



# Supporting Your EU GDPR Compliance Journey

With Microsoft Project Online  
Release 1



# Contents

<a href="#">Disclaimer</a>	3		
<a href="#">Introduction</a>	4		
Using this Document	5		
Shared Responsibility Model	6		
<a href="#">The GDPR and its Implications</a>	7		
<a href="#">Key GDPR Compliance Roles</a>	8		
<a href="#">Key Data</a>	9		
Data definitions	9		
Data pseudonymization	9		
General user data	10		
<a href="#">Journey Toward GDPR Compliance</a>	11		
Four stages to follow	11		
Key GDPR steps	12		
<a href="#">Microsoft Project Online and the GDPR</a>	13		
<a href="#">Project Online and the GDPR Journey</a>	15		
Key messaging	15		
<a href="#">Discover</a>	16		
Search for and identify user data	17		
Facilitate data classification	17		
Key takeaways	17		
<a href="#">Manage</a>	18		
Facilitate requests for the rectification, erasure, or transfer of user data	19		
		Rectify inaccurate or incomplete user data regarding data subjects	19
		Erase user data regarding a data subject	19
		Provide data subject with their user data in a common, structured format	19
		Restrict the processing of user data	19
		Key takeaways	19
		<a href="#">Protect</a>	20
		Data protection and privacy by design and default	21
		Secure user data through encryption	21
		Detect and respond to data breaches	21
		Facilitate regular testing of security measures	21
		Key takeaways	21
		<a href="#">Report</a>	22
		Maintain audit trails to show GDPR compliance	23
		Track and record flows of user data into and out of the EU	23
		Track and record flows of user data to third-party service providers	23
		Facilitate a Data Protection Impact Assessment (DPIA)	23
		Key takeaways	23
		<a href="#">Want to learn more?</a>	24
		<a href="#">Resources</a>	24

# 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.

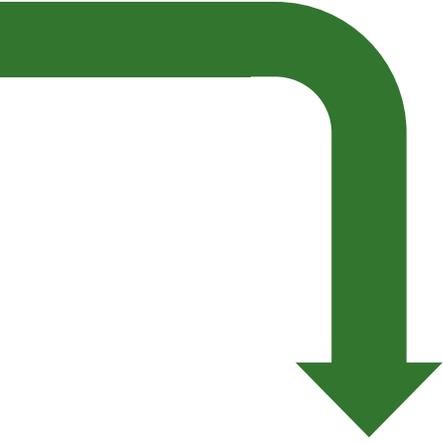
Published October 2018

Version 1.0

© 2018 Microsoft. All rights reserved.



# Introduction



On May 25, 2018, a European Union (EU) privacy law took effect that sets a new global bar for privacy rights, security, and compliance. If your organization is a Microsoft Project Online customer that finds itself considered a data controller (see Key GDPR Compliance Roles below) as defined by the General Data Protection Regulation, or GDPR, this white paper is addressed to you.

The GDPR is fundamentally about protecting and enabling the privacy rights of individuals. The GDPR establishes strict privacy requirements governing how you manage and protect user 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 and mandates 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, including Microsoft.

We have outlined our commitment to the GDPR and how we are supporting our customers within the [“Get GDPR compliant with the Microsoft Cloud”](#) blog post by our Chief Privacy Officer Brendon Lynch and the [“Microsoft’s commitment to GDPR, privacy and putting customers in control of their own data”](#) blog post by Julie Brill, Microsoft’s Corporate Vice President and Deputy General Counsel.

Although your journey toward GDPR compliance may seem challenging, we are here to help you. For specific information about the GDPR, our commitments and beginning your journey, please visit the [GDPR section of the Microsoft Trust Center](#) and [Microsoft Service Trust Portal](#).

# Using this Document



The GDPR is new and your organization will need to develop its own interpretation as to how it applies to your business. Project Online can be an important part of your journey toward GDPR compliance. The purpose of this document is to provide you with some basic understanding of the GDPR and relate that to Project Online. While compliance with the GDPR is mandatory in specific situations outlined below, it is not a “check box” exercise. It is also a way to enhance your overall data protection and privacy capabilities.

Throughout this document you will find references to specific GDPR sections (e.g., Article 7). These are provided as a reference to better connect your understanding of the GDPR with capabilities related to Project Online. It is not meant to imply that by using specific features or capabilities within Project Online, your organization then complies with a specific requirement of the GDPR.

In addition to the Project Online capabilities outlined in this white paper, Microsoft has provided the Trust Center as a cross-Microsoft Cloud services solution designed to help organizations meet complex compliance obligations like the GDPR. It provides recommended actions and step-by-step guidance.

The first few sections of this document will provide an overview of the GDPR and suggest an approach for how you can think about both enhancing your data protection capabilities as well as how you may want to think about complying with the GDPR as expressed in four stages: Discover, Manage, Protect, and Report.

The next sections go into specific detail on how Microsoft Project Online can help address your needs in each of the four stages.

# Shared Responsibility Model

As you read through this document, keep in mind that your compliance with the GDPR involves your role as a “controller” and, in some cases, Microsoft as a “processor.” These roles are defined in the GDPR overview section further below. You may find that you are both controller and processor, or have a shared responsibility with Microsoft.

In a recent publication, "[Shared Responsibilities for Cloud Computing](#)," Microsoft outlines the types of responsibilities it shares with its customers that can vary from the traditional on-premises IT environment to the cloud environments that have come to be known as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The shared responsibility model for these IT environments is summarized graphically to the right.

This model directly relates to how you utilize Project Online. Depending on how you have implemented and are using the solution, the following may apply.

- Runs on-premises where you are in both the controller and processor roles. Microsoft may provide important features but is not directly involved with your GDPR compliance.
- Is an on-premises version but you are using IaaS to host the solution. You remain the controller and processor, but Microsoft provides important controls for you.

- Is a SaaS version where you are the controller and Microsoft is the processor and provides important controls.

Additional information about the responsibilities outlined in this model can be found in the Microsoft publication “Shared Responsibilities for Cloud Computing” referenced above.

Responsibility	On-prem	IaaS	PaaS	SaaS
Data classification and accountability	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Client and end-point protection	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider
Identity and access management	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Customer / Cloud Provider
Application level controls	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider
Network controls	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider	Cloud Provider
Host infrastructure	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider	Cloud Provider
Physical security	Cloud Customer	Cloud Provider	Cloud Provider	Cloud Provider

Legend: ■ Cloud Customer ■ Cloud Provider

# The GDPR and its Implications

The GDPR is a complex regulation that may require significant changes in how you gather, use, and manage user data. Microsoft has a long history of helping our customers comply with complex regulations, and when it comes to preparing for the GDPR, we are your partner on this journey.

The GDPR imposes new rules on organizations established in the EU and on organizations—wherever they are located—that offer goods and services to people in the EU or that monitor the behavior of people that takes place in the Union. Among the key elements of the GDPR are the following:

**Enhanced user privacy rights** – strengthened data protection for individuals within the EU by ensuring they have the right to access their user data, correct inaccuracies in that data, have their user data erased upon request, object to the processing of their user data, and move their user data;

**Increased duty for protecting user data** – reinforced accountability of companies and public organizations that process user data, providing increased clarity of responsibility in ensuring compliance;

**Mandatory user data breach reporting** – companies are required to report user data breaches to their supervisory authorities without undue delay, and generally no later than 72 hours; and,

**Significant penalties for non-compliance** – steep sanctions, including substantial fines that are applicable whether an organization has intentionally or inadvertently failed to comply.

As you might anticipate, the GDPR can have a significant impact on your business potentially requiring you to update user privacy policies, implement/strengthen user data protection controls and breach notification procedures, deploy highly transparent policies, and further invest in IT and training.

# Key GDPR Compliance Roles

As noted in the [Shared Responsibility Model](#) section above, there are specific roles defined within the GDPR that are important to keep in mind as you look at your compliance efforts and how your technology vendors, like Microsoft, impact those efforts. The GDPR defines the term “data subject” as well as two roles, controller and processor, which have specific obligations under the GDPR. These are called out in Article 4 of the GDPR:

- **Data Subject** – defined as, “an identified or identifiable natural person” and for the purposes of the scope of the GDPR that data subject is covered, regardless of their nationality or place of residence with the EU, in relation to the processing of their user data.
- **Controller** – defined as, “the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of user data.” Within the context of the GDPR, a controller does not have to be located within the EU for the GDPR to apply.
- **Processor** – defined as, “a natural or legal person, public authority, agency or other body which processes user data on behalf of the controller.”

It should be noted that the applicability of certain GDPR requirements may change depending on different variables such as a controller’s size (e.g., organizations defined as micro, small and medium-sized enterprises employing fewer than 250 persons); or, the nature of the processing (e.g., for the purposes of prosecuting criminal offences, by the data subject in the course of a purely user or household activity). For this reason, it is recommended that you seek legal assistance to determine your organization’s specific interpretation of the GDPR. Microsoft’s role as a controller and/or processor varies based on these definitions.

In some situations, such as holding its own employees’ data or certain types of data that can be considered as user data, Microsoft acts as a controller using its own technologies and Cloud Services or technologies and Cloud Services from others.

There are also situations, such as with a Cloud Service like Project Online, where Microsoft can act as a processor since a customer in the role of a controller is dependent upon Microsoft, as a processor, to provide capabilities upon which a controller will depend to meet its obligations such as in the area of notification of a user data breach. For more information on how Microsoft addresses these obligations, visit the [Microsoft Trust Center](#).

# Key Data

## Data definitions

As part of your effort to comply with the GDPR, you will need to understand both the definitions of user and sensitive data and how they relate to the types of data held by your organization within Project Online.

Based on that understanding you will be able to discover how that data is created, processed, managed, and stored.

The GDPR considers user data to be any information related to an identified or identifiable natural person. That can include both direct identification (i.e., your legal name) and indirect identification (i.e., specific information that makes it clear it is you the data references). Information relating to an identified or identifiable natural person (data subject). Examples include:

- Name
- Identification numbers
- Location data (e.g., home address)
- Online identifier (e.g., e-mail address, screen names, IP address, device IDs)

The GDPR makes clear that the concept of user data includes online identifiers (e.g., IP addresses, mobile device IDs) and location data.

Sensitive data are special categories of user data that are afforded enhanced protections and generally require an individual's explicit consent where these data are to be processed.

## Data pseudonymization

The GDPR also addresses the concept of pseudonymous data, or user data that has been separated from its direct identifiers so that linkage to an identity is no longer possible without additional information that is being stored separately. This is different from anonymized data, where the direct link to user data is destroyed. With anonymized data, there is no way to re-identify the data subject and, therefore, it is outside the scope of the GDPR.

As noted in the GDPR (Recital 28), "The application of pseudonymization to user data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymization' in this Regulation is not intended to preclude any other measures of data protection."

If your organization pseudonymizes your data you may benefit from the relaxation of certain provisions of the GDPR, such as user data breach notification requirements. The GDPR also encourages pseudonymizing in the interests of enhancing security and as a privacy by design measure.

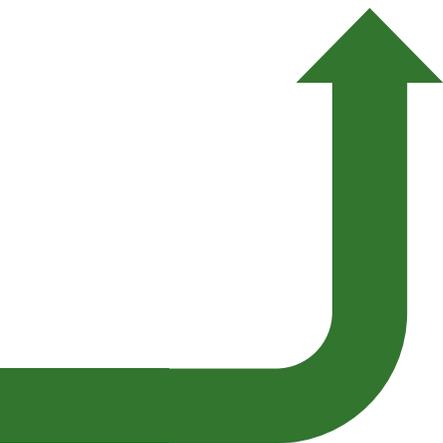
You will have very strong incentives to employ data pseudonymizing technologies under the GDPR to mitigate your compliance obligations and manage your risks. But bear in mind, while the GDPR considers both encryption or pseudonymization as safeguards, under Article 34, breach notification may be avoided if "the controller has implemented appropriate technical and organizational protection measures... such as encryption."

## General user data

With the data definitions outlined in the GDPR in mind, let's look at data contained in Project Online and see how they relate. Microsoft defines specific data categories related to its online services, such as Project Online, in the Microsoft Online Privacy Statement. As noted below, some of this data will be your responsibility as the controller to manage in a way that is in line with the GDPR. This list will start you on your [Discover](#) step.

- **Customer data** is all data, including text, sound, video, or image files and software, that you provide to Microsoft or that is provided on your behalf through your use of Microsoft enterprise online services. For example, it includes data that you upload for storage or processing, as well as applications that you upload for distribution through a Microsoft enterprise Cloud service. Customer data does not include administrator or other contact data, payment data, or support data.
- **Content** is a subset of customer data and includes, for example, Exchange Online emails and attachments, Power BI reports, SharePoint Online site content, IM conversations, and data about your interactions with customers.
- **Administrator data** is the information about administrators supplied during signup, purchase, or administration of Microsoft services, such as names, phone numbers, and email addresses. It also includes aggregated usage information and data associated with your account, such as the controls you select. We use administrator data to provide services, complete transactions, service the account, and detect and prevent fraud.
- **Support data** is the information we collect when you contact Microsoft for help, including what you supply in a support request, results from running an automated trouble shooter, or files that you send us. Support data does not include administrator or payment data.

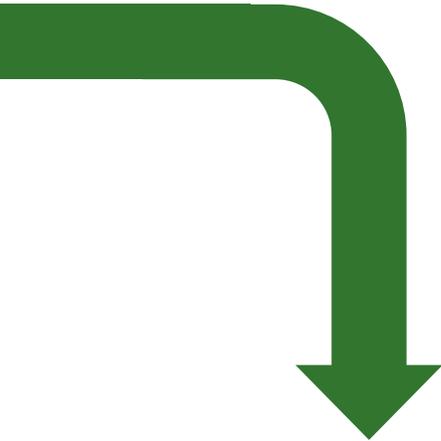
All these data categories may contain user data subject to the GDPR.



A man and a woman are walking through a modern office hallway. The woman, on the left, is wearing a black blazer over a white blouse with a black bow and is holding a silver laptop. The man, on the right, is wearing a maroon blazer over a light green sweater and blue jeans, and is also holding a silver HP laptop. They are both looking down at the laptop held by the woman. The background shows an office with desks, chairs, and computer monitors.

# Journey Toward GDPR Compliance

Four stages to follow



Where do you begin? How do you start the journey toward GDPR compliance as you utilize the Project Online services and applications? In the general white paper "[GDPR Overview](#)," we addressed topics such as an introduction to GDPR, how it impacts you, and what you can do to begin your journey today. We also recommended that you begin your journey to GDPR compliance by focusing on four key steps.

### Key GDPR steps

1. **Discover** – Identify what user data you have and where it resides.
2. **Manage** – Govern how user data is used and accessed.
3. **Protect** – Establish security controls to prevent, detect, and respond to vulnerabilities and data breaches.
4. **Report** – Execute on data requests, report data breaches, and keep required documentation.

For each of the steps outlined in the general white paper referenced above, we 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 white paper for Project Online 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](https://Microsoft.com/GDPR).

Given how much is involved, you should not wait to prepare until GDPR enforcement begins. You should review your privacy and data management practices now. The balance of this white paper is focused on how Project Online can support your compliance with the GDPR following the four steps introduced above, as well as approaches, recommended practices, and techniques to support your ongoing GDPR compliance journey.



# Microsoft Project Online and the GDPR

As described above, the scope of GDPR is intended to apply to the processing of user data whatever technology is used. Because Microsoft Project Online may be used to process user data, there are certain requirements within the GDPR (as noted by the references to regulation Articles contained in the GDPR below) where Project Online users should pay close attention (but this is not to the exclusion of other Articles containing GDPR requirements with which you must comply).

**Consent (Article 7)** – Under the new regulation, there must be a basis for any processing. If the basis is consent, that consent must be demonstrable and “freely given.” Furthermore, the data subject must also have the right to withdraw consent at any time. This may change how marketing and sales activities are managed.

**Rights to access (Article 15), rectification (Article 16), and erasure (Article 17)** – Under the GDPR, mechanisms need to be provided for data subjects to request access to their user data and receive information on the processing of that data, to rectify user data if incorrect, and to request the erasure of their user data, sometimes known as the “right to be forgotten.” You should ensure that any user data that is requested to be erased does not conflict with other obligations you may have around data retention (e.g., proof of payment, proof of tax).

**Documentation (Articles 24 and 30)** – An important aspect of the GDPR is to maintain audit trails and other evidence to demonstrate accountability and compliance with the GDPR requirements, and to maintain an inventory of your organization’s user data detailing categories of data subjects and the user data held by the organization.

**Privacy by design (Article 25)** – This is a key element of the GDPR. It requires controllers and processors to implement the necessary privacy controls, safeguards, and data protection principles, such as minimizing the data collected, not just at the time of processing but, in advance, when determining the means of processing.

**Data security (Articles 25, 29, and 32)** – The GDPR requires controllers and processors to control access to user data (e.g., role-based access, segregation of duties) and implement appropriate technical and organizational measures to protect the confidentiality, integrity, and availability of that data and processing systems.



**The capabilities of Project Online described in this white paper are designed to help you get started on your journey to GDPR compliance. The Trust Center highlights our four trust pillars.**

**Security** – Project Online is built using the Security Development Lifecycle (SDL), a mandatory Microsoft process that embeds security requirements into every phase of the development process. Azure Active Directory helps protect Project Online from unauthorized access by simplifying the management of users and groups and enabling you to assign and revoke privileges easily.

For example, Microsoft uses encryption technology to protect your data at rest in a Microsoft database and when it travels between user devices and our Azure datacenters. Project Online production environments are monitored to help protect against online threats by using distributed denial-of-service (DDoS) attack prevention and regular penetration testing to help validate security controls. At the interface with the public network, Microsoft uses special-purpose security devices for firewall, NAT, and IP filtering functions.

**Privacy** – You are the owner of your data. We do not mine your data for advertising. If you ever choose to terminate the service, you can take your data with you. Microsoft is the custodian or processor of your data. We use your data only for purposes that are consistent with providing the services to which you subscribe. If a government approaches us for access to your data, we redirect the inquiry to you, the customer, whenever possible. [We have challenged](#), and will challenge in court, any invalid legal demand that prohibits disclosure of a government request for customer data.

**Compliance** – Microsoft complies with leading data protection and privacy laws applicable to cloud services, and our compliance with world-class industry standards is verified by third parties. As with all our cloud services products, Project Online is enabled to help customers comply with their national, regional, and industry-specific laws, and regulations.

**Transparency** – In line with the tenets of the GDPR, we provide you with clear explanations about where your data is stored and how we help secure it, as well as who can access it and under what circumstances. Further, if you have requested notifications, we will notify you about changes in our service operations.

If your organization collects, hosts, or analyzes user data of EU residents, the GDPR requires you only use third-party processors, such as Microsoft, who provide the required guarantees of compliance set out in Article 28 of the GDPR.



# Project Online and the GDPR Journey

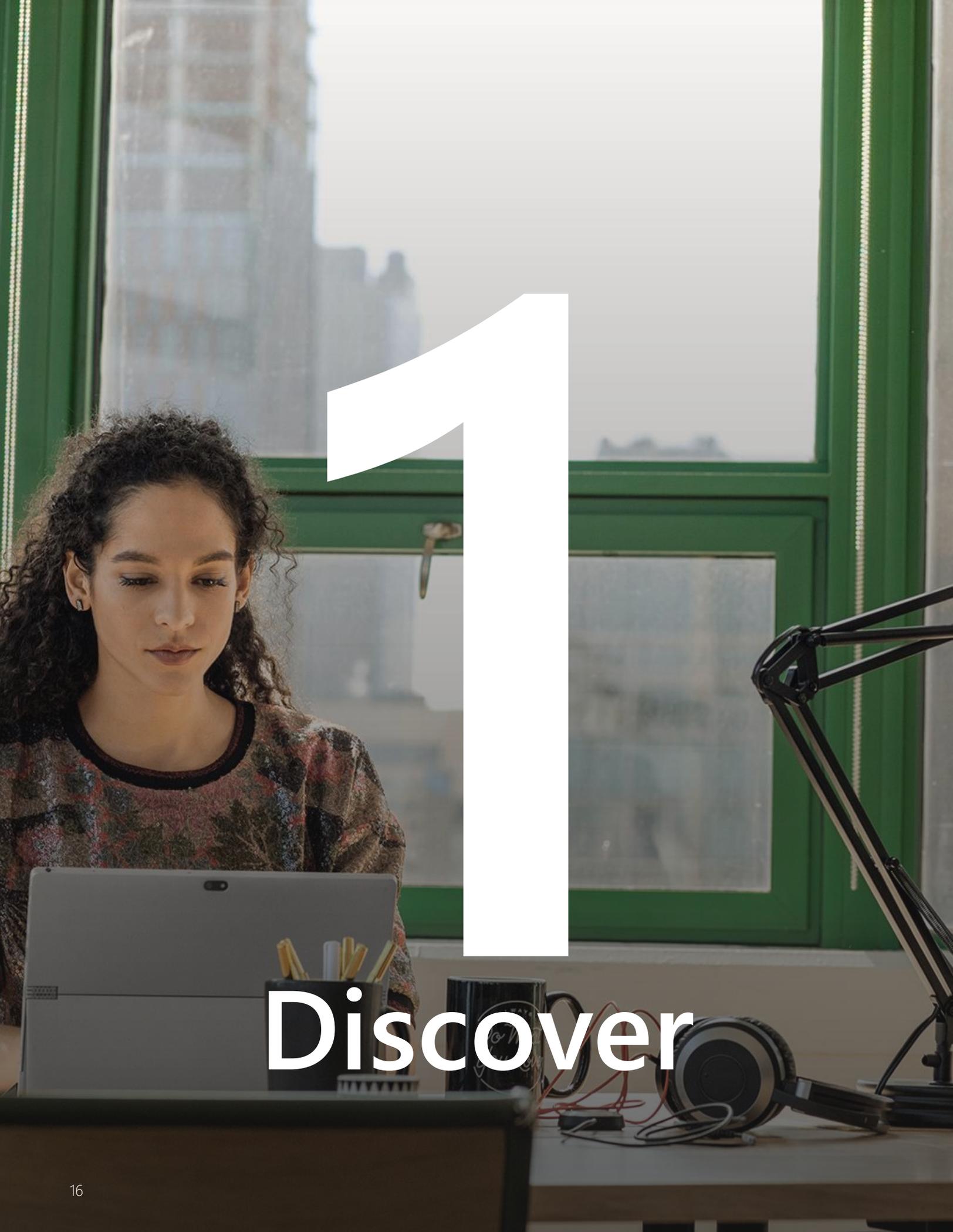
In this section, you will see how the key features within Project Online can be brought to bear on the important steps of your journey—Discovery, Manage, Protect, and Report—toward GDPR compliance. It should be noted that there are many other ways of achieving GDPR compliance and you can always adjust your Project Online solution design to your exact business and solution requirements.

## Key messaging

Project Online helps you comply with GDPR to:

- Obtain explicit consent from customers to process their data by providing tools to create notifications to inform customers about how their data will be used.
- Respect data subject rights by:
  - Enabling your customers to request rectification, erasure, or transfer of their user data.
  - Enabling portability of your customers' user data in a commonly used and machine-readable format.
  - Incorporating privacy-by-design and privacy-by-default methodologies into the design of your systems.
  - Increasing data security by providing you with multiple ways to grant or restrict access to user data and encrypting user data at rest and in transit.
  - Enabling audit trails to help document compliance with GDPR regulations.
  - Reducing the transfer of user data (except for directory data) outside the EU.





1

Discover

# Discover

## Search for and identify user data

Project Online provides multiple methods for you to search for user data within records such as PowerShell, Quick Find, and Relevance Search. These functions enable you to identify (find) user data. Information can all be found through the Project Web Interface.

Use the following ways to search Project Online for user data.

1. PowerShell for export and redacting.
2. Quick Find options for the organization (on-premises only). Quick Find relies on SQL filters and indexing information, therefore additional considerations are required to set and maintain the appropriate schedule for your organizational needs.
3. Relevance Search, which can be saved for future reference using dashboards.

## Facilitate data classification

Project Online offers the flexibility to build an application extension for data classification that is implemented using solution customization, where customers can configure Views to look for user information based on GDPR requests. Without such classification, search for user data will not be available in solutions.

Customers can create the name- or data-based classification, use a hidden entity to customize information, or create a global option set to identify entities with user information. It is possible to couple several entities to provide classification needed for future management of data through tagging.

## Key takeaways

There is potential for user data to reside within Project Online that can vary across the applications you have licensed.

- Project Online provides several reporting and auditing capabilities that can be used to identify user data.
- Project Online provides customers with the ability to customize privacy notices displayed to users in the application through the administrator settings console.
- As the controller, you are responsible for identifying user data that you have collected and responding to data subject rights requests. Depending on what information you capture and the part of the solution where the information is stored, this may require some combination of configuration or customization of Project Online or Office 365.
- Your organization may have other applications or services related to the Project Online application where user data is stored. As a controller, you are responsible for managing the user data that flows to or from those applications or services.



Manage

# Manage

## **Facilitate requests for the rectification, erasure, or transfer of user data**

Project Online provides users with several tools to erase and edit user data associated with data subjects. Users can create support cases to track and manage data subject rights requests. The use of Service Level Agreement (SLA) capabilities will help ensure requests are addressed in a timely manner. 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.

## **Rectify inaccurate or incomplete user data regarding data subjects**

Project Online offers you several methods to rectify inaccurate or incomplete user data. For example, resource information can be edited directly in Project Online as both single or multiple rows. Other information can be edited by manually changing the specific data element containing the target user data.

## **Erase user data regarding a data subject**

The Project Online administrative interface gives you several methods for erasing data regarding a data subject. Project Online lets you locate the data using various search and reporting capabilities.

## **Provide data subject with their user data in a common, structured format**

Project Online data can be exported to a static Excel file to facilitate a data portability request. Using Excel, you can then edit the user data to be included in the portability request and then save as a commonly used, machine-readable format such as .csv or .xml.

## **Restrict the processing of user data**

Project Online helps to protect user data and service availability as required by the GDPR by incorporating security measures at the platform and service levels. With Project Online, administrative users grant and restrict user access to user data through security roles and categories.

## **Key takeaways**

- Make sure any information that qualifies as user data is proactively identified.
- When exporting or bringing in information into Project Online, you should ensure that the processes and solution used is consistent with your interpretation of the GDPR requirements.
- The Microsoft Service Trust portal capabilities can be an option to help with GDPR compliance efforts.



3

Protect

# Protect

## **Data protection and privacy by design and default**

Project Online services are developed using the Microsoft Security Development Lifecycle (SDL), which incorporates privacy-by-design and privacy-by-default methodologies, and in accordance with Microsoft privacy policies. Project Online follows the same compliance standards and certifications as a part of the Office 365 family. To demonstrate Microsoft's commitment to the privacy and security of customer data, Project Online services are audited at least annually against various compliance offerings, including ISO 27001, ISO 27018, and SOC 1 Type 2.

## **Secure user data through encryption**

Project Online uses technology such as Transparent Data Encryption (TDE) to encrypt data at rest, and Transport Layer Security (TLS) to secure communication between services.

## **Detect and respond to data breaches**

Project Online operates with our data centers and network infrastructure. This infrastructure deploys security measures intended to prevent and detect data breaches, including software to provide intrusion detection and distributed denial-of-service (DDoS) attack prevention. Microsoft 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.

## **Facilitate regular testing of security measures**

Project Online provides administrative users with the ability to extend the platform to provide additional audit functionality. These can in turn be used to help identify opportunities and improve the security posture to protect user data, in addition to detecting data breaches. Microsoft also conducts ongoing monitoring and testing of the Office 365 security measures in which Project Online resides. These include ongoing threat modeling, code review, security testing, live site penetration testing, and centralized security logging and monitoring.

## **Key takeaways**

- Project Online is enabled to help customers comply with their national, regional, and industry-specific laws and regulations.
- You can use the security concepts for Office 365 to protect the data integrity and privacy in a Project Online organization.
- Microsoft Project Online can support an auditing capability where entity and attribute data changes within an organization can be recorded over time for use in analysis and reporting purposes.



# 4

# Report

# Report

## **Maintain audit trails to show GDPR compliance**

Project Online includes technology that can allow you to track and record data changes in a Project Online environment. The data and operations that can be audited in Project Online include the creation, modification, and deletion of projects; the addition and deletion of users; the assignment of tasks; and, the association of users with projects. 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 user data.

## **Track and record flows of user data into and out of the EU**

Project Online lets you reduce the need for transfer of user data (except for directory data needed to authenticate your access to the online service) 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 datacenters 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 Project Online that enable the appropriate flow of user data within the Microsoft ecosystem. Microsoft has implemented EU Model Clauses and is certified to the EU-US Privacy Shield framework.

## **Track and record flows of user data to third-party service providers**

Project Online customers acting as controllers are responsible for tracking distribution of user data to third parties by their custom services and applications hosted on Project Online. 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.

## **Facilitate a Data Protection Impact Assessment (DPIA)**

Microsoft provides detailed information regarding its privacy standards, its collection and processing of customer data, and the security used to protect that data. This information, accessible via the Microsoft Trust Center, includes what data Microsoft collects and processes; Microsoft privacy standards; access to data controlled by Microsoft; details on 365 security measures; and, details regarding the Microsoft privacy reviews process.

## **Key takeaways**

- Project Online is enabled to help customers comply with their national, regional, and industry-specific laws and regulations
- Project Online has implemented security and privacy controls. These reports include SOC 1 Type 2 reports, ISO/IEC 27001 and ISO/IEC 27018 audit reports, and Security assessment reports.

# Want to learn more?

Microsoft has spent years preparing for GDPR. Visit our dedicated GDPR [Trust Center](#) site to learn more about what Microsoft is doing to help customers meet the new requirements. The site includes information on getting started with GDPR compliance, how Microsoft products comply with the regulation, a host of resources, and an FAQ section.

## Resources

### Articles

- Export user data
  - [Project Online](#)
  - [Project Server](#)
- Delete user data
  - [Project Online](#)
  - [Project Server](#)
- [Project Online and Project Server export definitions](#)



© 2018 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred. This document does not provide you with any legal rights to any intellectual property in any Microsoft product.