Supporting Your EU GDPR Compliance Journey

With Microsoft Dynamics 365 Business Central

Release 1

Table of Contents

Disclaimer

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

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

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

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

Published May 2018

Version 1.0

Introduction

On May 25, 2018, the General Data Protection Regulation (GDPR) comes into effect. GDPR is a European privacy and security law that establishes a new global standard for privacy rights, security, and compliance. If your organization is a Microsoft Dynamics 365 Business Central customer and a data processor or data controller as defined by the GDPR (see the GDPR Glossary online for definitions), then 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 organizations 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 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.

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 toward GDPR compliance may seem challenging, we are here to help you. For specific information about the GDPR, our commitments, and to begin your journey, please visit the GDPR section of the Microsoft Trust Center.

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. Business Central 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 Business Central. While compliance with the GDPR is mandatory in the specific situations outlined below, this document is not a "check box" exercise. Rather, the content is intended to help you enhance your overall data protection and privacy capabilities.

This GDPR-related white paper is focused on Business Central. Other GDPR white papers have been created for all the Dynamics 365 Customer Engagement Plan Business Applications that includes:

- Dynamics 365 for Sales
- Dynamics 365 for Customer Service
- Dynamics 365 for Project Service Automation
- Dynamics 365 for Field Service

A similar set of GDPR-related white papers have been developed for the Dynamics 365 Unified Operations Plan Business Applications that includes:

- Dynamics 365 for Finance and Operations

- Dynamics 365 for Retail
- Dynamics 365 for Talent

In addition to the Dynamics 365 Business Central capabilities outlined in this white paper, Microsoft has announced the Compliance Manager, a cross–Microsoft Cloud Services solution designed to help organizations meet complex compliance obligations like the GDPR. It performs a real-time risk assessment that reflects your compliance posture against data protection regulations when using Microsoft Cloud Services, along with recommended actions and step-by-step guidance. Learn more about Compliance Manager.

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 for how Business Central can help address your needs in each of the four stages.

In this paper, some sections, where the context so permits, refer to "you" as a customer. References to "we" or "us" in this paper are to Microsoft.

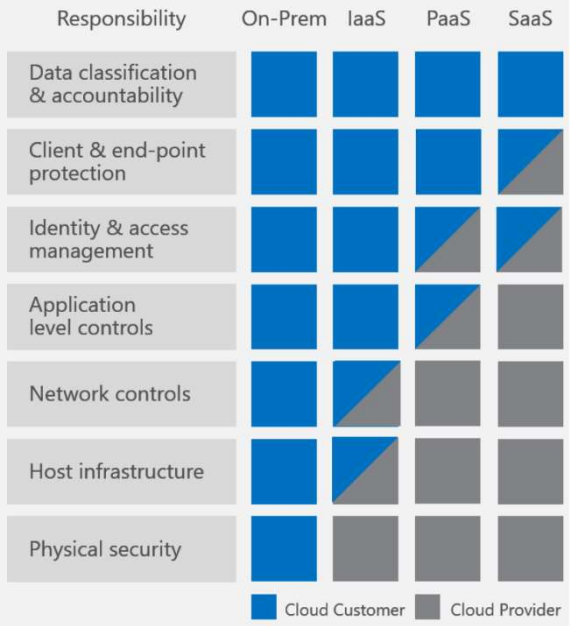
Shared Responsibility Model

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 and summarized in the overview section below. Depending upon which of the Dynamics applications you have, you may find that you are both a 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 are summarized graphically below.

As this model relates to how you utilize Microsoft Dynamics, you will find that you have a version that:

- Runs on-premises where you are in both the controller and processor roles. Microsoft may choose to provide important features but is not directly involved with your GDPR compliance unless you have enabled capabilities like Microsoft Watson or other similar features that may return personal data to Microsoft.
- Is an on-premises version of Dynamics but you are using IaaS to host the solution. You remain the controller and processor for the personal data that remains on your premises, but Microsoft may choose to provide important controls for you.
- Is a SaaS version of Dynamics (e.g., Dynamics 365) where you are the controller and Microsoft is the processor and provides important controls.



The GDPR and Its Implications

The GDPR is a complex regulation that may require significant changes in how you gather, use and manage personal 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 European Union (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 EU. Among the key elements of the GDPR are the following:

- **Enhanced personal privacy rights** - strengthened data protection for individuals within the EU by ensuring they have the right to: access their personal data, correct inaccuracies in that data, have their personal data erased upon request, object to the processing of their personal data, and move their personal data;
- **Increased duty for protecting personal data** - reinforced accountability of companies and public organizations that process personal data, providing increased clarity of responsibility in ensuring compliance;
- **Mandatory personal data breach reporting** - companies are required to report personal 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 personal data protection controls and breach notification procedures, deploy highly transparent policies, and further invest in IT and training.

Key GDPR Compliance Roles

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.

- **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 within the EU, in relation to the processing of their personal 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 personal 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 personal 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 personal 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, processor, or both 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 personal 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 Dynamics 365 Business Central, 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 personal data breach. For more information on how Microsoft addresses these obligations visit the Microsoft Dynamics Trust Center.

Personal 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 Business Central. Based on that understanding, you will 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 (your legal name) and indirect identification (specific information that makes it clear it is you the data references).

The GDPR makes clear that the concept of personal data includes online identifiers (such as IP addresses, mobile device IDs) and location data.

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

Information relating to an identified or identifiable natural person (data subject) - examples

- Name
- Identification number (such as a social security number)
- Location data (such as a home address)
- Online identifier (such as email address, screen names, IP address, or device IDs)

Data Pseudonymization

The GDPR also addresses the concept of pseudonymous data, or personal data which has been separated from its direct identifiers so that linkage to an identity is no longer possible without additional information which is being stored separately. 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.

As noted in the GDPR (Recital 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."

If your organization pseudonymizes its data you may benefit from the relaxation of certain provisions of the GDPR, such as personal 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 manage your compliance obligations and mitigate 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 Business Central Data

With the data definitions outlined in the GDPR in mind, let's look at data contained in Dynamics 365 Business Central and see how they relate. Microsoft defines specific data categories related to its Cloud Services, such as Dynamics 365 Business Central, 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 Cloud 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 email and attachments, Power BI reports, SharePoint Online site content, IM conversations, or data about your interactions with customers.
- **Administrator data** is the information about administrators supplied during signup, purchase, or administration of Microsoft Cloud 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.
- **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.
- **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 personal data subject to the GDPR.

Journey Towards 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 Business Central product?

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:

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.

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 Business Central is not a comprehensive "how to," we have included links for you to find out more details. You can find more online as described in the Microsoft Trust Center section.

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 Business Central 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 Dynamics 365 Business Central and the GDPR

As described above, the scope of GDPR is intended to apply to the processing of personal data whatever technology is used. Because Business Central may be used to process personal data there are certain requirements within the GDPR (as noted by the references to regulation Articles contained in the GDPR below) where Business Central 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 personal data and receive information on the processing of that data, to rectify personal data if incorrect, and to request the erasure of their personal data, sometimes known as the "right to be forgotten". You should ensure any personal 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 personal data detailing categories of data subjects and the personal 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 personal 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 Business Central 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** – Business Central is built using the Security Development Lifecycle, a mandatory Microsoft process that embeds security requirements into every phase of the development process. Azure Active Directory helps protect Business Central from unauthorized access by simplifying the management of users and groups. In addition, Business Central enables you to assign and revoke privileges to these accounts easily.

  For example, Microsoft uses encryption technology to protect your data while at rest in a Microsoft database and when it travels between user devices and our Azure datacenters. Dynamics 365 Business Central 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.

- **Privacy** – You are the owner of your data. We do not mine your data for advertising. If you ever choose to terminate Dynamics 365 Business Central, 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 Cloud 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, Dynamics 365 Business Central, 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. For more information, see Microsoft Trust Center Transparency.

If your organization collects, hosts, or analyzes personal 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.

Business Central and the GDPR Journey

In this section, you will see how key features within Business Central can be brought to bear on the important steps of your journey toward GDPR compliance – Discover, Manage, Protect, and Report. It should be noted that there are many other ways of achieving GDPR compliance, and you can customize your Business Central solution design to meet your business and solution requirements.

Key Messaging

Dynamics 365 Business Central helps you comply with GDPR regulations to:

- Obtain explicit consent from customers to process their data by providing integration and customization capabilities to create notifications to inform customers about how their data will be used.
- Respect data subject rights by:
    - Supporting correction, erasure, or access of your customers' personal data.
    - Enabling portability of your customers' personal 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 the ability to grant or restrict access to personal data at multiple levels and also encrypting personal data in transit and at rest in Microsoft datacenters.
    - Enabling audit trails to help document compliance with GDPR regulations.

Discover - Identify and classify personal data

The ability to clearly identify where you store personal data and classify fields for personal data can help to serve as a foundation for subsequent tasks and requirements under the GDPR.

You can build extensions for Business Central and classify table fields using the DataClassification property to assign *data classification*s such as: customer content, end user identifiable information, organization identifiable data, or system metadata.

This data classification feature can help you categorize any personal data by setting the data sensitivity classification. For example, an extension includes a table, My Table, with three fields, Name, Email, and Last Modified By. You can classify the Name and Email fields as Customer Content and the Last Modified By field as *EndUserIdentifiableInformation*. Then you can use this information to determine if personal data persists in this table.

As a controller, you can further define or refine the data sensitivity classification in the new Data Classification Worksheet by setting the data sensitivity, such as Sensitive, Personal, Company Confidential or Normal, to document what kind of data you store in standard and custom fields. Using the Data Classification Worksheet, you can set the data sensitivity in Excel, for example.

Most, but not all, personal data is likely to reside in one of the following tables in Business Central:

- Customer
- Vendor
- Contact (when of type Person)
- Employee
- Salespeople/Purchaser
- Resource (when of type Person)
- User

Personal data may also exist in tables that are related to these listed above. The exact tables containing personal data depend on customizations to your Business Central solution.

Business Central provides methods for you to search for personal data, including capabilities to sort and filter to find the data. The list of tables above (and related tables) help narrow down such a search.

Such classifying and setting data sensitivity in the above-mentioned master tables (and related tables) can assist with identifying and classifying personal data more precisely and finding data in customized tables as well. Using filtered search of all levels of classification that you, the customer, have in the specific solution can help you to identify places where personal data resides in Business Central.

While Business Central provides functionalities that facilitate your identification and classification of personal data, it is your responsibility to ensure that personal and sensitive data are located and classified appropriately to meet your obligations under the GDPR.

Discover - Key Takeaways

- There is potential for personal data to reside within Dynamics 365 Business Central.
- As the controller, you are responsible for identifying personal data that you have collected and responding to data subject requests. This may require you to utilize the customization capabilities of Dynamics 365 Business Central.

Manage - Data Subject Rights (DSR)

The GDPR allows data subjects to exercise various Data Subject Rights (DSR) relative to their personal data. While Business Central has tooling and documentation that assist you with responding to those DSR requests, the decision to honor a DSR request and the implementation thereof is your responsibility. These capabilities are described in the Manage sections below.

Manage - Export data subject's personal data

Under the GDPR, a data subject has the right to make a data portability request from a data controller, meaning, in part, that you must export the data subject's personal data from your systems and provide the same to the data subject in a structured, commonly used format. The above-described data classification (see the Discover - Identify and classify personal data section) will help administrators identify personal data, thereby making it easier to locate personal data for responding to export requests from a data subject.

Once personal data in Business Central is identified and located, it can be exported to an Excel file to facilitate a data portability request. Using Excel, you can edit the personal data that will be included in the request and save the data in a commonly used, machine-readable format, such as .csv or .xml. Business Central data can also be exported using Rapid Start configuration packages. If you are an administrator with the company that uses Business Central, in the configuration packages, you can configure master data tables and their related tables that contain personal data.

While Business Central provides capabilities for exporting, and thereby accessing, personal data, it is your responsibility to ensure that personal and sensitive data are located and classified appropriately for you to meet your obligations under the GDPR. For more information, see the Discover - Identify and classify personal data section.

Manage - Delete data subject's personal data

Under the GDPR, a data subject has the right to request the data controller to delete its personal data. The above-described data classification (see the Discover - Identify and classify personal data section) will help administrators identify personal data, thereby making it easier to locate personal data for responding to delete requests from a data subject.

Business Central gives you several methods for correcting inaccurate or incomplete personal data, or erasing personal data regarding a data subject using the customization capabilities, but the decision and implementation is your responsibility. In some cases, you may choose to use the Business Central windows to directly edit your data, such as modifying or deleting a contact.

While Business Central provides capabilities for deleting personal data, it is your responsibility to ensure that personal and sensitive data are located and classified appropriately for you to meet your obligations under the GDPR. You can also use customization capabilities of Business Central to add further tooling to help you with properly locating and classifying data. For more information, see the Discover - Identify and classify personal data section.

Manage - Modify data subject's personal data

Under the GDPR, a data subject has the right to request rectification of inaccurate personal data concerning the data subject. Business Central gives you the following methods for correcting inaccurate or incomplete personal data. In some cases, you can export data to Excel to quickly bulk-edit multiple Business Central records, then reimport the data to Business Central. For more information, see Exporting your Business Data to Excel. You can also amend stored personal data by manually editing the field containing the personal data, such as editing information about a customer in the Customer card.

Certain types of Business Central records, namely business transaction records (such as general, customer, tax ledger entries) are essential to the integrity of the enterprise resource planning system. Thus, the modification of personal data in such records is restricted. If you store personal data in such business transaction records, you can use the Business Central customization capabilities for any decision you make to honor a DSR to modify such personal data.

While Business Central provides capabilities for modifying personal data, it is your responsibility to ensure that personal and sensitive data are located and classified appropriately for you to meet your obligations under the GDPR. For more information, see the Discover - Identify and classify personal data section above.

Manage - Mark people, customers, and vendors as blocked due to privacy

Under the GDPR, a data subject has a right to restrict the processing of its personal data. When you receive such a request from a data subject, you can mark the data subject's record as blocked due to privacy. Business Central will then discontinue the processing of that data subject's personal data.

Business Central includes support for marking records, such as customers, vendors, or resources, as blocked due to privacy. When a record is marked as blocked, you cannot create new transactions that use that record. For example, you cannot create a new invoice for a customer, when either the customer or the salesperson is blocked.

If the restriction on that data subject's personal data is lifted, then you can mark the data subject as unblocked by removing a checkmark. After that, Business Central will again allow transactions that use that record, such as creating new invoices for that customer.

Manage - Manage data subject requests

Because data subjects can make multiple requests under the GDPR, you are expected to keep track of all incoming requests and any actions you make as a result of a request. You can manually track data subject requests for rectification, erasure, or transfer of personal data by using the Cases functionality in Dynamics 365 for Customer Service if you have a subscription. Users can create support cases to track and manage data subject rights requests in the Dynamics 365 for Customer Service application.

The use of the Service Level Agreements capabilities in Dynamics 365 for Customer Service can help ensure that you can address requests in a timely manner. Of course, it is your responsibility to configure your SLA in the Dynamics 365 Customer Service application in a manner that adheres with the timelines within the GDPR. Additionally, actions taken during the lifecycle of the request can be tracked in the case, and then marked as resolved in Dynamics 365 for Customer Service upon your completion of the request.

Alternatively, you can use the customization capabilities of Business Central to support the tracking of data subject requests.

Manage - Provide detailed notice of processing activities to data subjects

The GDPR requires any business to notify their customers of how it manages personal data. To provide a detailed notice of processing activities to your customers, you can use the Dynamics 365 portal capabilities available in Dynamics 365 for Sales, a platform capable of hosting a customer's external-facing privacy notices. When your prospective customers register themselves on websites that use this Dynamics 365 portal platform, they can then access your custom privacy notice. It will be your responsibility to ensure that the specific language of the notice meets your obligations under GDPR.

For internal users of Business Central you can use the customization capabilities of Business Central to facilitate your ability to display your organization's own privacy notice to them or use the capabilities in Azure AD (AAD) to present a such a notice.

Manage - Enable data governance practices and processes

Business Central provides you with a set of features to manage access to personal data by users and groups. Using Business Central user setup, you can assign permissions that limit the tasks a user can perform. The role-based security that permissions and user groups rely on lets you restrict access to specific records. The Business Central security architecture enables an extensible data security framework for securing or filtering data based on permissions.

Manage - Restrict the processing of personal data

Business Central helps you protect personal data and service availability as required by the GDPR by incorporating security measures at the platform and service levels. With Business Central, administrative users grant and restrict user access to personal data through user groups, restricting access to individuals or groups of users.

Manage – Key Takeaways

- Business Central helps you respond to DSRs and gives you several methods for correcting, erasing, and/or exporting personal data regarding a data subject using the customization capabilities, but the decision and implementation is your responsibility.
- You can block people's data from being processed per their request through a DSR. As the controller, you need to make sure that any data export files that you author based on Dynamics 365 Business Central are consistent with your interpretation of the GDPR requirements.

Protect - Data protection and privacy by design and default

Business Central is developed using the Microsoft Security Development Lifecycle, which incorporates privacy-by-design and privacy-by-default methodologies, and in accordance with Microsoft privacy standards. To demonstrate Microsoft's commitment to the privacy and security of customer data, the out-of-the-box Microsoft provided version of Business Central is audited at least annually against various compliance offerings, including ISO 27001, ISO 27017, ISO 27018, SOC 1 Type 2, and SOC 2 Type 2 reports.

Protect - Secure personal data through encryption

Business Central uses technology such as SQL Server with Transparent Data Encryption (TDE) to encrypt data at rest and Transport Layer Security (TLS) for all communications between browser client and server. Additionally, Microsoft's key platform, productivity, and communications services will encrypt customer content as it moves between our datacenters.

Protect - Detect and respond to data breaches

Dynamics 365 Business Central deploys security measures intended to help 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.

Depending on your role as a data controller or a data processor, the GDPR obligates you to report and notify the relevant supervisory authority, affected data subjects and/or data controller of certain types of personal data breaches.

Protect - Facilitate regular testing of security measures

As one of the cornerstones of GDPR, the regulation reinforces and imposes an increased duty for protecting personal data. This includes administrators monitoring access to personal data.

As an administrator, you can grant users permissions to data based on their role in Business Central. Administrators can also apply security filters so that users can, for example, see data about one customer but not other customers. For more information, see Data Security.

Business Central also provides administrative users with audit functionality that can help identify opportunities and improve the security posture to protect personal data. Use the Change Log Entries window to audit data access. For more information, see Logging Changes in Business Central.

Microsoft also conducts ongoing monitoring and testing of Dynamics 365 Business Central security measures. These include ongoing threat modeling, code review, security testing, live site penetration testing, and centralized security logging and monitoring.

Protect – Key Takeaways

- You can use the security architecture and role-based security to protect the data integrity and privacy in a Dynamics 365 Business Central organization.
- Microsoft Dynamics 365 Business Central supports an auditing capability where certain personal data changes within an organization can be recorded over time for use in analysis and reporting purposes.

Report - Maintain and report on audit trails to show GDPR compliance

An important aspect of the GDPR is to maintain audit trails and other evidence to demonstrate accountability and compliance with the GDPR requirements. In Business Central, you can track and record data changes in a Business Central environment. The data and operations that can be audited in Business Central 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

You can use logging and auditing tools in Business Central to log and track events associated with amending, erasing, and creating data, roles, and privileges. This ability is based on the audit trail and role-based security in Business Central.

For more information, see Logging Changes in Business Central and Manage Users and Permissions in Business Central.

Report - Track and record flows of personal data into and out of the EU

Business Central lets you reduce the need for transfer of personal data outside of the EU by storing your data in an Azure datacenter that is in your geographic region.

Additionally, Microsoft has made several contractual commitments related to Dynamics 365 business applications that enable the appropriate flow of personal data within the Microsoft ecosystem.

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

Business Central customers acting as controllers are responsible for tracking distribution of personal data to third party custom services and applications. Microsoft maintains an inventory of subcontractors who may have access to customer data and is expanding that process to additional products and scenarios to meet GDPR compliance needs.

Report - Facilitate Data Protection Impact assessments

Business Central offers audit capabilities to help inform your Data Protection Impact Assessment (DPIA).

In addition, 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; Microsoft privacy standards; access to data controlled by Microsoft; details on Dynamics 365 security measures; and details regarding the Microsoft privacy reviews process.

Report – Key Takeaways

- Dynamics 365 Business Central can help you track and record data changes and the flow of data for audit trail and other evidence to demonstrate accountability and compliance with GDPR.
- The audit capabilities in Business Central can help support and inform your Data Protection Impact Assessment (DPIA).

Microsoft Trust Center

The Microsoft Trust Center has many tips for how other Microsoft products and services offer additional assistance with GDPR compliance. Both if you are a Business Central customer, a good starting point is the GDPR Frequently Asked Questions section in the Microsoft Trust Center.

How You Can Obtain Business Central

Get started with Business Central today

- Connect and grow your business
- Get an end-to-end view of your business
- Take the next steps for your business
- Meet your specific business needs using prebuilt solutions from AppSource

Dynamics 365 Business Central is an all-in-one business management solution that's easy to use and adapt, helping you connect your business and make smarter decisions. If your business is growing and ready to take on more opportunities, Business Central can help.

Learn more about security and compliance for Dynamics 365