

Microsoft Trust Center

# GDPR Assessment Responses

September 2017







# 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.

© 2017 Microsoft. All rights reserved.



# Contents

4

## **Introduction**

6

## **The GDPR and its implications**

Personal and sensitive data

11

## **Journey toward GDPR compliance**

Four stages to follow

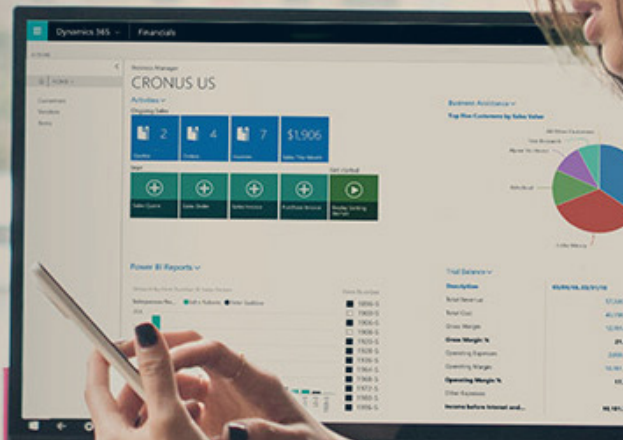
24

## **How you can obtain Dynamics**


Get started with Dynamics 365





# Introduction



**i** Introduction

 The GDPR and its implications

 Journey toward GDPR compliance

 How you can obtain Dynamics

# Introduction

## Introduction

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

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

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

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 “Earning your trust with contractual commitments to the General Data Protection Regulation” blog post by Rich Sauer, Microsoft Corporate Vice President & Deputy General Counsel.

Although your journey to GDPR 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.

## Links

“Get GDPR compliant with the Microsoft Cloud” blog post.

[BLOG POST >](#)

Read more from Brendon Lynch.

[BRENDON LYNCH >](#)

“Earning your trust with contractual commitments to the General Data Protection Regulation” blog post.

[BLOG POST >](#)

Read more from Rich Sauer.

[RICH SAUER >](#)

Visit the GDPR Section of the Microsoft Trust Center.

[TRUST CENTER >](#)







# The GDPR and its implications

## Personal and sensitive data

- Data definitions
- Data pseudonymization
- Dynamics 365 data

 Introduction

 **The GDPR and its implications**

 Journey toward GDPR compliance

 How you can obtain Dynamics





# The GDPR and its implications

## The GDPR and its implications

The GDPR is a single, binding legislative act that reflects the implementation of the Digital Single Market Strategy. It is a complex regulation that may require significant changes in how you gather, use, and manage data. Microsoft has a long history of helping our customers comply with complex regulations, and when it comes to preparing for the GDPR, we're your partner on this journey.

The GDPR imposes new rules on organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents, no matter where they are located. Among the key elements of the GDPR are the following:

- **Enhanced personal privacy rights:** Strengthened data protection for individuals within the European Union (EU) by ensuring they have the right: to have access to data, to correct inaccuracies, to erase data, to object to processing of their information, and to move their data;
- **Increased duty for protecting data:** Reinforced accountability of companies and public organizations that process Personal Data, providing increased clarity of responsibility in ensuring compliance;
- **Mandatory data breach reporting:** Companies are required to report 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 personal privacy policies, implement/strengthen data protection controls and breach notification procedures, deploy highly transparent policies, and further invest in IT and training.

## Links

Learn more about the Digital Single Market Strategy.

[WEBSITE >](#)



# The GDPR and its implications

In addition to encompassing operations of both controllers and processors in the EU, and those outside the EU who offer goods and services to, or collect personal data from, EU residents, the GDPR clarifies the rights of data subjects in relation to the types of data to be protected and enables additional mechanisms to prosecute violations.

## Personal and sensitive data

### Data definitions

As part of your effort to comply with the GDPR, you will need to understand both the definitions of personal and sensitive data and how they relate to the types of data held by your organization within Dynamics 365. Based on that understanding, you'll be able to discover how that data is created, processed, managed, and stored.

The GDPR considers personal data to be any information related to an identified or identifiable natural person. That can include both direct identification (such as your legal name) and indirect identification (such as, specific information that makes it clear it is you that the data references).

The GDPR makes clear that the concept of personal data includes online identifiers (such as IP addresses and mobile device IDs) and location data where the EU Data Protection Directive had previously been less explicit.

Sensitive personal data is afforded enhanced protections and generally requires an individual's explicit consent where these data are to be processed.

### Data pseudonymization

The GDPR also addresses the concept of pseudonymous data, or personal data which has undergone pseudonymization. This is different from anonymized data, where the direct link to personal 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. However, this type of data may not be very useful in your application.

As noted in the GDPR (Provision 28), "The application of pseudonymization to personal 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."

You can achieve data pseudonymization, for instance, if you use a "token" such as using a separate look-up table linking a person's name with a randomly gen-

### Examples of information relating to an identified or identifiable natural person (data subject)

- Name
- Identification number (such as SSN)
- Location data (such as home address)
- Online identifier (such as e-mail address, screen names, IP address, or device IDs)





# The GDPR and its implications

erated identification number (for example, "12345" is the identifier for "John Smith"). You can also use encryption where a mathematical algorithm is utilized to protect the data of a natural person. If you lose the token or encryption key, you essentially have anonymized data.

If your organization pseudonymizes your data, you will benefit from the relaxation of certain provisions of the GDPR with respect to 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."

## Dynamics 365 data

With the data definitions outlined in the GDPR in mind, let's look at data contained in Dynamics 365 and see how they relate. Microsoft defines specific data types related to its online services, such as Dynamics 365 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 discovery 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. This data could potentially contain personal data that will be governed by the GDPR.
- **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. Because a portion of this data could include personal information about a "natural person" it may fall within the GDPR.

## Link

Read the Microsoft Online Privacy Statement.

[ONLINE PRIVACY >](#)

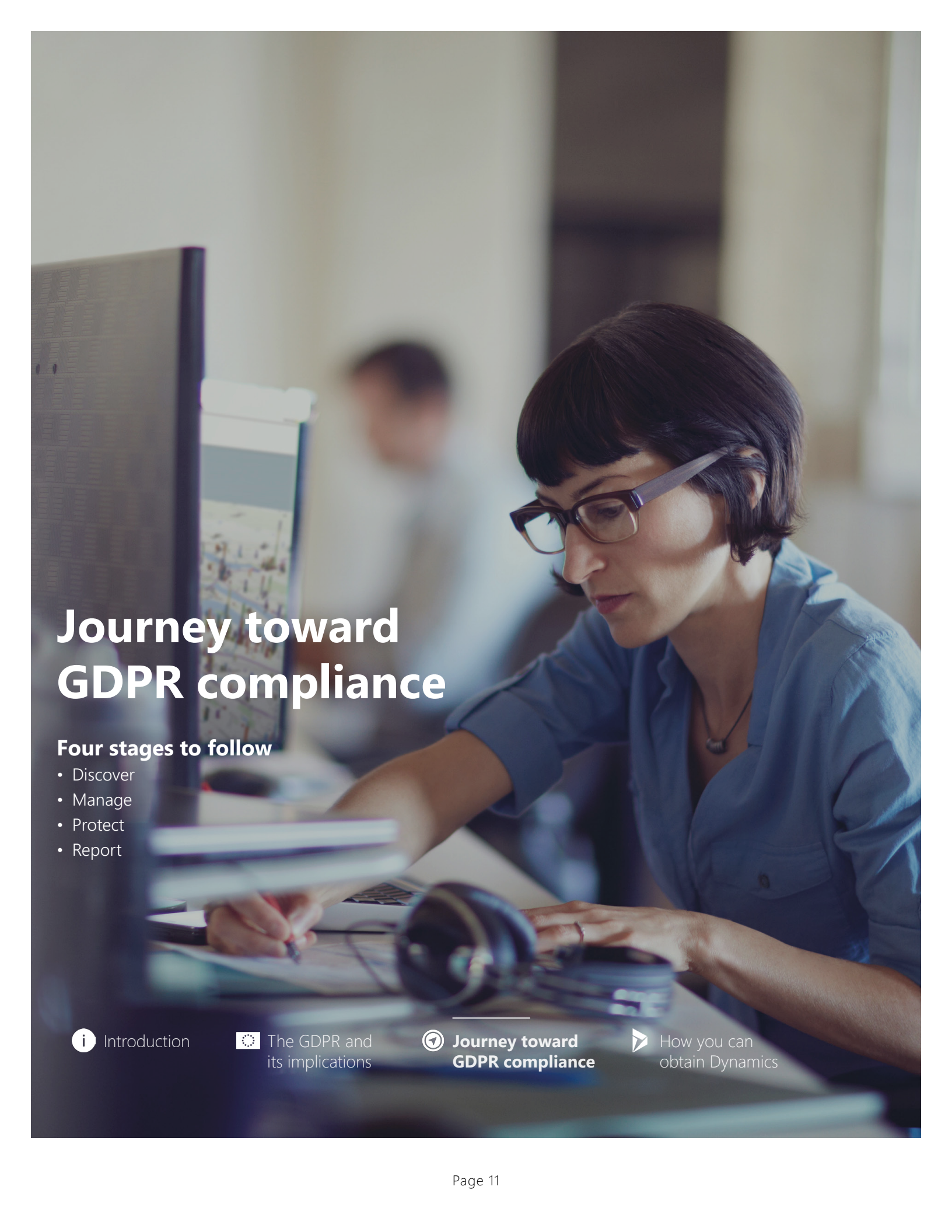


# The GDPR and its implications

- **Payment data** is the information you provide when making online purchases with Microsoft. It may include a credit card number and security code, name and billing address, and other financial data. We use payment data to complete transactions, as well as to detect and prevent fraud. The extent to which this payment data is associated with an individual rather than a corporate ID (for example, personal credit card vs. a corporate procurement card) may find that some of this data will be subject to the requirements of the GDPR.
- **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 payment data but it may contain administrator data to track the source of a support ticket logged in our systems.

In addition to the types of data noted above and the personal data described in detail in the previous section, there are specific requirements related to children. As noted in the GDPR text, children (defined as a natural person under the age of 16 or as specified by Member State law) merit specific protection about their personal data. As it relates to your Customer and/or Content data within Dynamics 365 as defined above, you as a controller will be required to obtain the consent of the holder of parental responsibility of that child regarding the use of personal data.







# Journey toward GDPR compliance

## Four stages to follow

- Discover
- Manage
- Protect
- Report

 Introduction

 The GDPR and  
its implications

 **Journey toward  
GDPR compliance**

 How you can  
obtain Dynamics

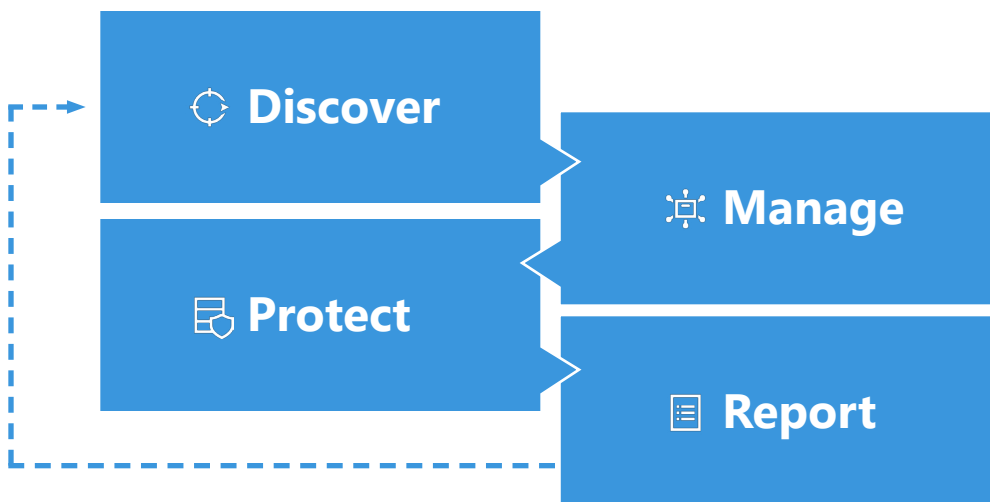
# Journey toward GDPR compliance

## Four stages to follow

*Where do you begin? How do you start the journey toward GDPR compliance as you utilize the Dynamics 365 applications?*

In the general white paper “Beginning your General Data Protection Regulation (GDPR) Journey,” 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:

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



## Link

Read the “Beginning your General Data Protection Regulation (GDPR) Journey” white paper

[WHITE PAPER >](#)

## Key GDPR steps

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

**Manage:** Govern how personal data is used and accessed.

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

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





# Journey toward GDPR compliance

 Discover

## Discover

*Identify what personal data you have and where it resides*

The GDPR has many requirements pertaining to the collection, storage, and use of personal data, making it necessary to first identify the personal data you possess about your data subjects. Once you have identified what data you are storing and using, you must classify all personal data, which with their GDPR-elevated rights, users are entitled to request.

### **Search for and identify personal data**

The GDPR has many requirements pertaining to the collection, storage, and use of personal data, making it necessary to first identify the personal data you possess about your data subjects.

*Dynamics 365 approach:* Microsoft Dynamics 365 provides multiple methods for you to search for personal data within your records, including Advanced Find, Quick Find, and Relevance Search. These functions enable you to identify personal data with greater accuracy and speed.

### **Facilitate data classification**


The GDPR has new requirements that elevate the rights of data subjects. As a result, it is necessary to classify personal data.

*Dynamics 365 approach:* The Dynamics 365 platform offers the flexibility to build an application extension around data classification, such as the Entity and Field-level. With these levels, customers can configure Forms and Views to look for personal information based on GDPR requests. At the row-level, data classification can be achieved via solution customization.

## **Questions to consider**

*How much of the personal data about your data subjects under your organization's control have you identified?*

*How confident are you in the tools your organization currently leverages to classify personal data?*



# Journey toward GDPR compliance

 **Manage**

## **Manage**

*Govern how personal data is used and accessed*

Best practice for data management under the GDPR is to implement an organizational governance program that includes the ability to notify subjects about the intended processing of personal data; obtain consent from data subjects regarding the processing of their personal data; provide a mechanism for subjects to request the discontinuation of that processing; or to have “inaccurate personal data” rectified, “incomplete personal data” completed, and personal data transferred or erased. Your data management program should also dictate how those requests will be processed, tracked, and closed.

Under the GDPR, data subjects have the right to data portability, which allows subjects to request and receive their personal data in a structured, commonly used, machine-readable format. Finally, your organization must be able to restrict the processing of data due to temporary-restriction requests on certain processing activities from data subjects.

### **Enable data governance practices and processes**

To manage data and support the rights of data subjects under the GDPR, organizations should implement a data governance program.

*Dynamics 365 approach:* Dynamics 365 provides a set of features to manage access to personal data. Dynamics 365 uses Azure Active Directory to protect your data from unauthorized access by simplifying the management of users and groups and enabling admins to easily assign and revoke privileges. Role-based security allows you to group privileges that limit the tasks a user can perform, Record-based security lets you restrict access to specific records, and Field-level security lets you restrict access to specific high-impact fields, such as those containing personally identifiable information.

## **Question to consider**

*Does your organization have a data governance program in place that meets the demands of the GDPR?*



# Journey toward GDPR compliance

 Manage

## **Provide detailed notice of processing activities to data subjects**

The GDPR requires that controllers be transparent with data subjects about the intended processing of personal data.

*Dynamics 365 approach:* Dynamics 365 provides the ability to display custom privacy notices with detailed information; this information can be displayed on a form or on the login screens of the internal and external Portals. While Dynamics 365 provides a platform capable of hosting external-facing privacy notices, it is your responsibility to ensure that the specific language of the notice meets the obligations under the GDPR.

## **Discontinue processing on request**

The GDPR requires that organizations give data subjects the right to object to the processing of their data and discontinue processing on request.

*Dynamics 365 approach:* Dynamics 365 has several tools to help you discontinue processing on request. Tools like Advanced Find, Quick Find, and Relevance Search enable you to manually discontinue processing in features of Dynamics 365, including marketing and text analytics.

## **Collect unambiguous, granular consent from data subjects**

Before processing data, the GDPR requires that controllers have a legal basis to do so, such as through the affirmative consent of the data subject.

*Dynamics 365 approach:* Dynamics 365 offers Portals, through which you can request and obtain consent prior to processing personal data. When collecting personal data, Dynamics 365 Customer Engagement allows you to create checkboxes and other elements that enable data subjects to indicate affirmative consent prior to submitting their personal data. While Dynamics 365 can provide a platform capable of hosting external-facing privacy notices, it is your responsibility to ensure that the specific language of the notice meets the obligations under the GDPR.

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

The GDPR requires that a controller processing personal data provides data subjects with a way to submit requests to rectify, erase, or transfer their personal data.

## **Questions to consider**

*Do your existing privacy notices meet GDPR requirements?*

*Would your organization currently be able to discontinue processing on request?*

*In how many cases would your organization currently be able to obtain needed consent?*

*Does your organization currently have a way for these requests to be submitted by data subjects and processed?*

# Journey toward GDPR compliance



**Dynamics 365 approach:** Dynamics 365 provides users with several tools to erase and edit personal data associated with third-party data subjects, as well as with employee user accounts. Users can manually track their requests for rectification, erasure, or transfer of personal data, and they can create support cases to track and manage data subject rights requests. Additionally, actions taken during the lifecycle of the request can be tracked, and the case can be marked as resolved upon completion. Using Portals, Dynamics 365 Customer Engagement administrators can make and receive requests pertaining to personal data.

## **Rectify inaccurate or incomplete personal data on request**

The GDPR requires controllers that process personal data to enable data subjects to request the rectification of “inaccurate personal data” and the completion of “incomplete personal data.”

**Dynamics 365 approach:** Dynamics 365 offers you several methods to rectify inaccurate or incomplete personal data. Using Excel Online, you can export, bulk edit, then re-import multiple records to Dynamics 365. You can change personal data stored as Contacts by manually amending the data element containing the target personal data. Alternatively, you can edit a single row or modify multiple rows directly using Dynamics 365 forms.

## **Erase personal data on request**

Under the GDPR, all data subjects have the right to request the erasure of their personal data by controllers.

**Dynamics 365 approach:** Dynamics 365 offers several methods to erase personal data about a data subject. With tools like Advanced Find to help you identify the personal data, Dynamics 365 enables you to easily locate and directly delete records.

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

Under the GDPR, data subjects have the right to data portability. This means they can request and receive their personal data from controllers in a structured, commonly used, and machine-readable format.

**Dynamics 365 approach:** 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 that will be included in the request and then save the data in a commonly used, machine-readable format, such as .csv or .xml.

## **Questions to consider**

*Could your organization currently rectify inaccurate or incomplete personal data if requested to do so by a data subject?*

*How would your organization currently handle a request to erase personal data?*

*If a data subject made a portability request for personal data, would your organization be able to accommodate this request?*





# Journey toward GDPR compliance

 Manage


## **Restrict the processing of personal data**

Under the GDPR, data subjects may request a temporary restriction of processing activities that utilize their data in certain circumstances, as may be the case if a data subject objects to the processing of data but the controller has a legal requirement to retain the data. Accordingly, controllers may need to employ technical means to prevent a specific data subject's personal data from undergoing certain processing activities.

*Dynamics 365 approach:* To protect sensitive information and the service availability required by the GDPR, Dynamics 365 incorporates security measures at the platform and service levels. Dynamics 365 has several tools to assist with requests to restrict the processing of personal data, such as using Advanced Find, Quick Find, or Relevance Search to manually locate the specified data and restrict processing.

## **Questions to consider**

*Would your organization currently be able to handle a request to restrict the processing of an individual data subject's personal data?*



# Journey toward GDPR compliance

 **Protect**

## **Protect**

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

Your processing activities and supporting technology must contain built-in data privacy and security controls that ensure the confidentiality, integrity, and availability of personal data. Encryption is one potential tool that satisfies the GDPR requirements for high standards of security. Should a data breach occur, once aware of the breach, you must notify regulators quickly and may also be required to notify affected data subjects. Regularly testing, assessment, and evaluation of the effectiveness of your technical and organizational security measures will help ensure that you are properly protecting personal data.

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

The GDPR requires controllers that collect or process personal data to ensure that their activities and supporting technology are built to include data privacy and security principles.

**Dynamics 365 approach:** Dynamics 365 services are developed utilizing the Microsoft's Secure Development Lifecycle, which incorporates privacy-by-design and privacy-by-default methodologies, and are in accordance with Microsoft privacy policies. Furthermore, many Dynamics 365 services are audited at least annually against several global data privacy and network security standards, including ISO/IEC 27018. Learn more at the Microsoft Dynamics 365 Trust Center.

Learn more about the global data privacy and network security standards.

[STANDARDS >](#)

[ISO/IEC 27018 >](#)

## **Questions to consider**

*Does your organization's IT resources meet this standard today?*

Learn more about Microsoft's Secure Development Lifecycle.

[WEBSITE >](#)

[PRIVACY POLICY >](#)

[TRUST CENTER >](#)



# Journey toward GDPR compliance



## Secure personal data through encryption

The GDPR requires controllers that process personal data to maintain a high standard of security. The GDPR identifies encryption as one potential tool that supports this requirement.

*Dynamics 365 approach:* 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 field-level encryption is available for a set of default entity attributes that contain sensitive information.

## Secure personal data by leveraging 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, considering the state of the business and the cost of measures.

*Dynamics 365 approach:* Dynamics 365 offers multiple tools to help safeguard data according to an organization's specific security and compliance needs. This includes 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 privileges that limit the tasks a user can perform; Record-based security, which allows you to restrict access to specific records; Field-level security, which allows you to restrict access to specific high-impact fields; and Transparent Data Encryption (TDE) and cell-level encryption. Learn more at the Microsoft Dynamics 365 Trust Center.

## Detect and respond to data breaches

The GDPR requires controllers to maintain appropriate technologies and 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 notify regulators quickly and may also be required to notify affected data subjects.

*Dynamics 365 approach:* 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.

## Questions to consider

*How much of the personal data that you currently store is encrypted?*

TDE >

TLS >

ENCRYPTION >

*Does your organization's approach to securing personal data currently meet this standard?*

TRUST CENTER >

*Does your organization currently have a process in place to handle personal data breach notifications?*

Learn more about Security Incident Responses Management processes.

LEARN MORE >



# Journey toward GDPR compliance

 **Protect**

## **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.

*Dynamics 365 approach:* Dynamics 365 provides administrative users with audit functionality that can help identify data changes, as well as highlight opportunities to improve the security posture to protect personal data and detect data breaches. Microsoft also conducts ongoing monitoring and testing of Dynamics 365 security measures. These include ongoing threat modeling, code review and security testing, live site penetration testing, and centralized security logging and monitoring.

## **Question to consider**

*Does your organization's approach to security testing meet the GDPR's testing standard?*





# Journey toward GDPR compliance

☰ Report

## ☰ Report

*Execute on data requests, report data breaches, and keep required documentation*

To show GDPR compliance through reporting, you should maintain an audit trail of all processing activities, requests, and their resolution. You will also need to track and record flows of personal data into and out of the EU and third-party service providers, as the transfer of personal data is restricted to those countries and third parties with adequate safeguards. Finally, a Data Protection Impact Assessment (DPIA) must be conducted when processing personal data that might pose a high risk to the rights and freedoms of individuals. This internal procedure evaluates potential risks and proposes appropriate mitigations.

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

Controllers should maintain records of processing activities under their responsibility. Records must contain both the nature of every request—for example, to view or rectify personal data—and their resolution.

*Dynamics 365 approach:* 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 requests by a data subject and to log events associated with amending, erasing, or transferring personal data.

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

The GDPR restricts the transfer of personal data outside of the EU to those countries with adequate safeguards or where other specified safeguards exist.

## Questions to consider

*Does your organization currently maintain records of processing activities?*

*Do you have mechanisms in place to transfer personal data outside the EU, such as Binding Corporate Rules or Standard Contractual Clauses?*

# Journey toward GDPR compliance

 Report

**Dynamics 365 approach:** Dynamics 365 reduces your need to transfer personal data out of the EU by giving you choice in where you store your data. During the initial setup, you can select data centers from more than 30 regions around the globe. 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.

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

The GDPR requires controllers to keep records of the transfer of personal data to third parties and requires that third parties meet GDPR requirements.

**Dynamics 365 approach:** Dynamics 365 customers acting as controllers are responsible for tracking distribution of personal data to third parties via their custom services and applications hosted on Dynamics 365. Microsoft maintains an inventory of third-party service providers who may have access to customer data. The Microsoft Online Services Subcontractor List covers the subcontractors for all the online services offered under the Data Processing Terms section of the Online Services Terms.

## Facilitate Data Protection Impact Assessments

Controllers must conduct a Data Protection Impact Assessment (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, privacy risks and to propose appropriate mitigations.

**Dynamics 365 approach:** Dynamics 365 enables you to use the Dynamics 365 audit log. This allows you to track and record processing activities across the Dynamics 365 ecosystem to inform your organization's DPIA processes. To help you find information that may support a DPIA addressing your use of Dynamics 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, how and where Microsoft sends customers' data, sub-processors who have access to customers' data, details on Dynamics 365 security measures, and details regarding Microsoft's privacy reviews process.

## Questions to consider

Learn more about Microsoft's contractual commitments.

[COMMITMENTS >](#)

*How frequently does your organization track and record the transfer of personal data of EU data subjects to third-party services providers?*

[PROVIDERS >](#)

*Does your organization currently conduct DPIAs?*

### Learn more

Learn what data Microsoft collects and processes.

[LEARN MORE >](#)

Learn how and where Microsoft sends customers' data.

[LEARN MORE >](#)



# Journey toward GDPR compliance

 Report

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 Dynamics 365 can support your compliance with the GDPR, as well as approaches, recommended practices, and techniques to support your GDPR compliance journey.

## Additional links

Learn more about GDPR at [Microsoft.com/GDPR](https://Microsoft.com/GDPR).

[WEBSITE >](#)

See plans and pricing for Dynamics 365.

[PRICING >](#)

## Links

Learn about the sub-processors who have access to customers' data.

[LEARN MORE >](#)

Learn about the security measures of Dynamics 365.

[LEARN MORE >](#)

Learn about Microsoft's privacy review process.

[LEARN MORE >](#)



 Introduction

 The GDPR and its implications

 Journey toward GDPR compliance

 **How you can obtain Dynamics**

# How you can obtain Dynamics

*Get started with Dynamics 365 today*

- Options for one or many products
  - Choices for any type of user
- Editions for businesses of any size

GET STARTED >