masking it to non-privileged users. Free trial evaluation of SQL Server
Windows 10/Windows Server	Windows 10 and Windows Server 2016 both support Azure Rights Management Service in Azure Information Protection, which lets you assign and enforce persistent restrictions on sharing files that contain personal data, as well as enforce encryption requirements. Dynamic Access Control lets you apply and enforce access-control permissions and restrictions based on defined rules that can include the sensitivity of the resources, the job or role of the user, and the configuration devices that access resources. Windows permissions enables you to manage the process of authorizing users, groups, and computers to access objects on a network. Try Windows Server 2016 Try Windows 10 Enterprise edition for free

Question 2/9

Provide detailed notice of processing to data subjects. The GDPR requires that controllers be transparent with data subjects about the intended processing of personal data.Which of the following GDPR requirements do your existing privacy notice meet? (Check all that apply)

Your answers : Identity and contact details of the data controller,State when and how information is shared with third parties,Any recipient or categories of recipients of the personal data

Offering	How it helps you become GDPR compliant
Dynamics 365	Dynamics 365 Customer Engagement includes the ability to use Portals to display custom privacy notices with detailed information, either through a form or on a sign in screen on both internal and external Portals. While Dynamics 365 can provide a platform capable of hosting external-facing privacy notices, it is the responsibility of the customer to ensure that the specific language of the notice meets their obligations under the GDPR.See plans and pricing for Dynamics 365
EMS	Enterprise Mobility + Security includes Intune, which allows controllers to present their own customized privacy notice and contact information to end users. Further, Intune allows controllers to present their own custom terms and conditions for a click-through acceptance. Getting started with Enterprise Mobility + Security

Question 3/9

Discontinue processing on request: The GDPR requires that companies give data subjects the right to restrict or object to the processing of data.In how many cases would your organization be able to do this right now?

Your answers : Most

Offering	How it helps you become GDPR compliant
Azure	Microsoft assists Azure customers in addressing requests by data subjects to stop the processing of personal data by providing Azure customers with the ability to export and delete customer data at any time. Customer data typically includes personal data, including Azure customers' data subjects in Azure Active Directory (AAD) and the content relating to data subjects in Azure Storage, SQL Database, and any other Azure service that stores content. Create a free Azure account
Office 365	Office 365 allows you to run a PowerShell cmdlet that will disable data subject access to target services to prevent additional processing of personal data. See plans and pricing for Office 365 Business
SQL	The SQL Server family of products and services provides you with tools that can be used to discontinue the processing of data subjects. The Extended Properties feature allows you to add custom properties to database objects and tag data as "Discontinued" to support application logic to prevent the processing of the associated personal data. Row-Level Security enables you to define policies to restrict access to data to discontinue processing. Free trial evaluation of SQL Server
Windows 10/Windows Server	Windows Server 2016 allows you to use Windows Search or PowerShell to discontinue the processing of files containing personal data that are housed in local or shared storage using file permissions functionality. You can also meet the requests of data subjects to discontinue the processing of their personal data by revoking access to files that contain personal data. Try Windows Server 2016

Question 4/9

Obtain consent. The GDPR requires that before processing personal data, controllers must have a legal basis to do so, such as the affirmative consent of the data subject.In how many cases would your organization be able to obtain needed consents right now?

Your answers : Most

Offering	How it helps you become GDPR compliant
Azure	Azure lets you deploy technologies that may be used to obtain consent for relevant processing activities. Azure Active Directory (AAD) lets you request and obtain consent from users when accessing personal data that is already stored in AAD, Intune, or Office 365 services. Using AAD, data subjects can authenticate and grant affirmative consent to the use of their data. Microsoft customers can also use Azure SQL Database to record affirmative consent granted for processing activities. While Azure can provide a platform capable of hosting external-facing privacy notices, it is the responsibility of the customer to ensure that the specific language of the notice meets their obligations under the GDPR. Create a free Azure account
Dynamics 365	Dynamics 365 Customer Engagement offers Portals, which allows you to request and obtain consent prior to processing personal data. When collecting personal data through a form or login on an internal or external Portal, Dynamics 365 Customer Engagement allows you to create checkboxes or other elements that enable data subjects to indicate affirmative consent prior to submitting personal data. While Dynamics 365 can provide a platform capable of hosting external-facing privacy notices, it is the responsibility of the customer to ensure that the specific language of the notice meets their obligations under the GDPR.See plans and pricing for Dynamics 365
EMS	Enterprise Mobility + Security includes Intune, which allows controllers to present their own customized privacy notice and contact information to end users. Further, Intune allows controllers to present their own custom terms and conditions for a click-through acceptance. Getting started with Enterprise Mobility + Security
SQL	The Microsoft SQL relational database system can be used as a storage and processing technology to help manage the process of documenting consent for processing activities. Using other supporting technologies, Microsoft customers can dynamically populate SQL databases that documents the affirmative consent of a data subject obtained by a customer application. While SQL can provide a platform capable of hosting external-facing privacy notices, it is the responsibility of the customer to ensure that the specific language of the notice meets their obligations under the GDPR.Free trial evaluation of SQL Server

Question 5/9

Receive requests for the rectification, erasure, or transfer of personal data. The GDPR requires that a controller processing personal data must enable data subjects to exercise their rights by giving them a way to submit requests to rectify, erase, or transfer their personal data.In how many cases would your organization be able to enable data subjects to submit these requests?

Your answers : Some

Offering	How it helps you become GDPR compliant
Azure	Microsoft assists Azure customers in addressing requests by data subjects to stop the processing of personal data by providing Azure customers with the ability to export and delete customer data at any time. Customer data typically includes personal data, including Azure customers' data subjects in Azure Active Directory (AAD) and the content relating to data subjects in Azure Storage, SQL Database, and any other Azure service that stores content. Create a free Azure account
Dynamics 365	Dynamics 365 provides users with several tools to erase and edit personal data associated with data subjects as well as employee user accounts. Users can also manually track requests for rectification, erasure or transfer of personal data by using the support cases function. Users can create support cases to track and manage data subject rights requests. Additionally, actions taken during the lifecycle of the request can be tracked in the case, and then marked as resolved upon completion of the request. See plans and pricing for Dynamics 365
Office 365	Office 365 provides a suite of productivity applications that you can use to manually track requests for rectification, erasure, or transfer of personal data. For example, organizations can use SharePoint Online to manually track and manage data subject rights requests. Office 365 allows you to manage requests from data subjects in a central location by using Exchange Online mail flow rules to route mail with certain keywords, such as data subject rights or erasure, to specific mailboxes. This allows you to create a customized process for receiving, managing, and responding to these requests.See plans and pricing for Office 365 Business
SQL	The Microsoft SQL relational database system can be used as a storage and processing technology to document the requests of data subjects and the actions taken against requests. Free trial evaluation of SQL Server
Windows 10/Windows Server	Windows 10 and Windows Server 2016 provide a platform on which you can access applications that will enable the facilitation of data subject rights requests. Microsoft provides several applications that can help Windows customers to track and manage data subject rights requests. Dynamics 365 lets you create and manage support cases to track and manage data subject rights requests. Office 365 provides a suite of productivity applications that you can use to manually track requests for rectification, erasure, or transfer of personal data.Try Windows Server 2016 Try Windows 10 Enterprise edition for free

Question 6/9

Rectify inaccurate or incomplete personal data regarding data subjects. The GDPR requires controllers who process personal data to enable data subjects to request rectification of ";inaccurate personal data"; and the completion of ";incomplete personal data.";In how many cases would your organization be able to do this right now?

Your answers : Most

Offering	How it helps you become GDPR compliant
Azure	Azure provides you with multiple tools capable of rectifying inaccurate or incomplete personal data stored in Azure. You can identify files containing the inaccurate or incomplete personal data using Azure Search and then rectify the target personal data in the applicable service. You can also search for user data in an Azure Active Directory deployment, then edit data associated with the user account. Using SQL queries, Microsoft customers can correct inaccurate or incomplete data hosted in Azure SQL Database. Create a free Azure account
Dynamics 365	Dynamics 365 offers you several methods to rectify inaccurate or incomplete personal data. You can export data to Excel Online to quickly bulk edit multiple Dynamics 365 records, then reimport them to Dynamics 365. You can also amend personal data stored as Contacts by manually amending the data element containing the target personal data. You can also use the Dynamics 365 forms to edit a single row directly or modify multiple rows directly. See plans and pricing for Dynamics 365
Office 365	Office 365 provides you with multiple ways to rectify personal data, including Content Search to identify personal data, and PowerShell to rectify identified personal data. You can also manually rectify specific personal and contact data in the administrative functions of Office 365 Admin Center.See plans and pricing for Office 365 Business
SQL	The SQL Server family of products and services enables you to search for and rectify personal data located in tables using full-text, regular expression, or general queries against character-based data in SQL Server tables. You can also use SQL statements or other techniques to edit data to rectify inaccurate or incomplete personal data. You may also enable SQL Server Audit to verify changes to data. Free trial evaluation of SQL Server
Windows 10/Windows Server	Windows 10 and Windows Server 2016 both offer PowerShell, a tool that enables you to conduct string-matching or regex queries to search for personal data based on the targeted data's structure and pattern. Using PowerShell, you can search for files and items by file name, properties, and full-text content for some common file types and data types. Once identified, you can use PowerShell to manually rectify personal data for some file types or use their preferred editing mechanism. Try Windows Server 2016 Try Windows 10 Enterprise edition for free

Question 7/9

Erase personal data. Under the GDPR, all data subjects have the right to request the erasure of their personal data by controllers. In how many cases would your organization be able to do this right now?

Your answers : Some

Offering	How it helps you become GDPR compliant
Azure	Azure provides you with multiple tools for identifying and erasing personal data stored in Azure. You can identify files containing personal data using Azure Search and then erase the target personal data in the applicable service. You can also search for user data in an Azure Active Directory deployment, then delete data associated with the user account. Using SQL queries, Microsoft customers can erase data hosted in Azure SQL Database. Create a free Azure account
Dynamics 365	Dynamics 365 gives you several methods for erasing data regarding a data subject. Once the data is identified using Advanced Find, Dynamics 365 lets you locate the data and directly delete records.See plans and pricing for Dynamics 365
Office 365	Office 365 provides you with multiple ways to find and erase personal data, including Content Search to identify personal data, and PowerShell to erase identified personal data. You can also manually erase specific personal and contact data in the administrative functions of Office 365 Admin Center.See plans and pricing for Office 365 Business
SQL	The SQL Server family of products and services enables you to search for and erase personal data located in tables using full-text, regular expression, or general queries against character-based data in SQL Server tables. You can also use SQL statements or other techniques to erase personal data. You may also enable SQL Server Audit to verify changes to data. Free trial evaluation of SQL Server
Windows 10/Windows Server	Windows 10 and Windows Server 2016 both offer PowerShell, a tool that enables you to conduct string-matching or regex queries to search for personal data based on the targeted data's structure and pattern. Using PowerShell, you can search for files and items by file name, properties, and full-text contents for some common file types and data types. Once these have been identified, you can use PowerShell to manually delete data for some file types or use their preferred editing mechanism. Try Windows Server 2016 Try Windows 10 Enterprise edition for free

Question 8/9

Provide data subjects with their personal data in a common, structured format. Under the GDPR, data subjects have the right to portability of their data. This means they can request and receive their personal data from controllers in a structured, commonly used, and machine-readable format. If a data subject made a portability request for their personal data today, your organization:

Your answers : Has a process in place to do some but not all of these requirements.

Offering	How it helps you become GDPR compliant
Azure	Azure enables you to export your data at any time, without seeking approval from Microsoft. Azure Active Directory (AAD) enables you to export data associated with AAD accounts in a .csv file. Using SQL queries, Microsoft customers can identify and then export personal data hosted in Azure SQL Database. Azure Cosmos DB provides the Azure Cosmos DB Migration Tool to help you to export source data to JSON. Using the Azure Storage REST API, you can identify and then export personal data stored in Azure File Service and Table Service. Create a free Azure account
Dynamics 365	Dynamics 365 data can be exported to a static Excel file to facilitate a data portability request. Using Excel, you can then edit the personal data to be included in the portability request and then save as a commonly used, machine-readable format such as .csv or .xml.See plans and pricing for Dynamics 365
Office 365	Office 365 lets you take several approaches to providing data subjects with an exportable copy of their personal data. You can search for and export relevant personal data across Office 365 environments using Advanced eDiscovery. You can then export all files in their native format. These exports can then be modified to include documents that fit the search parameters. Exchange Online allows you to download Exchange Online data at any time using the Import and Export wizards. Relevant files stored in either SharePoint Online or OneDrive for Business can be exported manually or in batches using PowerShell. See plans and pricing for Office 365 Business
SQL	The SQL Server family of products and services provides several methods to export personal data in a common structured format. To identify the target personal data, you can use full-text, regular expression, or general queries against character-based data in SQL Server tables to locate the target personal data. You can then export the data using SELECT statements to specify the structure of the output. Free trial evaluation of SQL Server
Windows 10/Windows Server	Windows 10 and Windows Server 2016 both offer PowerShell, a tool that enables you to conduct string-matching or regex queries to search for personal data based on the target data's structure and pattern. Once identified, you can use the native data export features of Windows 10 to manually transfer data in a variety of file formats. You may also use other Microsoft programs such as Excel, Word, or Notepad to prepare personal data for export. Try Windows Server 2016 Try Windows 10 Enterprise edition for free

Question 9/9

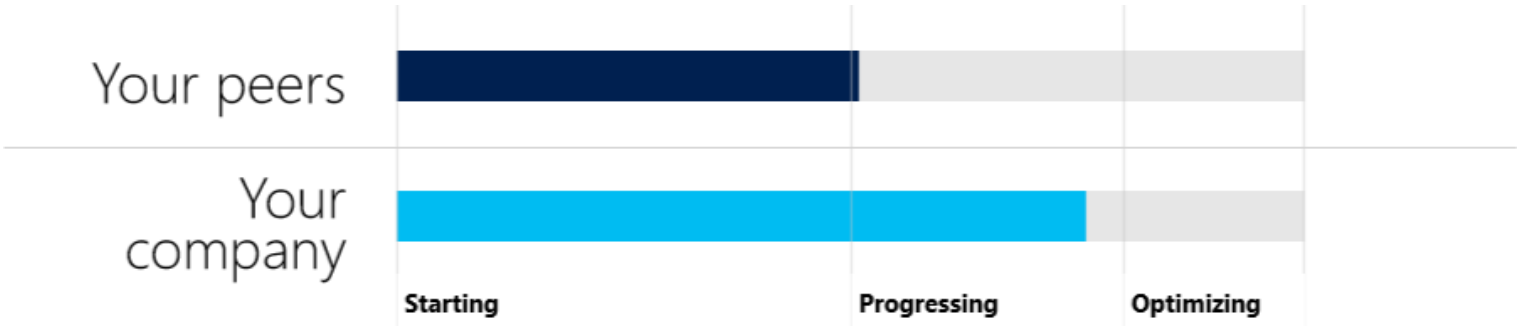
Restrict the processing of personal data. Under the GDPR, data subjects may request a temporary restriction of processing activities utilizing their personal data in certain circumstances, for example if a data subject objects to the processing of that data, but the controller has a legal requirement to retain it. Controllers may need to employ technical means to prevent a specific data subject's personal data from undergoing certain processing activities.In how many cases would your organization be able to do this right now?

Your answers : Most

Offering	How it helps you become GDPR compliant
Azure	Azure lets you minimize the number of people who have access to certain information such as personal data. Administrators can use Azure Active Directory Privileged Identity Management to discover, restrict, and monitor privileged identities and their access to resources. Create a free Azure account
Dynamics 365	Dynamics 365 helps to protect sensitive information and service availability as required by the GDPR by incorporating security measures at the platform and service levels.With Dynamics 365, administrative users grant and restrict user access to personal data through security roles, which are composed of record-level and task-based privileges. Access to personal data can also be managed through Field and Hierarchy level security models that are enabled by Dynamics 365. See plans and pricing for Dynamics 365
EMS	Using Azure Information Protection, you can restrict certain processing activities for specific data subjects by defining a new sub-label and applying protection templates that restrict the desired content permissions, such as forwarding, editing, and reading. You can use Cloud App Security to restrict certain processing activities associated with the target personal data by creating restrictive policies that use the relevant Azure Information Protection classification label. Getting started with Enterprise Mobility + Security
Office 365	Office 365 Data Loss Prevention (DLP) policies enable you to set limits on the processing of the personal data of specific data subjects by implementing processes such as preventing sending the data in email or restricting access to it on SharePoint Online. You can also use PowerShell to identify and place restrictions on files that match specific personal data types or match keyword queries. You can also customize the built-in DLP personal data types by creating a new information type that will target a certain data subject. See plans and pricing for Office 365 Business
SQL	The SQL Server family of products and services enables you to control and restrict access to data in a database table based on the characteristics of the user executing a query. Row-Level Security (RLS) enables you to implement restrictions on data row access, thereby restricting the processing of and access to personal data based on user authorization. The Extended Properties function enables you to restrict the processing of personal data by: adding text, such as descriptive or instructional content; by adding input masks; and by adding formatting rules as properties of objects in a database or as a property of the database itself. Free trial evaluation of SQL Server
Windows 10/Windows Server	Windows Server 2016 offers several ways to restrict the processing of personal data. Azure Rights Management Service in Azure Information Protection allows you to assign and enforce persistent restrictions on sharing files that contain personal data. Domain-based Dynamic Access Control (DAC) enables you to apply access-control permissions and restrictions based on rules that can include the sensitivity of data. Using the Windows File Explorer or PowerShell, you can restrict the processing of personal data by revoking access to files containing the target personal data. Try Windows Server 2016

Protect

Detailed Results and Resources



Question 1/5

Data protection and privacy by design and default. The GDPR requires controllers who collect or process personal data to ensure that their activities and supporting technology are built to include data protection and data privacy principles.Would you say your organization's IT resources meet this standard today?

Your answers : Somewhat

Offering	How it helps you become GDPR compliant
Azure	Azure services are developed utilizing the Microsoft Security Development Lifecycle, which incorporates privacy-by-design and privacy-by-default methodologies, and in accordance with Microsoft privacy policies. To demonstrate Microsoftâ€™s commitment to the privacy and security of customer data, core Azure services are audited at least annually against several global data privacy and network security standards, including ISO/IEC 27018. Create a free Azure account
Dynamics 365	Dynamics 365 services are developed utilizing the Microsoft Security Development Lifecycle, which incorporates privacy-by-design and privacy-by-default methodologies, and in accordance with Microsoft privacy policies. To demonstrate Microsoftâ€™s commitment to the privacy and security of customer data, core Dynamics 365 services are audited at least annually against several global data privacy and network security standards, including ISO/IEC 27018. See plans and pricing for Dynamics 365
EMS	Enterprise Mobility + Security services are developed utilizing the Microsoft Security Development Lifecycle, which incorporates privacy-by-design and privacy-by-default methodologies, and in accordance with Microsoft privacy policies. To demonstrate Microsoftâ€™s commitment to the privacy and security of customer data, certain EMS services are audited at least annually against several global data privacy and network security standards, including ISO/IEC 27018. Getting started with Enterprise Mobility + Security
Office 365	Office 365 services are developed utilizing the Microsoft Security Development Lifecycle, which incorporates privacy-by-design and privacy-by-default methodologies, and in accordance with Microsoft privacy policies. For example, by default, there is zero standing access to customers' content in Office 365. For added compliance and control, Customer Lockbox can enable controllers to demonstrate that there are explicit procedures in place for access to customer content during service operations.To demonstrate Microsoftâ€™s commitment to the privacy and security of customer data, core Office 365 services are audited at least annually against several global data privacy and network security standards, including ISO/IEC 27018. See plans and pricing for Office 365 Business
SQL	The SQL Server family services are developed utilizing the Microsoft Security Development Lifecycle, which incorporates privacy-by-design and privacy-by-default methodologies, and in accordance with Microsoft privacy policies. To demonstrate Microsoftâ€™s commitment to the privacy and security of customer data, Azure SQL Database is audited at least annually against several global data privacy and network security standards, including ISO/IEC 27018. Free trial evaluation of SQL Server
Windows 10/Windows Server	Windows 10 and Windows Server 2016 are developed using the Microsoft Security Development Lifecycle, which incorporates privacy-by-design and privacy-by-default methodologies. Windows 10 and Windows Server 2016 also include many secure-by-default technologies, such as Protected Processes, AppContainer sandbox, and Kernel pool protections. Try Windows Server 2016 Try Windows 10 Enterprise edition for free

Question 2/5

Secure personal data, such as through encryption. The GDPR requires controllers who process personal data to maintain a high standard of security. The GDPR identifies encryption as one potential tool that may be appropriate given the risk to support this requirement.How much of the personal data controlled by your organization is currently encrypted?

Your answers : Most

Offering	How it helps you become GDPR compliant
Azure	Azure encrypts all communications to and from Azure data centers by default. All transactions to Azure Storage through the Azure Portal occur via HTTPS. Additionally, Azure provides many features to enable Microsoft customers to encrypt personal data at rest and in transit: Azure Disk Encryption enables you to encrypt Azure Virtual Machines at rest; Azure VPN Gateway enables Microsoft customers transferring personal data from workstations to Azure to encrypt those communications in-transit; Azure Storage Service Encryption provides encryption for data at rest in Azure Storage; Azure Key Vault enables Microsoft customers to manage encryption keys used by their Azure applications and services. Create a free Azure account
Dynamics 365	Dynamics 365 uses technology such as Transparent Data Encryption (TDE) to encrypt data at rest, and Transport Layer Security (TLS) to secure communication between services. For Dynamics 365, Microsoft SQL Server cell level encryption is available for a set of default entity attributes that contain sensitive information. See plans and pricing for Dynamics 365
EMS	Enterprise Mobility + Security offers powerful encryption features, including Azure Information Protection which can identify and encrypt documents containing personal data located in Windows, mobile platforms, Office applications and services, Windows Server, and other supported applications. Once activated, you can create policies to automatically encrypt files containing sensitive personal data, as well as provide tools for employees to label sensitive files or emails. For devices managed by Intune, Microsoft customers can create, deploy, and monitor configuration policies that enforce device-level encryption for Android and iOS phones.Getting started with Enterprise Mobility + Security
Office 365	Office 365 encrypts all customer content at rest and in transit using multiple encryption technologies, such as BitLocker, Azure Storage Service Encryption, and Office 365 Service Encryption. In addition, each Office application, such as Word, Excel, and PowerPoint, enables you to encrypt documents. OneDrive for Business and SharePoint Online encrypt all personal data in transit. By default, all Skype-to-Skype voice data, video data, file transfers, and instant messages are encrypted. By default, Exchange Online encrypts communications between Office 365 and Exchange Online servers and between Exchange Online customers.Customer data within Office 365 is protected by various forms of encryption and is encrypted both at rest and in transit. For data at rest, Office 365 uses BitLocker, Azure Storage Service Encryption, and Office 365 Service Encryption. For data in transit, Office 365 uses multiple encryption technologies, including Transport Layer Security (TLS) and Internet Protocol Security (IPsec). Office 365 also includes additional customer-managed encryption options, such as message protection in Office 365, but regardless of customer configuration, customer content stored within Office 365 is protected using encryption.See plans and pricing for Office 365 Business
SQL	The SQL Server family of products and services offers you a set of encryption features applied at multiple layers, including the Always Encrypted feature which enables client-side encryption at the column level. SQL Server and Azure SQL Database have Transport Layer Security (TLS)1.2 support enabled by default. Transparent Data Encryption (TDE) performs real-time encryption and decryption of the database, associated backups, and transaction log files without requiring changes to the application. Free trial evaluation of SQL Server
Windows 10/Windows Server	Windows 10 and Windows Server 2016 offer multiple encryption technologies. BitLocker Drive Encryption provides volume-level encryption of operating system drives as well as other fixed or removable data drives. Azure Information Protection enables you to classify, label, and encrypt data in local storage and Windows Server file servers that support File Classification Infrastructure (FCI). Windows Information Protection (WIP) provides you with a tool to protect data against accidental or intentional disclosure using several security measures, including encryption.Try Windows Server 2016 Try Windows 10 Enterprise edition for free

Question 3/5

Establish security controls that ensure the confidentiality, integrity, and availability of personal data. The GDPR requires that controllers implement appropriate technical and organizational measures to secure personal data. Those measures must be appropriate for the risk in question, taking into consideration the state of the art and the cost of measures.Would you say that your organization's approach to securing personal data under its control meets this standard today?

Your answers : Somewhat

Offering	How it helps you become GDPR compliant
Azure	Azure helps protect sensitive information and service availability as required by the GDPR by incorporating a variety of security measures at the platform and service levels, including: Azure Security Center, which enables you to monitor traffic, collect logs, and analyze these data sources for threats; Advanced Threat Analytics, which helps protect against advanced persistent threats and malicious attacks; Application Gateway, a web application firewall; Azure Active Directory, which manages identities and controls access; Azure Key Vault, which lets you manages Azure encryption keys; Multi-Factor Authentication; Network Security Groups, which lets you enforce rules that allow or deny network traffic to resources; and VPN Gateway. Create a free Azure account
Dynamics 365	Dynamics 365 offers multiple tools to help safeguard data according to an organization's specific security and compliance needs, including: Security concepts for Dynamics 365, which helps protect data integrity and privacy in a Dynamics 365 organization; Role-based security, which allows you to group together a set of privileges that limits the tasks a user can perform; Record-based security, which allows you to restrict access to specific records; Field-level security, that allows you to restrict access to specific high-impact fields; and encryption options.See plans and pricing for Dynamics 365
EMS	Enterprise Mobility + Security (EMS) suite provides a holistic and innovative solution set to help organizations protect the confidentiality, integrity, and availability of the personal data they manage, including: Azure Information Protection, which provides persistent data classification and protection; Microsoft Advanced Threat Analytics, which helps protect against advanced persistent threats and malicious attacks; Microsoft Cloud App Security, which provides deep visibility and control of data inside cloud applications, as well as threat protection; Azure Active Directory (AAD), which can help manage employee identities and employee access privileges; and Microsoft Intune; which offers a full set of capabilities to help Microsoft customers protect the devices they manage, such as the enforcement of compliance policies and more. Getting started with Enterprise Mobility + Security
Office 365	Office 365 offers a robust suite of security measures that helps organizations protect personal data, including: Advanced Data Governance (ADG), which helps you automatically identify, classify, and manage personal data and sensitive data as well as apply retention and deletion policies; Threat Intelligence, which helps you proactively uncover and protect against advanced threats in Office 365; Advanced Threat Protection for Exchange Online, (requires an Office 365 E5 subscription) which helps protect email against unknown, sophisticated malware attacks; Advanced Security Management, which lets you identify high-risk and abnormal usage; Data Loss Prevention policies, which enable you to identify personal data as it travels through Exchange Online, SharePoint Online, and OneDrive for Business; Message Encryption; and Antimalware/antispam protection.See plans and pricing for Office 365 Business
SQL	The SQL Server family of products and services provides a powerful set of built-in capabilities that offer you security protections, including: Row-Level Security, which enables you to control access to rows in a database table; Dynamic Data Masking, which limits sensitive data exposure by masking the data to non-privileged users or applications; Transparent Data Encryption; which addresses protecting personal data at the physical storage layer; Always Encrypted, which enables you to encrypt sensitive data inside applications; and SQL Server Authentication and Azure Active Directory (AAD) Authentication; which enable you to ensure that only authorized uses with valid credentials can access the database server. Free trial evaluation of SQL Server
Windows 10/Windows Server	Windows 10 and Windows Server 2016 provide a diverse suite of security features including: Windows Hello, which provides biometric as well as multi-factor authentication; Credential Guard, which helps mitigate the risk of certain credential-theft attacks; Just Enough Administration for Windows Server, which restricts IT administrative rights; BitLocker, which provides both volume-level encryption and encryption for mobile devices; AppLocker, which can create and deploy application control policies; Device Guard, which enables you to construct and deploy code integrity policies; and Shielded Virtual Machines.Try Windows Server 2016 Try Windows 10 Enterprise edition for free

Question 4/5

Detect and respond to data breaches. The GDPR requires controllers to maintain appropriate technologies and/or processes to secure personal data and defend against personal data breaches. If a personal data breach does occur, once aware, a controller may be required to quickly notify regulators and may also be required to notify affected data subjects.For personal data breach notifications, would you say that your organization currently has a process in place to: (Check all that apply.)

Your answers : Notify data subjects,Provide information to regulators,Notify regulators within 72 hours

Offering	How it helps you become GDPR compliant
Azure	Azure provides several tools to help you defend against, detect, and respond to data breaches. Azure Security Center enables you to prevent and detect threats by providing tools to monitor traffic, collect logs, and analyze these data sources for threats. For incidents in which Microsoft holds some or all the responsibility to respond, we have established a detailed Security Incident Response Management process specifically for Azure. Microsoft will also notify affected Microsoft customers with enough details to conduct their own investigations, and to meet any commitments they have made while not unduly delaying the notification process. Create a free Azure account
Dynamics 365	Dynamics 365 deploys security measures intended to prevent and detect data breaches, including software to provide intrusion detection and distributed denial-of-service (DDoS) attack prevention. Dynamics 365 responds to incidents involving data stored in Microsoft datacenters by following a Security Incident Response Management process. Microsoft will also notify affected Microsoft customers with enough details to conduct their own investigations, and to meet any commitments they have made while not unduly delaying the notification process.See plans and pricing for Dynamics 365
EMS	Enterprise Mobility + Security provides tools to help you defend against, detect, and respond to data breaches: Microsoft Advanced Threat Analytics helps you defend against breaches by identifying abnormal behavior of entities, advanced attacks, and security risks; Microsoft Cloud App Security identifies anomalies in cloud app usage that may be indicative of a data breach; and Azure Active Directory Security Reports can provide you with reports of employee user accounts flagged for risk and risky sign-ins that may assist with the detection of abnormal behavior indicative of a breach or potential breach. Getting started with Enterprise Mobility + Security
Office 365	Office 365 provides several tools to help you prevent, detect and respond to data breaches: Office 365 Data Loss Prevention policies enable you to identify personal data and place restrictions on files that match specific personal data types or match keyword queries; and Message Protection in Office 365 allows organizations to deliver sensitive business communications with added protections, allowing you to send and receive encrypted email from inside or outside your organization. For incidents in which Microsoft holds some or all the responsibility to respond, we have established a detailed Security Incident Response Management process. Microsoft will also notify affected Microsoft customers with enough details to conduct their own investigations, and to meet any commitments they have made while not unduly delaying the notification process.See plans and pricing for Office 365 Business
SQL	The SQL Server family of products and services provides a powerful set of built-in capabilities that safeguard data and help you identify potential breaches, including: SQL Database Threat Detection, which can help Microsoft customers detect anomalous database activities; and Azure SQL Database Auditing and SQL Server Audit, that enable customers to understand ongoing database activities, and analyze and investigate potential threats or suspected abuse.For incidents in which Microsoft holds some or all the responsibility to respond, we have established a detailed Security Incident Response Management process. Microsoft will also notify affected Microsoft customers with enough details to investigate on their end, and to meet any commitments they have made while not unduly delaying the notification process. Free trial evaluation of SQL Server
Windows 10/Windows Server	Windows 10 and Windows Server 2016 provide a diverse suite of security features to defend against data breaches, including: Advanced Threat Analytics, which helps defend against breaches by identifying abnormal behavior, advanced attacks and security risks; Windows Defender Advanced Threat Protection for Windows 10, which enables you to help detect active attacks after a breach; and Enhanced Logging on Windows Server, which enables you to identify suspicious behavior by auditing access to sensitive processes.Try Windows Server 2016 Try Windows 10 Enterprise edition for free

Question 5/5

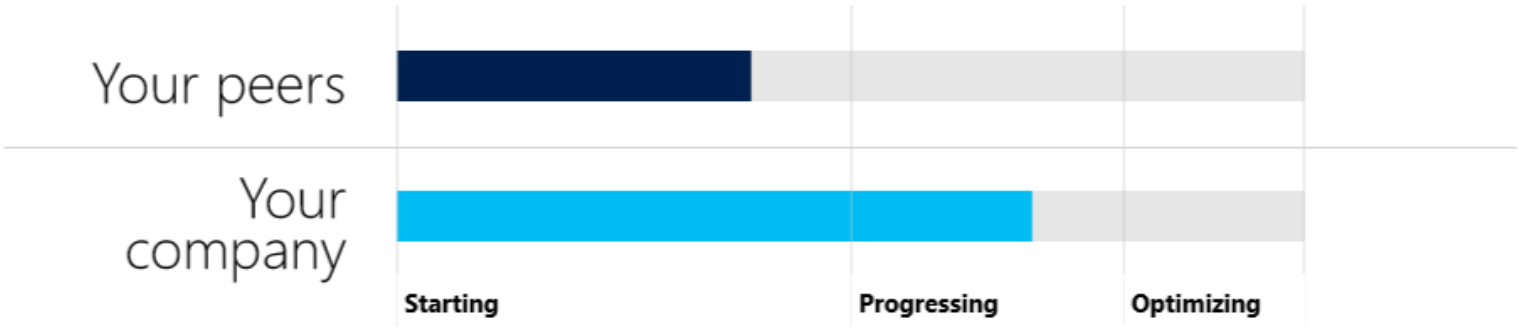
Facilitate regular testing of security measures. To meet the GDPR requirement to protect personal data, controllers should regularly test, assess, and evaluate the effectiveness of their technical and organizational measures to secure it.Would you say that your organization's approach to security testing meets this standard?

Your answers : Somewhat

Offering	How it helps you become GDPR compliant
Azure	Azure provides you with several tools to assess the security state of your Azure deployment and identify opportunities to better protect personal data, including: Azure Security Center, which will assess existing configuration of Azure services to provide configuration and service recommendations to help improve your security posture and protect personal data; and the Vulnerability Assessment tool in Azure Security Center, which identifies configuration recommendations for more secure deployments. Microsoft also conducts ongoing monitoring and testing of Azure security measures. These include ongoing threat modeling, code review and security testing, live site penetration testing, and centralized security logging and monitoring. Create a free Azure account
Dynamics 365	Dynamics 365 provides administrative users with audit functionality that can help identify opportunities to improve security posture and help protect personal data, in addition to detecting data breaches.Microsoft also conducts ongoing monitoring and testing of Dynamics 365 security measures. These include ongoing threat modeling, code review, security testing, live site penetration testing, and centralized security logging and monitoring. See plans and pricing for Dynamics 365
EMS	Enterprise Mobility + Security (EMS) provides tools to help you evaluate your security, including: an Attack Simulation playbook, which details how Microsoft Advanced Threat Analytics (ATA) can be used to detect several threat scenarios; and Azure Active Directory Privileged Identity Management (Azure AD PIM), which allows you to manage, control, and monitor access within your organization. Using Azure AD PIM, organizations can conduct ongoing access reviews and get reports about administrator access history and changes in administrator assignments.Getting started with Enterprise Mobility + Security
Office 365	Office 365 provides several tools to help you evaluate your security, including Office 365 Secure Score, which provides insight into your security posture, as well as the security features you have enabled. Microsoft regularly tests Office 365 security measures using third-party penetration testing and security audits, as well as assessments aligned with industry-standard frameworks. For example, Office 365 internal control framework is based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and Office 365 has been accredited to the latest NIST 800-53 standard. Microsoft releases reports of these security audits to the Service Trust Portal. See plans and pricing for Office 365 Business
SQL	The SQL Server family of products and services provide tools and processes to help assess your security posture. Vulnerability Assessment is a new capability available in preview for Azure SQL Database. It scans databases for insecure configurations, exposed surface area, and additional potential security issues. It gives actionable recommendations for how to resolve these issues and improve the security stature of databases.Microsoft also conducts ongoing monitoring and testing of Azure security measures. These include ongoing threat modeling, code review and security testing, live site penetration testing, and centralized security logging and monitoring. Free trial evaluation of SQL Server
Windows 10/Windows Server	Windows 10 and Windows Server 2016 provide tools that allow you to test certain security measures, including: Advanced Threat Analytics, which you can use to detect several threat scenarios; the Test-AppLockerPolicy PowerShell cmdlet, which can be used to determine whether any of the rules in a rule collection will be blocked; and Device Guard, which can be operated in audit mode to test code integrity policies. Try Windows Server 2016 Try Windows 10 Enterprise edition for free

Report

Detailed Results and Resources



Question 1/4

Maintain audit trails to show GDPR compliance. Controllers should maintain records of their responses to data subject requests. Records should contain both the nature of every request-for example, to view or rectify personal data—and their resolution.Would you say that your organization can demonstrate compliance with these GDPR requirements today?

Your answers : Somewhat

Offering	How it helps you become GDPR compliant
Azure	Azure provides logs and logging tools that you can use to track and record processing activities in Azure, including: Azure Active Directory, which produces logs detailing sign-in activity and application usage; Log Analytics, which can aggregate and analyze Windows Event logs, IIS logs, and Syslogs for Windows and Linux machines; Azure Monitor, which enables organizations to track API calls in customers' Azure resources; and Azure Security Center; which provides tools to enable you to collect and review security logs from across Azure applications and services. Create a free Azure account
Dynamics 365	Dynamics 365 allows you to track and record data changes in a Dynamics 365 environment. The data and operations that can be audited in Dynamics 365 include: the creation, modification, and deletion of records; changes to the shared privileges of records; the addition and deletion of users; the assignment of security roles; and the association of users with teams and business units. You can use these logging and auditing tools to record the resolution of rights requests by a data subject, and to log events associated with amending, erasing, or transferring personal data. See plans and pricing for Dynamics 365
EMS	Enterprise Mobility + Security provides you with tools that enable auditing and logging: Azure Information Protection provides you with logging and reporting functionality to analyze how sensitive data is distributed, including document tracking and revocation for users and admins; Azure Active Directory Audit Reports help you identify privileged actions that occurred in your Azure Active Directory; Microsoft Cloud App Security Cloud Discovery Dashboard and continuous reporting allow you to determine the risk associated with applications; Advanced Threat Analytics provides an attack timeline for reporting anomalies, suspicious activities, malicious attacks and security issues. Getting started with Enterprise Mobility + Security
Office 365	Office 365 provides you with the Unified Audit log to track and record processing activities across the Office 365 environment, including user and administrator activities in Exchange Online, SharePoint Online, and OneDrive for Business.You can use the Unified Audit log to record the resolution of data subject rights requests and log events associated with amending, erasing, or transferring personal data. Auditable events include File and page activities, Folder activities, Sharing and access request activities, Exchange mailbox activities, and user administration activities.See plans and pricing for Office 365 Business
SQL	The SQL Server family of products and services provides you with tools to enable logging and auditing. SQL Server Audit and Azure SQL Database Auditing enable you to understand ongoing database activities, as well as analyze and investigate historical activity. Additionally, SQL Server Audit and Azure SQL Database Audit capabilities maintain audit logs for all Microsoft SQL activities and ensures the existence of a persistent record of database access and processing activities. SQL Server Audit also enables the creation of server audits, which can contain specifications for server-level events and database-level events. Free trial evaluation of SQL Server
Windows 10/Windows Server	Windows 10 and Windows Server 2016 provide comprehensive logs and logging tools that you can use to track and record processing activities that affect personal data. Windows Server 2016 offers you advanced audit and logging tools which can help organizations track compliance with important business-related and security-related rules by tracing defined activities. This detailed raw data can be forwarded into other solutions for deeper analysis or compliance reporting. Windows Server 2016 Advanced Audit Policy Configuration allows you to audit for security-related changes.Try Windows Server 2016 Try Windows 10 Enterprise edition for free

Question 2/4

Only transfer personal data to third countries with required safeguards in place. The GDPR restricts the transfer of personal data outside of the EU to those countries with adequate safeguards or where other specified safeguards exist.Do you have mechanisms in place for the transfer of personal data outside the EU such as Binding Corporate Rules or Standard Contractual Clauses?

Your answers : Yes, in some cases

Offering	How it helps you become GDPR compliant
Azure	Azure lets you reduce the need for transfer of personal data outside of the EU by enabling you to select a region or a national cloud during the initial setup of services, and to store your data in any of more than 30 regions around the globe. These choices include multiple regional choices within Europe as well as the German sovereign data storage region. Additionally, Microsoft has made several contractual commitments related to Azure that enable the appropriate flow of personal data within the Microsoft ecosystem. Microsoft has implemented EU Model Clauses and is certified to the EU-US Privacy Shield framework. Create a free Azure account
Dynamics 365	Dynamics 365 lets you reduce the need for transfer of personal data outside of the EU by enabling you to select a region or a national cloud during the initial setup of services, and to store your data in any of more than 30 regions around the globe. These choices include multiple regional choices within Europe as well as the German sovereign data storage region. Additionally, Microsoft has made several contractual commitments related to Dynamics 365 that enable the appropriate flow of personal data within the Microsoft ecosystem. Microsoft has implemented EU Model Clauses and is certified to the EU-US Privacy Shield framework. See plans and pricing for Dynamics 365
EMS	Enterprise Mobility + Security enables documents classified using Azure Information Protection to be geographically tracked using AIP's Document Tracking and Revocation functionality. After content is classified, Document Tracking and Revocation can monitor how it is used. Document tracking shows information such as the email addresses of the people who attempted to access protected documents that were shared, when these people tried to access them, and their geographic location. Getting started with Enterprise Mobility + Security
Office 365	Office 365 lets you reduce the need for the transfer of personal data outside of the EU. During the initial setup of Office 365 services, customers with an EU billing address will have their Office 365 tenants provisioned in the EU, where their Exchange Online mailbox content, SharePoint Online site content, and files uploaded to OneDrive for Business are stored at rest. Additionally, Microsoft has made several contractual commitments related to Office 365 that enable the appropriate flow of personal data within the Microsoft ecosystem. Microsoft has implemented EU Model Clauses and is certified to the EU-US Privacy Shield framework. See plans and pricing for Office 365 Business
SQL	Azure SQL Database lets you reduce the need for transfer of personal data outside of the EU by enabling you to select a region or a national cloud during the initial setup of services, and to store your data in any of more than 30 regions around the globe. These choices include multiple regional choices within Europe as well as the German sovereign data storage region. Additionally, Microsoft has made several contractual commitments related to Azure that enable the appropriate flow of personal data within the Microsoft ecosystem. Microsoft has implemented EU Model Clauses and is certified to the EU-US Privacy Shield framework. Free trial evaluation of SQL Server
Windows 10/Windows Server	Windows 10 and Windows Server 2016 customers can use Azure Information Protection to geographically track documents using AIP's Document Tracking and Revocation functionality. After content is classified, Document Tracking and Revocation can monitor how it is used. Document tracking shows information such as the email addresses of the people who attempted to access protected documents that were shared, when these people tried to access them, and their geographic location. Try Windows Server 2016 Try Windows 10 Enterprise edition for free

Question 3/4

Track and record transfers of personal data to third-party service providers. The GDPR requires that controllers only engage processors who institute the required technical controls and otherwise meet the requirements of the GDPR.Of the vendors you use who process the personal data of your customers, how many have made the required contractual commitments to support your GDPR compliance?

Your answers : Some

Offering	How it helps you become GDPR compliant
Azure	Azure customers acting as controllers are responsible for tracking distribution of personal data to third parties by their custom services and applications hosted on Azure. Microsoft maintains an inventory of third-party service providers who may have access to customer data and is expanding that process to additional products and scenarios to meet GDPR compliance needs. Create a free Azure account
EMS	Enterprise Mobility + Security enables documents protected and shared using Azure Information Protection and with third-parties to be traced using AIP's Document Tracking and Revocation functionality. Document tracking shows information such as the email addresses of the people who attempted to access protected documents that were shared, when these people tried to access them, and their location. Getting started with Enterprise Mobility + Security
Office 365	Office 365 offers several ways for you to track flows of personal data to third parties, including the Unified Audit log, which can provide insight into data that has been transferred to third parties; and Office 365 Management Activity API, which can be used to identify user sharing activities. Office 365 customers acting as controllers are responsible for tracking distribution of personal data to third parties by their custom services and applications hosted on Office 365. Microsoft maintains an inventory of third-party service providers who may have access to customer data and is expanding that process to additional products and scenarios to meet GDPR compliance needs. See plans and pricing for Office 365 Business
SQL	The SQL Server family of products and services includes features to support efforts to track and record flows of personal data to third-parties. You can use the Microsoft SQL relational database system as a storage and processing technology to document personal data that is transferred to additional processors. This may help customers trace personal data distributed to down-stream processors.SQL Server customers acting as controllers are responsible for tracking distribution of personal data to third parties by their custom services and applications. Microsoft maintains an inventory of third-party service providers who may have access to customer data and is expanding that process to additional products and scenarios to meet GDPR compliance needs. Free trial evaluation of SQL Server
Windows 10/Windows Server	Windows Server 2016 customers can use Active Directory Rights Management Services (AD RMS) to track the use of protected documents. With a subscription that supports document tracking, the document tracking site is enabled by default for all users in an organization. Document tracking can show information such as the email address and location of anyone who attempted to access protected documents that were shared, as well as when they attempted access. Try Windows Server 2016 Try Windows 10 Enterprise edition for free

Question 4/4

Facilitate Data Protection Impact Assessments (DPIAs). Controllers must conduct a DPIA when processing might pose a high risk to the rights and freedoms of individuals. This is an internal procedure that aims to evaluate, among other things, the impact of the proposed processing activity on the protection of personal data and to consider appropriate mitigations.Your organization conducts a DPIA when: (Check all that apply.)

Your answers : You are using a new technology,Processing is likely to result in a high risk to the privacy of individuals

Offering	How it helps you become GDPR compliant
Azure	Azure provides customers with detailed information regarding its collection and processing of customer data, as well as our underlying privacy and security practices that may support organizations conducting Data Protection Impact assessments on their use of Azure. In addition, to help customers seeking information that may be useful in performing a DPIA addressing their use of Azure, Microsoft provides detailed information regarding its privacy standards, its collection and processing of customer data, and the security measures used to protect that data. This information, accessible via the Microsoft Trust Center, includes: what data Microsoft collects and processes; Microsoftâ€™s privacy standards; access to data controlled by Microsoft; details on Azure security measures; and details regarding Microsoft's privacy reviews process.Create a free Azure account
Dynamics 365	Dynamics 365 enables you to use the Dynamics 365 audit log, so you can track and record processing activities across the Dynamics 365 ecosystem to inform a Data Protection Impact Assessment (DPIA).In addition, to help customers seeking information that may be useful in performing a DPIA addressing their use of Dynamics 365 , Microsoft provides detailed information regarding its privacy standards, its collection and processing of customer data, and the security measures used to protect that data. This information, accessible via the Microsoft Trust Center, includes: what data Microsoft collects and processes; Microsoftâ€™s privacy standards; access to data controlled by Microsoft; details on Dynamics 365 security measures; and details regarding Microsoft's privacy reviews process.See plans and pricing for Dynamics 365
EMS	Enterprise Mobility + Security includes Microsoft Cloud App Security, which allows you to identify applications in your environment and evaluate their security measures, information that may help customers who wish to perform a Data Protection Impact Assessment (DPIA) on the use of cloud applications.In addition, to help customers seeking information that may be useful in performing a DPIA addressing their use of EMS, Microsoft provides detailed information regarding its collection and processing of customer data and the security measures used to protect that data. This information, accessible via the Microsoft Trust Center, includes: what data Microsoft collects and processes; Microsoftâ€™s privacy standards; access to data controlled by Microsoft ; details on Azure security measures; and details regarding Microsoft's privacy reviews process.Getting started with Enterprise Mobility + Security
Office 365	Office 365 allows you to get information to conduct a risk assessment and view reports and audited controls using Office 365 Service assurance in the Office 365 Security & Compliance Center.In addition, to help customers seeking information that may be useful in performing a DPIA addressing their use of Office 365, Microsoft provides detailed information regarding its collection and processing of customer data and the security measures used to protect that data. This information, accessible via the Microsoft Trust Center, includes: what data Microsoft collects and processes; Microsoftâ€™s privacy standards, access to data controlled by Microsoft; details on Office 365 security measures; and details regarding Microsoft's privacy reviews process.See plans and pricing for Office 365 Business
SQL	The SQL Server family of products and services includes several mechanisms to help you perform a Data Protection Impact Assessment (DPIA), including: Vulnerability Assessment, which scans Azure SQL Databases for potential security issues; and Azure SQL Database Auditing and SQL Server Audit, which enable you to understand ongoing database activities.In addition, to help customers seeking information that may be useful in performing a DPIA addressing their use of SQL Server, Microsoft provides detailed information regarding its collection and processing of customer data and the security measures used to protect that data. This information, accessible via the Microsoft Trust Center, includes: what data Microsoft collects and processes; Microsoftâ€™s privacy standards; access to data controlled by Microsoft; details on Azure security measures; and details regarding Microsoft's privacy reviews process.Free trial evaluation of SQL Server
Windows 10/Windows Server	Windows 10 and Windows Server 2016 customers who wish to perform a DPIA can use the detailed information Microsoft provides regarding its collection and processing of customer data and the security measures used to protect that data. This information, accessible via the Microsoft Trust Center, includes: what data Microsoft collects and processes; Microsoftâ€™s privacy standards; access to data controlled by Microsoft; details on Windows security measures; and details regarding Microsoft's privacy reviews process.Try Windows Server 2016 Try Windows 10 Enterprise edition for free