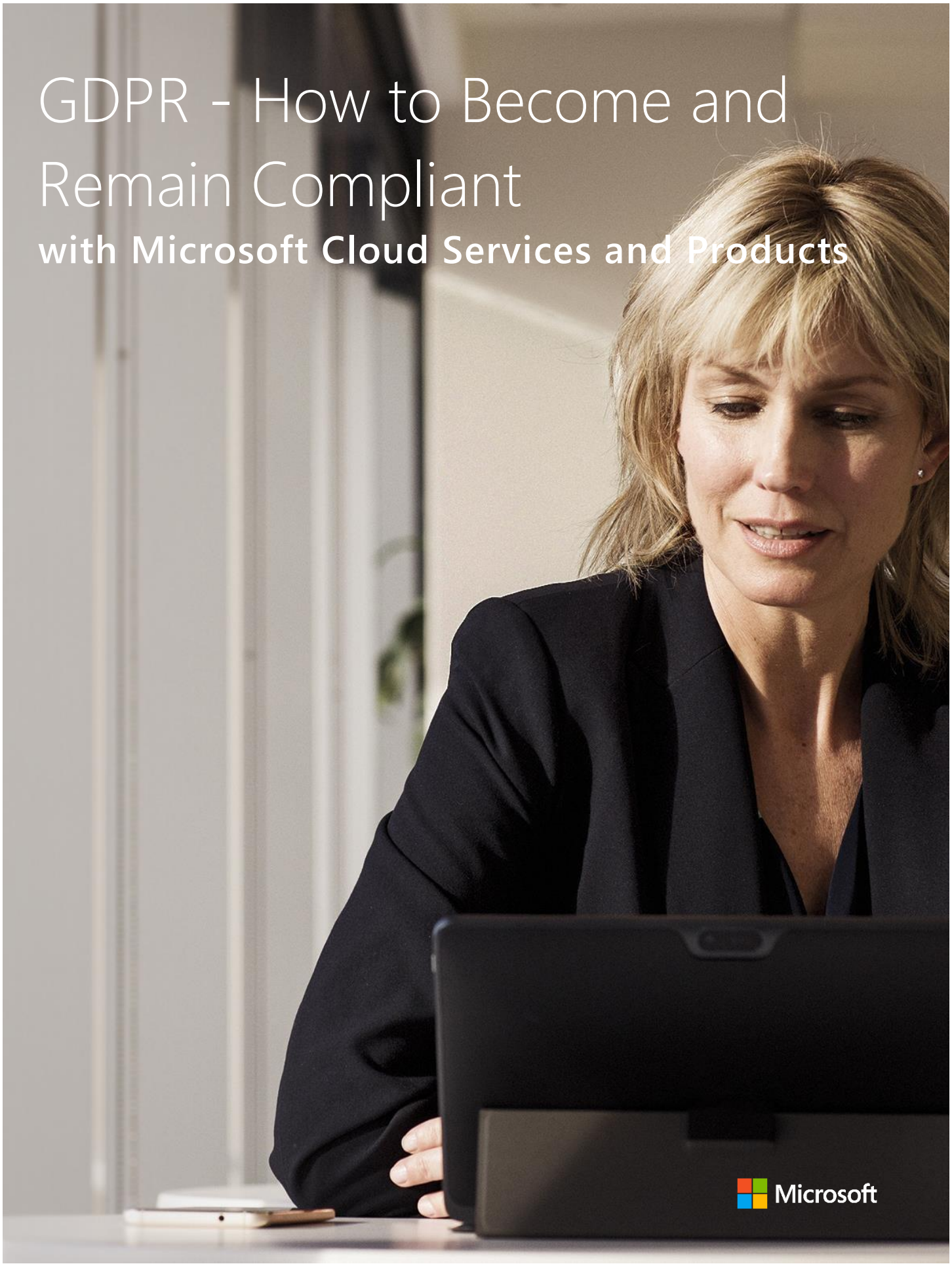
GDPR - How to Become and Remain Compliant

with Microsoft Cloud Services and Products



This page is intentionally left blank.

Contents

Notice

This white paper comments on the General Data Protection Regulation (GDPR) as Microsoft interprets it on the date of publication. We have spent a lot of time reflecting on the objectives of the GDPR and its meaning. However, the implementation of the GDPR can only be based on established facts; some of the aspects and interpretations of the GDPR are not yet well established.

Therefore, this document is provided for informational purposes only and should not be relied upon as constituting any legal opinion or how the GDPR may apply to you and your organization. We encourage you to work with a suitably qualified professional to discuss the GDPR, to verify how it will specifically apply to your organization, and to determine how best to ensure compliance.

MICROSOFT DISCLAIMS ALL WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, IN RELATION WITH THE INFORMATION CONTAINED IN THIS WHITE PAPER. The white paper is provided "AS IS" without warranty of any kind and is not to be construed as a commitment on the part of Microsoft.

Microsoft cannot guarantee the veracity of the information presented. The information in this white paper, including but not limited to internet website and URL references, is subject to change at any time without notice. Furthermore, the opinions expressed in this white paper represent the current vision of Microsoft France on the issues cited at the date of publication of this paper and are subject to change at any time without notice.

Publication: January 2018
Version 1.0

Abstract

In the age of digital transformation, privacy and improved security have become key issues. The General Data Protection Regulation[1] (GDPR) defines a new important step in privacy, security, and compliance.

The GDPR imposes many requirements and obligations for organizations around the world. Compliance with this regulation will require significant investments in data management and protection solutions for a large number of organizations and enterprises.

Microsoft customers who are subject to the GDPR, whether processing data in house, in the cloud, or in hybrid configurations, must ensure that personal data within their systems is properly processed and protected according to the principles of the GDPR. This requirement means that many customers will have to revise or modify their data processing procedures, the implementation of these processes, and the security of these processes as stipulated in the GDPR.

Microsoft has significant experience in successfully managing the principles of data protection and in complying with complex regulations. This experience finds its expression in the products and cloud services provided by Microsoft that can help its customers to achieve both the principles and objectives of the GDPR and meet its privacy requirements in their data processing. In this context, this paper highlights the benefits of solutions that can help organizations on the path to compliance with the GDPR.

[1] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL 2016 ON THE PROTECTION OF NATURAL PERSONS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA, AND REPEALING DIRECTIVE 95/46/EC (GENERAL DATA PROTECTION REGULATION): http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

Introduction

After more than four years of negotiations, which began when the Commission presented its proposals in January 2012, the Council of Europe adopted on 14 April 2016 the General Data Protection Regulation[2], more commonly referred to by its English acronym "GDPR" (and hereinafter referred to as the GDPR).

The GDPR came into force on May 24 of that year and will be applicable directly in all member states after a period of two years, on May 25, 2018, less than one year from the date of publication of this white paper.

The GDPR is fundamentally concerned with the issue of protecting the privacy of individuals and enabling them to exercise their privacy rights. To this end, the GDPR establishes a set of the most stringent global requirements imposed on organizations in terms of protection of privacy. These requirements govern how organizations must manage and protect personal data of individuals in the EU while respecting their individual choices, no matter where the data is processed, stored, or sent.

Thus, Microsoft and its customers have now set out on the path to achieve the privacy objectives set by the GDPR. Microsoft believes that privacy is a fundamental right, and that the GDPR represents an important advance in terms of privacy and protection of related rights. At the same time, we recognize that the GDPR will impose significant changes on organizations around the world.

In this context, and as Brad Smith, Chairman and Chief Legal Officer of Microsoft Corporation, points out, "The new Regulation significantly raises the bar on privacy, security, and compliance."

An initial white paper GDPR - ORGANIZING AND IMPLEMENTING THE RIGHT PROCESSES FOR COMPLIANCE WITH THE GDPR[3] suggests the outline of a program and a roadmap to achieve compliance with the GDPR. It addresses some important questions, such as relations with subcontractors, the security of personal data, and the notification of the supervisory authority, to mention just a few key points.

On the strength of this foundation program template, we feel that it is now important to explain how, with on-premises solutions and cloud services, Microsoft can help you to locate and catalog personal data in your systems' processing operations to build a more secure hybrid environment and to simplify the management and monitoring of personal data.

For example, Microsoft cloud services, such as Microsoft Azure[4], Microsoft Dynamics 365[5], and Microsoft Office 365[6], will facilitate the processes that you must implement to achieve compliance with the GDPR, thanks to artificial intelligence (IA) technology, innovation, and collaboration.

---

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation): http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[3] GDPR - ORGANIZING AND IMPLEMENTING THE RIGHT PROCESSES FOR COMPLIANCE WITH THE GDPR: https://aka.ms/GDPRprocess-en

[4] Microsoft Azure: https://azure.microsoft.com/en-us/

[5] Microsoft Dynamics 365: https://dynamics.microsoft.com/en-us/

[6] Microsoft Office 365: https://products.office.com/en-us/

Note Microsoft Azure is an expanding collection of integrated IaaS and PaaS-type cloud services – compute, storage, networks, databases, advanced analytics, mobile, web, APIs, and so on - that enable Microsoft customers to go faster and make savings in the implementation of their processing activities. Azure is a development environment (for DevOps, for example), a hosting service, and a service execution and management environment to host, scale, and manage applications and processing activities on the internet.

Note Microsoft Dynamics 365 is the next generation of smart business applications that enable organizations of all sizes to grow, change, and transform themselves in order to meet all the needs of their customers and seize new opportunities. It combines existing Microsoft cloud services, in terms of software for customer relationship management (CRM) and enterprise resource planning (ERP), in a single service, with new specific applications that help manage the specific functions of an enterprise (marketing, customer knowledge, sales, finance, customer services, operations, automation of project services, and so on).

Note Microsoft Office 365 is designed to respond to the needs of business organizations in terms of high reliability, security, and user productivity. Office 365 includes the familiar Microsoft Office suite, with cloud-based versions of the latest generation of Microsoft collaboration and communication services that use the internet to help users be more productive, almost anywhere, and on any device.

By moving forward with a "hyper-scale" cloud service provider (CSP) like Microsoft and taking advantage of cloud services such as Azure, Dynamics 365, and Office 365, your organization can benefit from an economy of compliance. Microsoft cloud services enable you to reduce programming efforts and the administrative burdens required to achieve compliance with the GDPR.

Note For more information, read the blog post ACCELERATE YOUR GDPR COMPLIANCE WITH THE MICROSOFT CLOUD[7] by Julia White, Microsoft Corporate Vice-President of the Cloud Platform.

Objectives

This white paper attempts to illustrate the benefits of Microsoft products and cloud services on the path to compliance with the GDPR, in terms of the technical aspects of implementing appropriate security controls. (In view of this purpose, this paper addresses organizational measures only very briefly, or not at all).

The adopted approach is pragmatic and can easily be activated for organizations through the study of a few fictitious data processing activities. The goal is to illustrate a series of typical situations in the collection, processing, and storage of personal data.

For global processing, these situations enable the three possible states of the data (at rest, in use, and in transit) to be addressed.

The means of achieving compliance with the GDPR for this processing of personal data represent an opportunity to put Microsoft technologies, products, and cloud services into perspective as part of a concrete, end-to-end approach.

[7] ACCELERATE YOUR GDPR COMPLIANCE WITH THE MICROSOFT CLOUD: https://blogs.microsoft.com/blog/2017/05/24/accelerate-gdpr-compliance-microsoft-cloud/

Organization of this white paper

In order to meet the objectives set out above, and beyond a reminder of the Microsoft commitments to the GDPR, this document is organized into the following sections:

- DID YOU SAY "PROCESSING OF PERSONAL DATA"?
- TAKE THE MEASURES TO ACHIEVE COMPLIANCE
- CONCLUSION

We hope you will find this organization of the paper to be progressive and clear in the different areas that it covers.

Audience for this white paper

This document is intended for Chief Security Officers (CSOs), Risk Management Officers, Chief Privacy Officers (CPOs), Compliance Officers, Chief Data Officers (CDOs), Chief Digital Information Officers (CDIOs), Data Protection Officers (DPOs), IT professionals, security specialists, and systems architects interested in understanding the pillars of the GDPR and how to ensure that their organizations' standards and practices in terms of security and protection of privacy help them to comply with the GDPR.

Reminders of Microsoft commitments to the GDPR

Microsoft underlined its commitment to the GDPR and how we support our clients in the blog post GET GDPR COMPLIANT WITH THE MICROSOFT CLOUD[8], published by our Privacy Officer Brendon Lynch[9], and the blog post EARNING YOUR TRUST WITH CONTRACTUAL COMMITMENTS TO THE GENERAL DATA PROTECTION REGULATION[10] by Rich Sauer[11], Vice President and Deputy General Counsel of Microsoft.

Since September 1, 2017, this commitment has been included in Microsoft Online Services Terms[12] (OST).

Although the path to GDPR compliance may appear difficult, we are here to help.

> **Note** For specific information about the GDPR, Microsoft commitments, and the start of your roadmap, visit the special GDPR section[13] in the Microsoft Trust Center[14].

[8] GET GDPR COMPLIANT WITH THE MICROSOFT CLOUD: https://blogs.microsoft.com/on-the-issues/2017/02/15/get-gdpr-compliant-with-the-microsoft-cloud/#4J5lDmd47PkIv6xL.99

[9] Brendon Lynch's blog: https://blogs.microsoft.com/on-the-issues/author/brendonlynch/

[10] EARNING YOUR TRUST WITH CONTRACTUAL COMMITMENTS TO THE GENERAL DATA PROTECTION REGULATION: https://blogs.microsoft.com/on-the-issues/2017/04/17/earning-trust-contractual-commitments-general-data-protection-regulation/#6QbqoGWXCLavGM63.99

[11] Rich Sauer's blog: https://blogs.microsoft.com/on-the-issues/author/rsauer/

[12] LICENSING TERMS AND DOCUMENTATION: http://go.microsoft.com/?linkid=9840733

[13] GDPR section of the Microsoft Trust Center: http://www.microsoft.com/GDPR

[14] Microsoft Trust Center: https://www.microsoft.com/en-us/trustcenter

Did you say "processing of personal data"?

A representative processing scenario

This white paper uses a representative data processing scenario to illustrate how Microsoft products and cloud services can help your organization become and remain compliant.

This scenario puts the concrete benefits on the path to compliance with the GDPR into perspective. At the same time, it illustrates certain activities in the programmatic approach described in the white paper GDPR – GET ORGANIZE AND IMPLEMENT THE RIGHT PROCESSES FOR COMPLIANCE WITH THE GDPR.

This scenario, which constitutes a common thread running throughout this white paper, is proposed by the fictitious company Litware 369 in France.

Litware 369 is a fictitious company with many partners

Litware 369 specializes in the residential alarms market. It offers a broad selection of connected alarms for different types of residences, plus a range of services to address the most diverse needs for remote surveillance and on-site intervention.

This company works with a network of partners for the installation of alarm systems, the delivery of services and options, the monitoring of the alarm services, and so on.

To be represented and present locally, Litware 369 has built tight partnerships with partners established in each region in France, or within each large town in a region.

The company's activity has grown following the launch of a new generation of innovative connected alarms. Consequently, it had to improve (the quality of) its presence on the internet, including new web interfaces. This presence has come in the form of:

- A new institutional website to promote its offers and take orders online
- A new Customer portal for the management of existing service contracts
- A new Partners portal for the acceptance of orders and the management of customer installation files

These B2C (business-to-consumer) and B2B (business-to-business) web interfaces are supported by a semi-automated processing flow for the entire process, from taking the order to the actual delivery of the ordered services.

These new interfaces and the processing flows are used to collect and process subscription orders to set up the services, which is their ultimate purpose.

In view of the nature of the data that is collected, used, and stored, these data processing operations fall within the category of personal data processing covered by the GDPR.

This new processing means that, in this precise case – other processing operations set up at Litware 369 may require the same approach – Litware 369 must comply with the GDPR by meeting its numerous objectives and requirements.

The planned processing operation

As briefly outlined above, the purpose of the processing operation is to collect and process subscription orders with a view to setting up the services.

To remain representative of the processing operations used in real life, or at least of certain facets, we wanted to use a scenario that is implemented in a hybrid manner, that is with some components of the

processing hosted internally on a Litware 369 on-premises information system (IS) but with some cloud services, too. This type of implementation represents the capacity to use existing internal resources – an Active Directory instance, a SQL Server database, and a Windows Server file server – while also benefitting from the relevant enhancements of functionality proposed by the public cloud in support of Litware 369's digital transformation. This approach shortens the time-to-market capability of the Litware 369 order-taking and processing environment, offers a better technical response to some of the specific requirements of the processing, and adds greater agility.

Moreover, this representative scenario provides the ability to develop processing that is distributed between a data controller and a data processor, according to the GDPR terminology – in this case Microsoft – for the Azure, Dynamics 365, and Office 365 cloud services.

> **Note** Article 4[15] of the GDPR introduces the different roles and concepts involved in the protection of personal data and, in particular, those of the data controller and data processor. In practice, it is the responsibility of the data controller to implement appropriate technical and organizational measures to ensure that processing of personal data is consistent with the objectives and requirements of the GDPR. Furthermore, the data controller must be able to demonstrate that this is effectively the case at any time.
>
> When data processors are employed, such as Microsoft in this case for the cloud services in question, the data controller must ensure that they provide sufficient guarantees to enable them to comply with the GDPR and to process personal data according to their instructions, in particular with regard to transfers outside of the European Union.

This so-called representative scenario enables us to envisage not only B2B collaboration with partners in the processing, but also B2C access for customers. These aspects are at the heart of the digital transformation, in the quest for new usages and the definition of new business models.

By definition, this new processing must be duly mapped out, at least as far as the design and construction are concerned, in terms of the services, applications, and repositories used to build it and of the corresponding data flows and lifecycle.

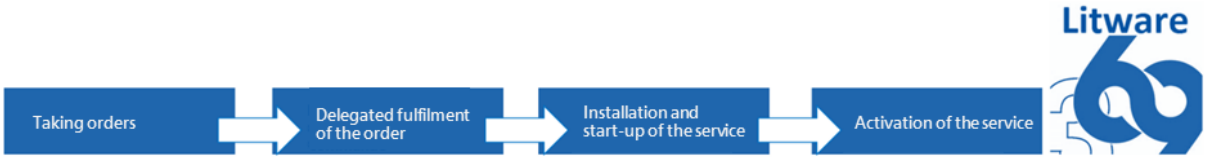
The next section shows the main steps of the processing scenario.

[15]Article 4 – Definitions: https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre1#Article4

The steps of the processing scenario

The processing scenario covers four steps:

1. Take orders
2. Delegated fulfilment of the order
3. Installation and start-up of the service
4. Activation of the service



The following sections describe the execution of these steps in the planned processing operation. In this context, they also describe certain aspects of the implementation required to understand the changes, actions, and controls proposed in this document. Specifically, these points concern the technical aspects of the processing in terms of products, cloud services, applications, and data repositories.

Take orders

As mentioned earlier, the Litware 369 institutional website can be used to subscribe to an offer of connected alarms and to certain options, depending on the offer.

This website is implemented using the Azure App Service[16], a PaaS (platform as a service) offering, which is designed to host high-performance cloud applications for web and mobile customers. This website can be accessed anonymously, without authentication.

Dedicated pages are available to browse through the various offers available with the new range of connected alarms and to subscribe to one of them that may appear to be particularly suitable. Technical information brochures can be downloaded on demand for more information about the solutions that are offered in the form of services.

> **Note** The salespeople in Litware 369 sales force have a mobile application to take orders when meeting prospects or on the occasion of consumer trade fairs. We will return to this point later in this paper (see section PROTECT DATA IN MOBILE DEVICES AND MOBILE APPLICATIONS).

[16] Azure App Service: https://azure.microsoft.com/en-us/services/app-service/

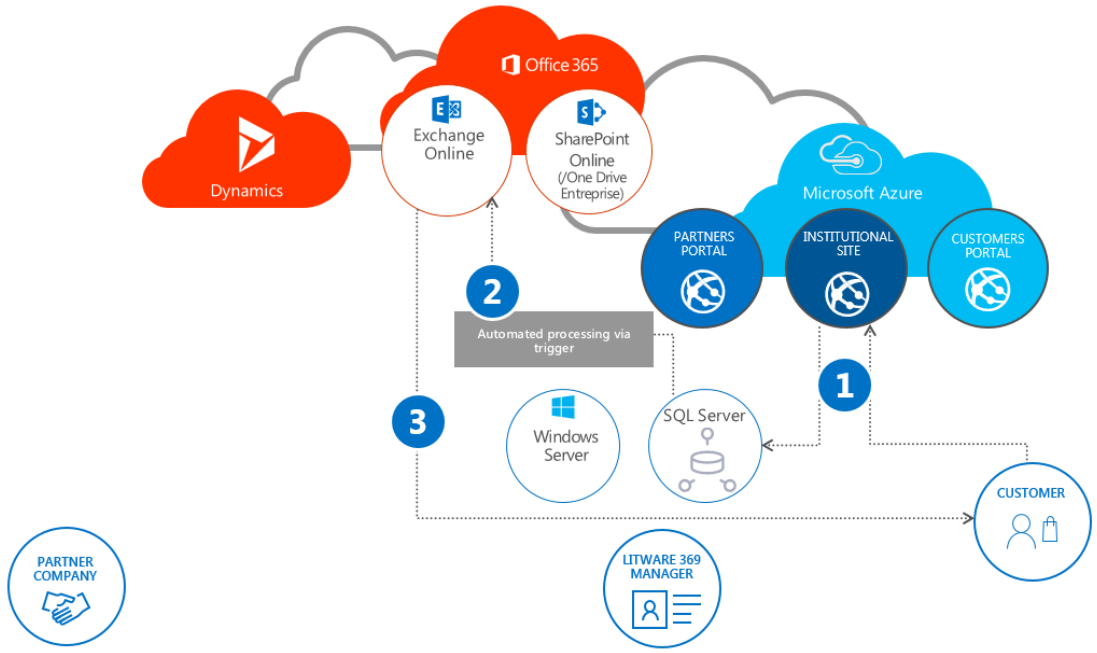


Figure 1. Overview of the order-taking process

When taking an order, the contact (and future customer) has to provide the following data:

- Contact information: Name, first name, complete address, phone number
- Other information required to fulfill the order: the chosen offer of a connected alarm along with the options, the type of residence, and so on.

When placing the order, information about the use of this data already appears on the page, along with a request for explicit consent to use this data to process the order.

The fact that this information will be shared with Litware 369 partners in the region where the contact's residence is located is clearly mentioned. A link is available to open the complete list of partner companies with their full contact details, their registry number in the corresponding region, with a link to the company's site where appropriate, and so on.

Additional links can be used to view Litware 369 practices in terms of privacy.

When confirming the order:

1. An order number is created automatically for the order and its date is registered.
2. A confirmation email is sent to the contact, containing the order number, the date of the order, a recap of the order, information about the next steps of the order fulfillment process, a link to track the order, a link to withdraw and cancel the order within 14 days, and so on.

The orders placed on the institutional website are registered in an internal SQL Server database. This database can be accessed from the website using the capacities of the Azure App Service hybrid connections[17].

Order confirmation closes the first step of the processing scenario.

[17] AZURE APP SERVICE HYBRID CONNECTIONS: https://docs.microsoft.com/en-us/azure/app-service/app-service-hybrid-connections

Delegated fulfilment of the order

The second step of the processing scenario starts with a daily extract of new orders. This extract is produced by region in the form of .CSV files (one per order) containing all the information about the order.

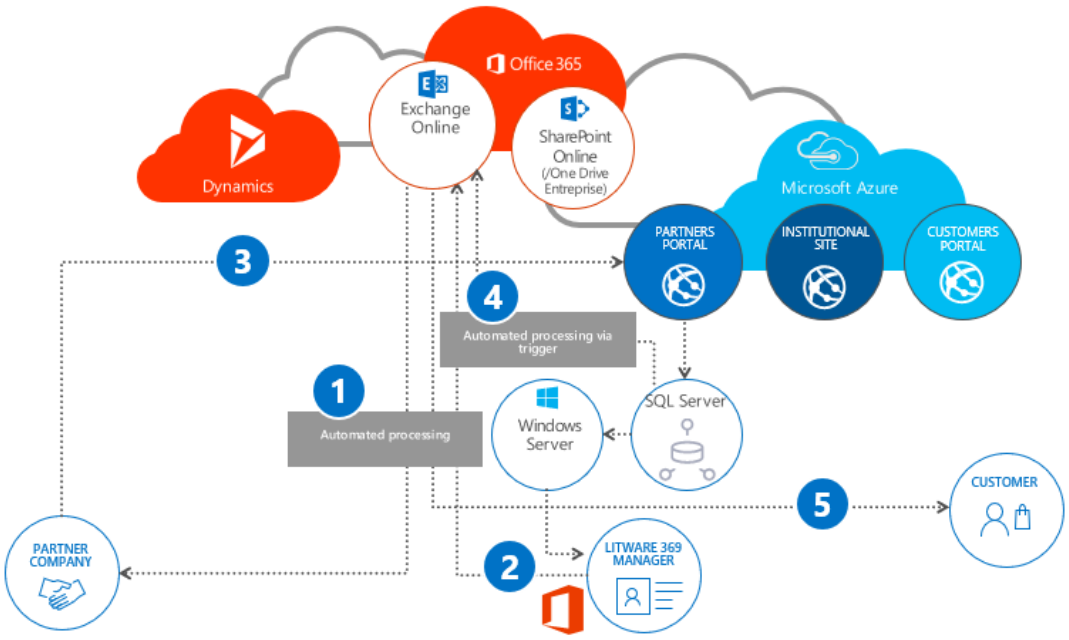


Figure 2. Overview of the delegated fulfilment of an order

The .CSV files are stored on an internal Windows Server file server, with one folder per region.

The manager in charge of each region of the Litware 369 partners entity emails the orders to the qualified partner(s) in the region for acceptance and fulfilment.

For greater simplicity, and because it does not make any difference for purposes of this white paper, we will assume that only one partner company is tasked with the effective fulfilment of open orders by region.

> **Note** Another possible variant for Litware 369 would consist calling on a number of partner companies and operating in "first to accept/first served" mode, for example.

A custom software add-in for Outlook is used to process the .CSV files automatically when producing the email messages, each of which is sent to a duly and previously defined address for each partner company.

> **Important note** At this point, we will introduce a deviation to the established process. In view of their proximity to the partner company qualified and selected for the region, some of the managers in the partners entity do not follow this process.
>
> Some of the managers simply copy the daily .CSV files into different shared cloud repositories (such as Box, Dropbox, and so on). Others send email messages to professional mailboxes that are not subject to a convention.

The partner company sends its acceptance of each order it receives to the Litware 369 Partners portal. To do this, the partner company updates the open order and changes its status. An appointment date and possible times for the appointment are registered for the order (order number).

This modification generates and sends an appointment email to the contact. This email contains the order number, the information on the proposed appointment, information about the partner who will make the installation and start the service, a link to change the appointment, a link to track the open order, and so on.

Unsurprisingly, from a technical perspective, the Partners portal also uses Azure App Service. However, it requires authenticated B2B access for the partner companies. To this end, each partner company has a generic account that is provided by the Litware 369 IS department.

The same internal SQL Server is used in this step, with the same means of connection from the Partners portal – that is, over the Azure App Service hybrid connections.

The authenticated access uses a table of partner accounts in the internal SQL Server database that contains one generic account per partner. The password is not stored directly. A subprocess is used to salt the password and to calculate a hash using the SHA-256 algorithm. This result is stored.

The third step of the processing scenario is described in the following section.

Installation and start-up of the service

As its name indicates, this step of the processing scenario corresponds to the effective fulfilment of the order. At the appointment with the customer, the partner company installs the connected alarm that corresponds to the purchased offer and starts the service, in accordance with the selected options of the offer.

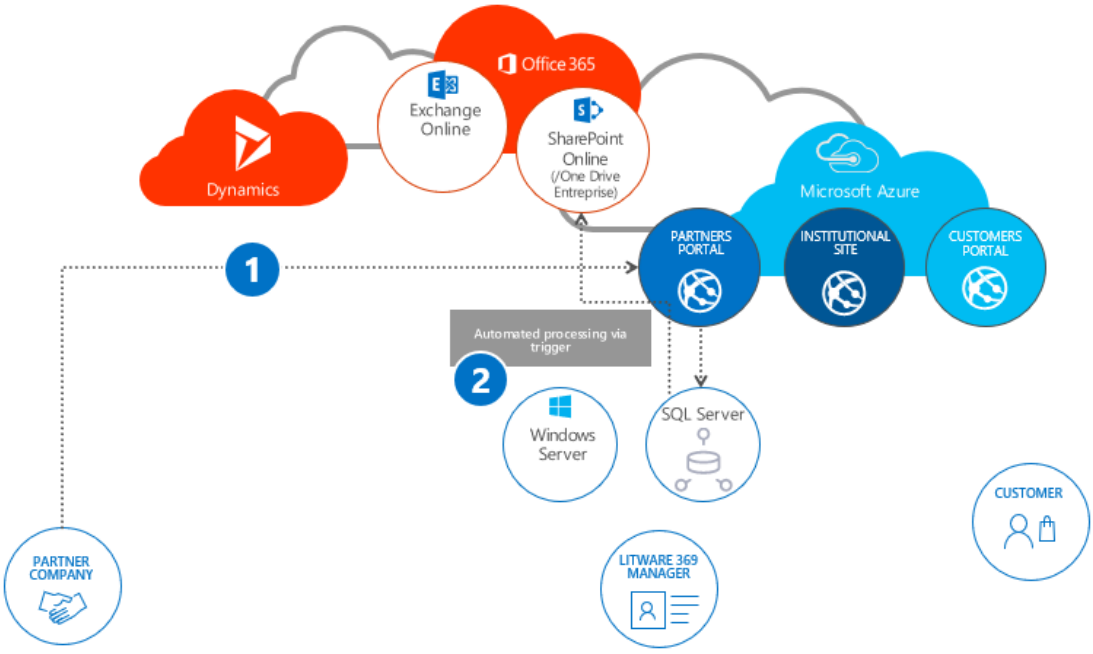


Figure 3. Overview of the installation and start-up of the service

After the appointment is completed, the partner company uses the same Partners portal to update the order with the technical characteristics of the installation, from the perspective of the complete activation of the service and the technical infrastructure options specifically installed by Litware 369 for the new range of connected alarms.

Note This technical infrastructure is based on Microsoft Azure IoT Suite[18], which includes a number of services from the Azure environment, with custom extensions in the form of preconfigured solutions that facilitate the start-up of IoT projects. These preconfigured solutions[19], which provide remote monitoring and predictive maintenance solutions, constitute the basic implementations of the common IoT solution models that were so appealing to Litware 369, thanks to their functionality and capacities, and the possibility of quickly deploying the IoT solution that forms the foundation of the company's new range of connected alarms.

Important note This white paper does not discuss any details of the data processing operations related to the connected alarms.

A customer identifier is created in the customer database for access to the Litware 369 Customer portal. This database is hosted on the same internal SQL Server. The Customer portal also consists of another application deployed in the Azure environment using the Azure App Service. As in previous cases, the database can be accessed over the Azure App Service hybrid connections.

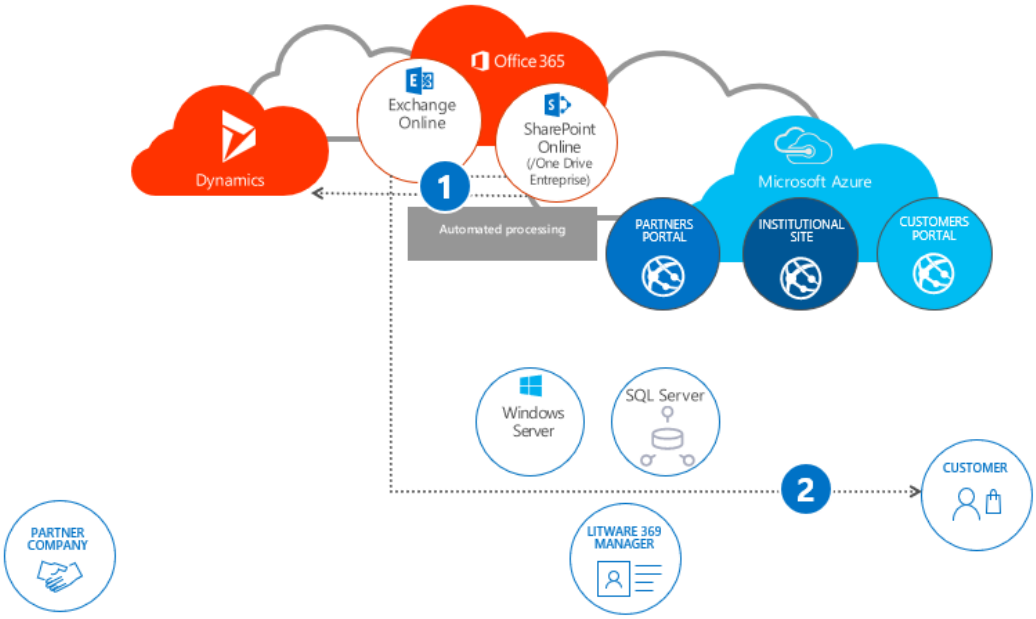
This Customer portal, which can be accessed from the Litware 369 institutional website, requires customer authentication. By default, the telephone number is used for identification purposes. A password is generated when the customer accesses the portal for the first time (see next step) by verifying the person using an account activation code. The first part of the code is sent to the telephone number in a text message. The second part is sent by email to the address specified in the order.

Finally, this step of the processing scenario includes a daily extract of the closed orders. The extract process automatically generates the completed orders as Microsoft Word forms and inserts them in a Litware 369 SharePoint Online library.

The following section describes the fourth step of the processing scenario.

Activation of the service

In the fourth and final step of the processing, the Word forms are processed by the Litware 369 Subscriptions entity.



[18] Azure IoT Suite: https://www.microsoft.com/en-us/internet-of-things/azure-iot-suite

[19] WHAT ARE AZURE IOT SUITE PRECONFIGURED SOLUTIONS?: https://docs.microsoft.com/en-us/azure/iot-suite/iot-suite-what-are-preconfigured-solutions

Figure 4. Overview of the activation of the service

A new customer account and a new contract are created in Dynamics 365 to invoice the subscription to the connected alarm offer, to manage the contract, and so on.

A confirmation email is sent to the customer that contains all the connection information that is required to manage the subscription and any related requests. As mentioned in the previous step, the telephone number is the default identifier. The email also requests bank account details for invoicing purposes.

This step concludes the description of the data processing scenario that must meet the objectives and the requirements of the GDPR.

Take the measures to achieve compliance

Activities required for compliance in the processing scenario

The implementation of a GDPR program on the path to compliance with the GDPR typically involves four main steps in the resultant processes and framework:

1. **DISCOVER.** Identify personal data that you have and where it resides.
2. **MANAGE**. Govern access to and the use of personal data.
3. **PROTECT**. Prevent, detect, and respond to any vulnerabilities and personal data breaches.
4. **REPORT.** Maintain the required documentation, and handle requests for personal data and infringement notifications.

Because the scope and the scale of GDPR programs vary from one organization to another, Litware 369 has already conducted a self-assessment of its global maturity with regard to its context and the main requirements of the GDPR using the GDPR Assessment[20] tool.

This tool, a questionnaire, is free of charge, available online, and provides a benchmark according to the four main activity categories discussed earlier. Where appropriate, it indicates the Microsoft solutions that may help meet GDPR requirements. We will return to this point later in the white paper.

Moreover, and looking beyond the technological dimension of things (which usually represents less than 20% of the whole), the elementary activities related to these main steps have to be integrated by adopting the best suited approach to the company (and any Agile-based practices that it uses in its programs and projects).

Microsoft suggests a programmatic approach, a detailed description of which is provided in the white paper GDPR – GET ORGANIZED AND IMPLEMENT THE RIGHT PROCESSES FOR COMPLIANCE WITH THE GDPR[21]. The proposed program uses a multicycle approach based on a PDCA (Plan-Do-Check-Act) model that seems to be particularly relevant in this context.

[20] GDPR Assessment: https://www.gdprbenchmark.com/

[21] GDPR – GET ORGANIZE AND IMPLEMENT THE RIGHT PROCESSES FOR COMPLIANCE WITH THE GDPR: https://aka.ms/GDPRprocess-en

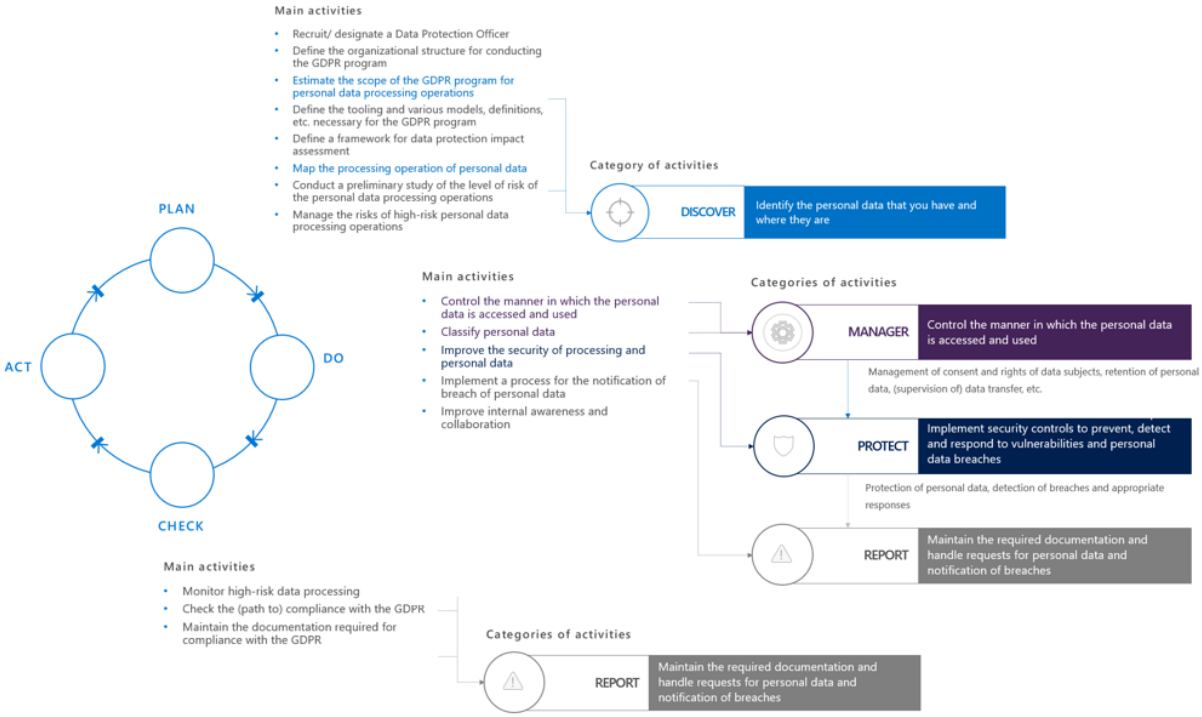


Figure 5. Consolidated view of the main activities to be carried out during a PDCA cycle, grouped by main categories

The previous main steps and their elementary activities naturally fit into the phases of this PDCA model: **PLAN, DO, CHECK** and **ACT**.

The rest of this white paper adopts this organization to cite examples of Microsoft products and functionality offered by its cloud services that can be used in a GDPR program and in the activities that typically take place in this context.

These examples are used to meet the objectives and the requirements of each of these main steps on the path to compliance with the GDPR, with reference to the previous representative scenario and the processing of personal data. Each main step is covered by a specific section. The following section involves the first step, or the discovery of personal data.

Discover - Identify personal data that you have and where it resides

This first main step of discovering personal data corresponds to a series of activities in the **PLAN** phase (of the PDCA model) of the GDPR program suggested in the white paper GDPR – GET ORGANIZE AND IMPLEMENT THE RIGHT PROCESSES FOR COMPLIANCE WITH THE GDPR.

At this stage, we assume that several activities in the **PLAN** phase have already been completed in order to accomplish the following:

- Select and appoint a data protection officer (DPO) at Litware 369, where appropriate.
- Set up the organizational structure of the GDPR program in accordance with the objectives and processes required to achieve the duly established and expected results.
- Define the tools and the various models required to conduct the GDPR program.
- Determine and prioritize the portfolio of personal data processing operations, including the associated services, applications, and repositories.

In our scenario, the scope has been deliberately reduced to a processing whose purpose, principles, and various components have already been described. This initial map includes the processing, the locations of the storage of personal data, and the management of its lifecycle. We also have a vision of the controls in place to protect it, which will enable us to check that these controls are sufficient and used correctly in the following steps, to guarantee compliance with the GDPR.

However, we must still check that our knowledge of the implementation and its use at Litware 369 is accurate and complete. One of the requirements of the GDPR consists of making sure that the description in the records of the processing activities is up-to-date, and that the technical and organizational security measures taken are effective and correctly described.

To begin, we need to determine whether the map available for the representative processing scenario is relevant and complete.

Complete the existing map

The identification of personal data collected, stored, and processed by an organization like Litware 369, and consequently the detailed knowledge of the associated processing activities, is a prerequisite for meeting the objectives and the requirements of the GDPR.

The goal consists of listing personal data and mapping out the processing activities precisely and comprehensively, according to the declarations of the businesses, branches, divisions, departments, entities, and so on of the organization, and even beyond.

Discover the cloud applications in your environment and gain an in-depth visibility of user activity

This section looks into the scenario of using repositories such as Box and Dropbox to send orders to the partner companies. As mentioned previously, this practice constitutes a deviation from the planned processing operation.

Subscribing to and using a cloud application is easier than ever before, and various entities in companies like Litware 369 avoid their own IT departments when they are not sufficiently attentive and/or responsive. Consequently, these entities meet their own business needs with cloud applications that are not centrally managed. This "Shadow IT" inevitably raises a number of challenges in terms of security

and privacy, and the usual security paradigms in the realm of perimeter security are shaken. (The article HOW SAAS ADOPTION IS CHANGING CLOUD SECURITY[22] offers an interesting take on this issue.)

The goal is to identify this "Shadow IT" dimension, and the corresponding applications and risks, to control any unidentified assets related to GDPR.

To protect personal data, such data must first be comprehensively identified. In practice, there are no means of gaining the visibility to apply the necessary controls of applications (and therefore of the corresponding processing activities and personal data) that a company like Litware 369 does not have the capacity to control. As the blog post WHY YOU NEED A CASB FOR GDPR COMPLIANCE[23] points out, these applications must be "brought out of the shadows."

To do so, it must be possible to identify personal data in transit and at rest for a broad selection of applications in the cloud, to assess the risks according to the identified cloud service providers / subcontractors, and, ultimately, to control flows of personal data and data transfers.

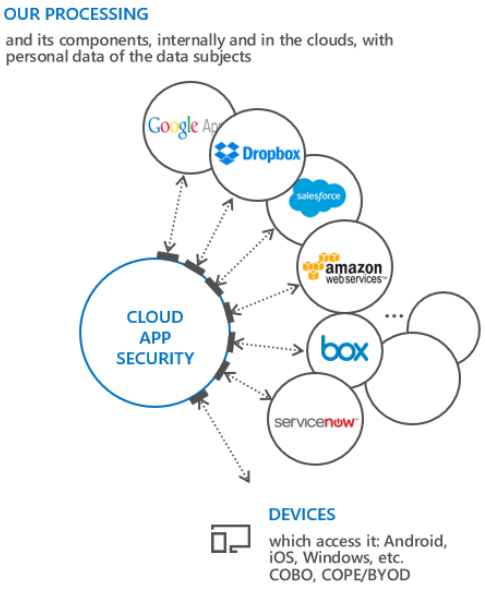


Figure 6. Discover cloud applications with Cloud App Security

In this case, Cloud App Security[24] can be used to discover all the cloud applications in the Litware 369 environment, without any agents, thanks to a constantly growing catalog of more than 15,000 cloud applications supplied by Microsoft teams of analysts. It is also possible to identify the users of these applications and how they use them. A risk score is produced for each application that can be used to assess them with regard to the regulatory certifications and accreditations, sector-specific standards, and other good practices. This risk assessment can be used to authorize (or not) the users to access these applications. In other words, like at Litware 369 and thanks to this catalog, Cloud App Security can be used to identify the use of applications in your organization to analyze the risks incurred according

[22] HOW SAAS ADOPTION IS CHANGING CLOUD SECURITY: http://www.darkreading.com/perimeter/how-saas-adoption-is-changing-cloud-security-/a/d-id/1316015

[23] WHY YOU NEED A CASB FOR GDPR COMPLIANCE: https://blog.cloudsecurityalliance.org/2017/04/04/need-casb-gdpr-compliance/

[24] PROFESSIONAL-LEVEL SECURITY FOR YOUR CLOUD APPLICATIONS: https://www.microsoft.com/en-us/cloud-platform/cloud-app-security

to more than 60 objective criteria and, where appropriate, to forbid the use of these applications by defining scripts for the organization's on-premises network equipment.

> **Note** For more information, see the article WHAT IS CLOUD APP SECURITY?[25] and view the webinars INTRODUCING MICROSOFT CLOUD APP SECURITY[26] and GET VISIBILITY, DATA CONTROL AND THREAT PROTECTION WITH MICROSOFT CLOUD APP SECURITY[27].

Easily identify data

To continue identifying the data, this section considers the use scenario of SharePoint Online if the latter was not listed in the map that was produced previously.

Control assets like SharePoint Online with Cloud App Security

As previously noted, Cloud App Security provides a series of application connectors to integrate the solution with cloud applications, such as Office 365 in this case. The application connectors use the cloud application vendors' APIs to extend control and protection. They also provide access to data directly from these applications in the cloud for analysis by Cloud App Security.

Cloud App Security can then provide visibility, control, and protection against threats to the data stored in these applications. Security in the cloud can be configured by defining and implementing policies in cloud applications and solutions from third parties and Microsoft. In short, when Cloud App Security detects an anomaly, you receive an alert.

Quickly identify personal data in Office 365 with advanced eDiscovery

Looking beyond this integration with Office 365, we would like to point out that the Office 365 environment is not left out. By way of example, the search functionality of Office 365 eDiscovery[28] can be used to search for text and metadata in Litware 369 Office 365 resources (SharePoint Online, OneDrive Enterprise, Skype Enterprise Online, and Exchange Online).

Thanks to machine learning technology (one of the branches of AI), advanced eDiscovery can quickly identify documents relevant to a specific subject (for example, an open order) with greater precision than traditional searches by key words, or a manual examination of a large number of documents.

> **Note** For more information, refer to the paper REDUCE EDISCOVERY COSTS AND CHALLENGES WITH OFFICE 365 ADVANCED EDISCOVERY[29] and view the webinar OFFICE 365 ADVANCED EDISCOVERY[30].

---

[25] WHAT IS CLOUD APP SECURITY?: https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security

[26] INTRODUCING MICROSOFT CLOUD APP SECURITY: https://youtu.be/DyUmFWfJQvU

[27] GET VISIBILITY, DATA CONTROL AND THREAT PROTECTION WITH MICROSOFT CLOUD APP SECURITY: https://youtu.be/zPS1_WuGSW8

[28] Office 365 compliance solutions: https://products.office.com/en-us/business/compliance-tools-ediscovery

[29] REDUCE EDISCOVERY COSTS AND CHALLENGES WITH OFFICE 365 ADVANCED EDISCOVERY: https://blogs.office.com/2015/12/10/reduce-ediscovery-costs-and-challenges-with-office-365-advanced-ediscovery/

[30] OFFICE 365 ADVANCED EDISCOVERY: https://youtu.be/yPEGF3Auw_M

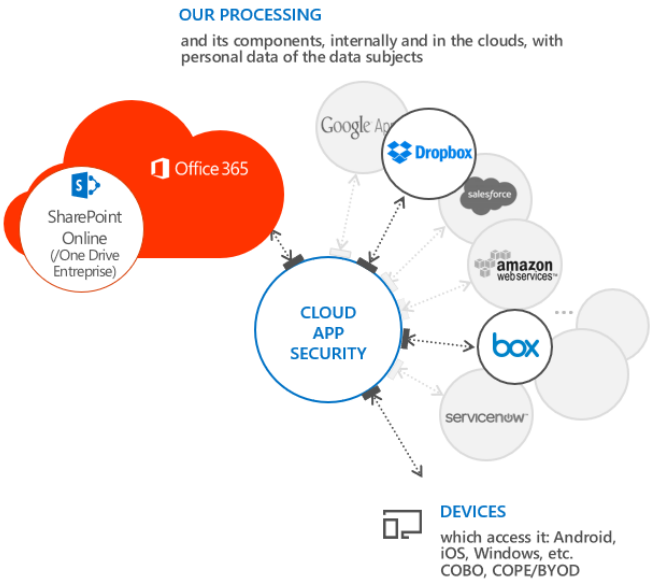


Figure 7. Identify SharePoint Online data with Cloud App Security and Advanced Data Governance in Office 365

Update the records of processing activities

The previous steps have enabled Litware 369 to verify the reality of the processing in terms of implementation, and therefore to update the inventory data.

This inventory is kept in a processing record and, in accordance with article 30, contains the following information.

- **For the data controller and the data processor**, that is, for the Microsoft Azure, Dynamics 365, and Office 365 cloud services, and the network of partner companies in France (for the installation of its alarm systems, the start-up of the services and options, monitoring of the services, and so on):
    - The name and contact details of the data controller / data processor, the representatives, and in particular the data protection officer, if, there is one.
    - Where appropriate, any transfers of personal data to third-party countries, with the name of the country and the documentation of the measures taken to protect the data, if the transfer is made on legitimate grounds. In our scenario, this applies to Microsoft cloud services (see next section).
    - A general description of the technical and organizational security measures (where applicable). In this context, the various measures illustrated in the section THE STEPS OF THE PROCESSING SCENARIO are specified in relation to the four main planned steps of the processing.
- **For the data controller**:
    - The purpose of the processing. In this case, the collection of subscription orders and their processing, with a view to setting up the service for the selected connected alarm and options.
    - The categories of the data subjects. In this case, the contacts and (future) customers of the purchased offer.
    - The categories of personal data. In this case, the name, first name, full address, and telephone number collected when the order is taken.

    - The recipients of the data processing. In this case, the future customer and the partner company that qualifies, installs, and starts the purchased offer.
    - The retention periods, where applicable.

- **For each data processor:**
    - The names and contractual details of each data processor in the data processing chain, and the type of processing performed by each data processor (see next section).

The notion of processing records is addressed in the white paper GDPR – GET ORGANIZE AND IMPLEMENT THE RIGHT PROCESSES FOR COMPLIANCE WITH THE GDPR.

In the GDPR program implemented by Litware 369, the records of processing activities take the form of a SharePoint Online library. This library is part of a program management environment based on the GDPR Activity Hub[31] software stub, made available by Microsoft in open source on the community forge GitHub to help organizations get started and make progress on the path to compliance with the GDPR.

The objective of this stub is to provide organizations with a basis for keeping track of all core activities, associated tasks, essential events, requests received, and so on for compliance with GDPR requirements.

Update the records of data processor risks

As mentioned in the previous steps, Litware 369 also specified the information about data processors and third parties involved in the processing.

Litware 369 also uses the GDPR Activity Hub to materialize the notion of records of data processor risks.

The processing record completed in the previous section enables Litware 369 to identify and review all the processor contracts, and to demand that the latter take account of the obligations and responsibilities of the GDPR that are incumbent on data processors. The term used is co-responsibility.

This term means that Litware 369 must check that the contractual clauses applying to the protection and security of personal data are present. Regarding Microsoft, as an identified data processor, and for the Azure, Dynamics 365, and Office 365 cloud services used in the processing, Litware 369:

- Can call on the resources of the GDPR section[32] of the Microsoft Trust Center for the cloud services in question.
- Review the corresponding Online Services Terms (OST)[33].
- Decide on the location of the data for these services. For example, like for Office 365[34] when it is used by the Litware 369 Subscriptions entity, and for any transfers of personal data to third-party countries, see the WHERE YOUR DATA IS LOCATED[35] in the Microsoft Trust Center.

  In practice, customers who want to keep their data in a specific geographical location, such as the European Union for Litware 369, can take advantage of the Microsoft global datacenter

[31] GDPR Activity Hub: https://github.com/SharePoint/sp-dev-gdpr-activity-hub

[32] THE GENERAL DATA PROTECTION REGULATION (GDPR): https://www.microsoft.com/GDPR

[33] Licensing Terms and Documentation: http://go.microsoft.com/?linkid=9840733

[34] WHERE IS MY DATA?: http://o365datacentermap.azurewebsites.net/

[35] Where your data is located: https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located

infrastructure all over the world. Microsoft obeys international data protection laws regarding transfers of customer data across borders.

Note Microsoft and its subsidiaries in the United States abide by the EU-US Privacy Shield with regard to the collection, use, and retention of data transferred from the European Union to the United States. See the press release MICROSOFT AND THE UE-US PRIVACY SHIELD.

Following the invalidation of the Safe Harbor Act in October 2015, the Article 29 Working Party[36] (so-called WP29), named in reference to Article 29 of Directive 95/46 / EC – and representing the 28 authorities for the protection of personal data in the European Union – and the United States Department of Trade and Industry defined a new regulatory framework, called the EU-US Privacy Shield, that governs data flows between Europe and the United States on a solid legal basis.

This new framework, adopted by the European Commission on July 12, 2016, provides for greater transparency, enhanced control, and more possibilities for recourse against predecessors. This framework guarantees Europeans the right to judicial settlement, reinforces the role of the data protection authorities, provides for an independent instance of control, and clarifies the data collection practices used by American security agencies. It also includes new rules for the retention and subsequent transfer of data. Another important point is that the main provisions of this framework extend to other transfer mechanisms, such as standard contractual clauses in the European Union.

- Review the reports on the verifications at least once a year with regard to several global data protection standards, including several ISO/IEC standards, the STAR register of the CSA (Cloud Security Alliance), HIPAA, and HITECH. These reports can be found at https://servicetrust.microsoft.com/Documents/ComplianceReports.

Litware 369 must also enter into contracts with its entire network of partner companies, which are all considered to be data processors. Here again, the goal consists of making sure that all these partners offer the necessary guarantees with regard to the requirements of the GDPR.

All these items are recorded by the data processor in the records of data processor risks.

Set up a data catalog

For Litware 369, mapping the processing activities is also an opportunity to decompartmentalize its application silos and data repositories by establishing the basis of a genuine data catalog in the company. To do this, Litware 369 has decided to use the Azure Data Catalog[37] cloud service.

Azure Data Catalog is a cloud service that enables organizations like Litware 369 to make better use of their existing investments, such as the on-premises SQL Server environment. This service includes a cloud sourcing model for metadata and annotations for the indexing of data sources. It centralizes all the information that enables the users in an organization to share their knowledge and to create a data community and culture. In this way, any users (analysts, data scientists, or developers) can detect, understand, and use data sources.

Note For more information, read the article WHAT IS AZURE DATA CATALOG?[38].

[36] Article 29 Working Party: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm

[37] Azure Data Catalog: https://azure.microsoft.com/en-us/services/data-catalog/

[38] WHAT IS AZURE DATA CATALOG: https://docs.microsoft.com/en-us/azure/data-catalog/data-catalog-what-is-data-catalog

Examples of solutions

Updating the map of the representative processing scenario shows how Cloud App Security and advanced eDiscovery in Office 365 contribute to improving our knowledge of the processing and the relevance of the map.

The discovery of personal data in general, and not only within the restricted framework of our illustration, can also take advantage of other products and cloud services from Microsoft.

> **Note** The white paper THE START OF YOUR ROAD TO COMPLIANCE WITH THE GENERAL REGULATION ON DATA PROTECTION[39] contains examples of actions that you can take with Microsoft right away to get started on your path to compliance with the GDPR. The paper contains an illustration of the measures to be taken in the main step of personal data discovery, and of how Microsoft products and cloud services can contribute to the execution (or the effective expression) of these actions.

This closes exploration of the first main step, Discover. The second main step, Manage, is described in the following section.

[39] THE START OF YOUR ROAD TO COMPLIANCE WITH THE GENERAL REGULATION ON DATA PROTECTION: https://aka.ms/gdprwhitepaper

Manage - Control the way personal data is accessed and used

The step of managing personal data corresponds to a series of activities in the **DO** phase (of the PDCA model) of the GDPR program suggested in the white paper GDPR – GET ORGANIZE AND IMPLEMENT THE RIGHT PROCESSES FOR COMPLIANCE WITH THE GDPR.

At this stage, we assume that several actions in the **PLAN** and **DO** phases have already been completed to make sure that:

- The up-to-date map of the representative processing scenario has been completed with personal data flows and the descriptions of the controls put in place.
- The processing records have been created and included in the record of processing activities.
- A preliminary study has been made and the decision has been taken **not to** proceed with a data protection impact analysis (DPIA) because none of the criteria requiring a DPIA have been associated with the processing (large-scale processing, particularly sensitive data categories, profiling, and so on).

Moreover, the preliminary study defined a series of actions and measures that should be taken to begin the process of embarking on the path to GDPR compliance.

In particular, it is necessary to draw up a complete personal data governance plan, with a definition of the policies, roles, and responsibilities for the management and use of personal data according to its type and sensitivity. The governance of personal data covers the way the data is accessed and used.

This governance supposes that the data is known and, consequently, that its classification and labeling is known. In this case, we assume that Litware 369 already has a suitable classification taxonomy that the company can take advantage of.

Classify and label personal data

After the data processing has been duly mapped and personal data has been identified, the goal is to organize and label the data so that personal data can be identified in the data repositories and the necessary security measures can be taken, according to the type and sensitivity of the data.

This section considers the processing scenario of semi-structured or unstructured data. For example:

- The Windows Server file server containing the .CSV files.
- The email messages generated by the Outlook add-in.

Label personal data with Azure Information Protection in a hybrid world

Azure Information Protection[40] helps to guarantee that Litware 369 personal data can be identified, so it can be protected according to its type and sensitivity – a key requirement of the GDPR – and regardless of where it is stored and how it is shared.

[40] Azure Information Protection: https://www.microsoft.com/en-us/cloud-platform/azure-information-protection

Azure Information Protection classifies and labels data according to the classification established in the organization and, where appropriate, protects new and existing data according to the chosen policy (see the section ENFORCE THE DATA PROTECTION POLICIES).

Note For more information, view the webinars AN INTRODUCTION TO MICROSOFT AZURE INFORMATION PROTECTION[41] and LEARN HOW CLASSIFICATION, LABELING, AND PROTECTION DELIVERS PERSISTENT DATA PROTECTION[42].

The previous operations can be performed when creating this data with Office apps or, for existing data, directly on the Windows Server file server for the CSV files that correspond to new orders.

In the latter case, a set of PowerShell[43] cmdlets can be used to perform these operations for an entire folder from the command prompt to apply the same label to the orders.

A scanner type capability is available in public preview to scan the various resources in the organization's internal network (and the on-premises SharePoint Server sites) to apply the necessary classification labels to personal data in question.

Use the Data Classification Toolkit for the file server

The Data Classification Toolkit[44] can be used in different ways. This toolkit is designed to enable companies like Litware 369 to identify, classify, and protect personal data on Windows Server file servers. Examples of classification and rules that apply to searches for regular expressions can help organizations develop and deploy their policies for the protection of such information on their Windows Server file servers.

Note For more information, refer to the articles DATA CLASSIFICATION TOOLKIT[45] and IMPORTANT INFORMATION ABOUT THE DATA CLASSIFICATION TOOLKIT[46].

Enforce personal data policies

Regardless of the approach that is adopted, the labels are then used to apply the management and/or protection policies.

To continue with the file server in our scenario, Dynamic Access Control (DAC)[47], which is based on the domain, is used to apply access control authorizations and restrictions according to rules that can include the previous labels. Moreover, Windows File Explorer or PowerShell can be used to restrict the processing of personal data by barring access to files containing the target personal data.

---

[41] AN INTRODUCTION TO MICROSOFT AZURE INFORMATION PROTECTION: https://youtu.be/N9lp0m6d3G0

[42] LEARN HOW CLASSIFICATION, LABELING, AND PROTECTION DELIVERS PERSISTENT DATA PROTECTION: https://youtu.be/ccBus_Yx69g

[43] PowerShell: https://msdn.microsoft.com/en-us/powershell/mt173057.aspx

[44] Data Classification Toolkit for Windows Server 2012 R2: http://go.microsoft.com/fwlink/p/?LinkId=226045

[45] DATA CLASSIFICATION TOOLKIT: https://msdn.microsoft.com/en-us/library/hh204743.aspx

[46] IMPORTANT INFORMATION ABOUT THE DATA CLASSIFICATION TOOLKIT: https://msdn.microsoft.com/en-us/library/hh367453.aspx

[47] DYNAMIC ACCESS CONTROL OVERVIEW: https://docs.microsoft.com/en-us/windows/access-protection/access-control/dynamic-access-control

Integrate with other solutions

The goal is to integrate with CASB (Cloud Access Security Broker)-type data loss prevention (DLP) functionality or solutions.

In our scenario, the Data Loss Prevention policies[48] in Office 365 enable companies such as Litware 369 to use the previous labels to configure the measures to protect sensitive information and to prevent their accidental disclosure.

> **Note** The data loss prevention policies in Office 365 can also identify more than 80 common types of sensitive data,[49] including personal identification data.

Similarly, Cloud App Security, which was referenced earlier with regard to the detection of "Shadow IT" applications, can also contribute to the control of personal data by modeling the Litware 369 cloud environment using custom or ready-to-use policies for data sharing and data loss prevention. These policies can obviously be based on the use of the previous labels for the data in question.

In this way, the classification defined by the company using Azure Information Protection can be used by Cloud App Security by integrating these two services. In this case, Cloud App Security uses the classification labels to detect sensitive files in the cloud applications it controls that contain, for example, personal data that falls within the scope of the GDPR. Cloud App Security itself offers a centralized view of the sensitive labeled files, and of their location. Filters can be used to search for files that do not respect the company's policies. By way of example, a filter can be created to produce a list of the files with a "Personal data" label that are stored on OneDrive, Box, or Dropbox, in contravention of the security policies[50].

Furthermore, thanks to the integration with the Azure Information Protection service, Azure Rights Management can allow files detected as sensitive – in this case according to the GDPR and not to the organization – to be protected on the basis of their label, either manually from the Cloud App Security portal, or automatically using rules[51].

---

[48] OVERVIEW OF DATA LOSS PREVENTION POLICIES: https://support.office.com/en-us/article/Overview-of-data-loss-prevention-policies-1966b2a7-d1e2-4d92-ab61-42efbb137f5e

[49] SENSITIVE INFORMATION TYPES IN EXCHANGE 2016: https://technet.microsoft.com/en-us/library/jj150541(v=exchg.160).aspx

[50] INTEGRATION OF AZURE INFORMATION PROTECTION: https://docs.microsoft.com/en-us/cloud-app-security/azip-integration

[51] Undergoing integration at the time of writing. Available for SharePoint Online and OneDrive for Business.

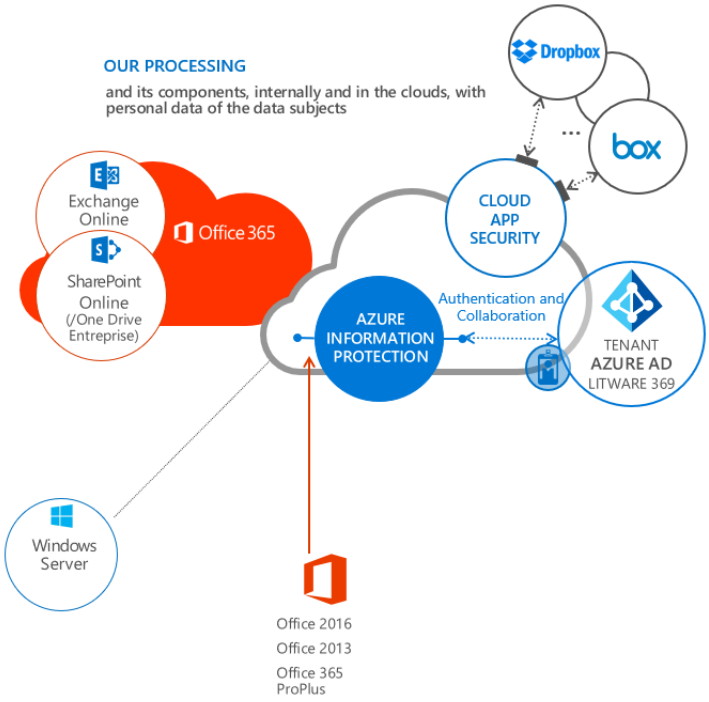


Figure 8. Label personal data and integrate with multiple solutions

The section ENFORCE THE DATA PROTECTION POLICIES later in this white paper specifically examines the definition of data protection policies and their application in terms of personal data controls.

Note For more information, refer to the white paper PROTECT AND CONTROL YOUR KEY INFORMATION ASSETS THROUGH INFORMATION CLASSIFICATION[52].

However, before policy examination, the following sections continue exploring the data management dimension.

Automatic protection against the risk of accidental deletion

This section considers the processing scenario for the library of Word forms in SharePoint. This library contains the order files with the technical characteristics of the installation.

In Office 365, protection against the risk of accidental deletion can be based entirely on the use of advanced data governance mechanisms. Advanced Governance in Office 365 takes advantage of computer-aided information to help Litware 369 find, classify, and define policies and take measures to manage the lifecycle of the company's essential data.

Note For more information, refer to the paper ADVANCED DATA GOVERNANCE IN OFFICE 365[53] and view the webinar OFFICE 365 ADVANCED DATA GOVERNANCE OVERVIEW[54].

[52] PROTECT AND CONTROL YOUR KEY INFORMATION ASSETS THROUGH INFORMATION CLASSIFICATION - CLASSIFY, LABEL, PROTECT, AND AUDIT (CLPA) YOUR KEY INFORMATION ASSETS: https://aka.ms/classify

[53] ADVANCED DATA GOVERNANCE IN OFFICE 365: https://blogs.office.com/2016/09/26/office-365-news-in-september-at-ignite-intelligence-security-collaboration-and-more/

[54] OFFICE 365 ADVANCED EDISCOVERY: https://youtu.be/dL5DF7LN07s

In addition to the automatic classification of data, the goal consists of being able to benefit from the recommendations on smart policies, retention, and disposal based on machine learning; taking actions to protect personal data; cleaning up anything that is redundant or obsolete; plus:

- Conducting analyses to detect what is important, delete what is not important, and share in accordance with the policies
- Recording actions in a log journal

In this way, the data retention functionality in Office 365 can help to manage the lifecycle of email messages and documents while keeping the content that Litware 369 needs and deleting the content when it is no longer necessary. One of the principles in the GDPR states that you are responsible for limiting the storage of personal data to the time required for the intended purpose.

Note For more information, refer to the article RETENTION IN THE OFFICE 365 COMPLIANCE AND SECURITY CENTER[55].

Finally, it is worth mentioning that disks, backups, and so on can be imported to implement and benefit from (more) global governance.

Manage roles and responsibilities

The time has come to determine how to define policies, roles, and responsibilities for the management and use of personal data as follows:

- Whether it is at rest, in use, or in transit
- And, in the lifecycle, whether its classification is for storage vs. recovery vs. retention vs. archiving vs. disposal

The protection of personal data starts by protecting identities and controlling access from the moment the data is brought into the system, starting at "the front door".

Litware 369 manages identity and access for its employees with Azure Active Directory[56] (Azure AD).

Azure AD helps to guarantee that only authorized users can access the computer environments, data, and applications, and includes tools such as multi-factor authentication[57] for highly secure session logins.

Note For more information, refer to the article WHAT IS AZURE ACTIVE DIRECTORY?[58].

In our scenario, Azure AD is used by the Azure cloud, Dynamics 365, and Office 365 services. As well as controlling access to the management portal, Azure AD also enables Litware 369 to segregate roles in the creation and configuration of the resources of the various workloads with Role-Based Access Control (RBAC)[59]. We will explain how the management of privileged identities is used in this context later on.

---

[55] RETENTION IN THE OFFICE 365 COMPLIANCE AND SECURITY CENTER: https://support.office.com/en-us/article/Overview-of-retention-policies-5e377752-700d-4870-9b6d-12bfc12d2423

[56] Azure Active Directory: https://azure.microsoft.com/en-us/services/active-directory/

[57] Azure Multi-factor Authentication: https://azure.microsoft.com/en-us/services/multi-factor-authentication/

[58] WHAT IS AZURE ACTIVE DIRECTORY?: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-whatis

[5959] USING ROLE-BASED ACCESS CONTROL TO MANAGE ACCESS TO THE RESOURCES OF AN AZURE SUBSCRIPTION: https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-control-configure

An existing internal deployment of Active Directory (AD) constitutes the on-premises security backbone for the on-premises workloads, servers, and workstations.

Note For its deployment of AD, Litware 369 took a number of internal technical measures at a very early stage to secure its privileged accesses. Cyberattack techniques such as Pass-the-Hash and Pass-the-Ticket[60] target accounts and other parts of the privileged access system to quickly gain access to the targeted information by stealing identification data.

To mitigate the risks, all the employees at Litware 369 with administrative privileges have a dedicated account for administrative tasks. They also use Privileged Access Workstations (PAW) which, as the article entitled PRIVILEGED ACCESS WORKSTATIONS[61] explains, provide a dedicated environment where sensitive tasks are protected against attacks from the internet and other sources of threats.

Furthermore, all the workstations and the Windows servers at Litware 369 have random and unique passwords configured by LAPS[62] (Local Administrator Password Solution) and recorded in the internal AD. These passwords are protected by access control lists (ACLs), guaranteeing that only legitimate users can read or reset them.

All these measures provide a first level of separation and protection of the administration. For more information, refer to the article SECURING PRIVILEGED ACCESS[63].

Azure AD Connect[64] can virtually build a single directory with controlled synchronization of the information between Azure AD and AD, so that Litware 369 employees have a common identity for the Dynamics 365 and Office 365 applications as well as other (SaaS) applications integrated in Azure AD. This common identity means that Litware 369 users have transparent access to their internal resources and their cloud resources, from inside and outside the company. That being said, all access is nonetheless carefully authenticated and controlled.

Note Azure AD Connect Health[65] can be used to monitor and analyze the on-premises identity infrastructure and the synchronization services at Litware 369. In this way, it maintains a reliable connection with Azure AD by providing monitoring capabilities of the key on-premises identity components, such as the Azure AD Connect servers (synchronization engine), the AD domain controllers, and so on. Azure AD Connect Health also produces usage data and other important information required to take informed decisions on the infrastructure.

Securely manage B2B access to data, applications, and other resources

This section considers the processing scenario of the Litware 369 Partners portal and the database of partner accounts on the internal SQL data server required for authenticated access to the portal.

The employees of a company clearly need to collaborate with partners to easily share (personal) data with the right persons in the partner companies on a daily basis. This processing scenario is no exception.

---

[60] PASS-THE-HASH (PTH): https://technet.microsoft.com/en-us/security/dn785092

[61] PRIVILEGED ACCESS WORKSTATIONS: https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/privileged-access-workstations

[62] Local Administrator Password Solution (LAPS): https://www.microsoft.com/en-us/download/details.aspx?id=46899

[63] SECURING PRIVILEGED ACCESS: https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access

[64] INTEGRATING LOCAL DIRECTORIES IN AZURE ACTIVE DIRECTORY: https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect

[65] MONITOR YOUR LOCAL IDENTITY INFRASTRUCTURE AND YOUR SYNCHRONIZATION SERVICES IN THE CLOUD: https://docs.microsoft.com/en-us/azure/active-directory/connect-health/active-directory-aadconnect-health

At the same time, partner companies are looking for seamless exchanges, without the need to create new accounts, configure federations, install servers, or change their configurations. For Litware 369, this involved defining one generic identity per partner.

Although this approach is simple enough and offers a quick response to the need to use this processing, it is not satisfactory for the Litware 369 IS security manager, who demands a much more fine-grained capacity to control, monitor, and audit partner access.

Securing identities beyond those of Litware 369 employees in response to the need to extend the network of partners to drive the growth of the company is a factor that is essential to the protection of the company's (personal) data.

The Azure AD B2B Collaboration capacity enables any organization that uses Azure AD to work in complete security with users from any other organization, small or large, with or without Azure AD, and even with or without an IS department.

With Azure AD B2B Collaboration, Litware 369 can benefit from all the identity and access management (IAM) functions for its partners. Organizations like Litware 369 that use Azure AD can provide access to documents, resources, and applications for their partners, while keeping complete control over the company's data. In other words, and regardless of their size and technical environments, the partner companies manage their own credentials while Litware 369 manages the access control policy for these "guest" accounts. In this case, Litware 369 can display the terms of use of such an application exposed in this way, and ask for acceptance, before granting access under the agreed terms.

Note For more information, refer to the article WHAT IS AZURE AD B2B COLLABORATION?[66] and view the webinar AZURE ACTIVE DIRECTORY B2B COLLABORATION: SIMPLE, SECURE EXTERNAL SHARING OF YOUR APPS AND SERVICES[67].

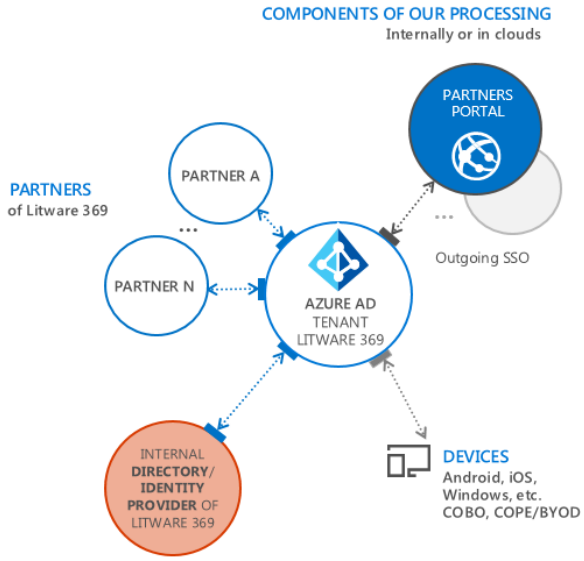


Figure 9. With Azure AD B2B Collaboration, you can benefit from all the IAM functions for your partners

[66] WHAT IS AZURE AD B2B COLLABORATION?: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-what-is-azure-ad-b2b

[67] AZURE ACTIVE DIRECTORY B2B COLLABORATION: SIMPLE, SECURE EXTERNAL SHARING OF YOUR APPS AND SERVICES: https://youtu.be/AhwrweCBdsc

Securely manage B2C access to data, applications, and other resources

This section considers the processing scenario of the Litware 369 Customers portal and the database of customer accounts on the internal SQL data server required for authenticated access to the portal.

Azure Active Directory B2C[68] (Azure AD B2C) is a cloud identity management service that provides web and mobile applications to customers by offering them a fully customizable experience.

> **Note** For more information, refer to the article AZURE AD B2C: CONCENTRATE ON YOUR APPLICATION, AND LET US TAKE CARE OF REGISTRATION AND CONNECTIONS[69] and view the webinar AZURE AD B2C: HOW TO ENABLE CONSUMER LOGINS AND ACCESS MANAGEMENT FOR YOUR B2C APPS[70].

Based on Azure AD, this solution offers optimal scalability, reliability, and availability to the applications for Litware 369 customers.

Azure AD B2C enables Litware 369 to benefit from all the customer identity and access management (CIAM) functions, in particular for the Customer portal, with a view to managing an audience of expected customers.

This solution results in the capacity to:

- Manage identities at scale, with no more need to manage any accounts in the internal SQL Server database.
- Offer better user journeys and related experiences (sign-up, sign-in, profile edit, password reset, and so on) that are both more attractive and more secure.
- Benefit from built-in predefined journeys or custom journeys and receive consent if the context requires so.
- Allow for the reuse of social identities to bootstrap the authentication process: Amazon, Google, LinkedIn, Microsoft, Twitter, and so on.
- Have a personalized user profile, because most consumer applications now need to store certain types of information. This personalization entails defining custom attributes, which can then be processed in the same way as any other attributes of a user account.

[68] Azure Active Directory B2C: https://azure.microsoft.com/en-us/services/active-directory-b2c/

[69] AZURE AD B2C: CONCENTRATE ON YOUR APPLICATION, AND LET US TAKE CARE OF REGISTRATION AND CONNECTIONS: https://docs.microsoft.com/en-us/azure/active-directory-b2c/active-directory-b2c-overview

[70] AZURE AD B2C: HOW TO ENABLE CONSUMER LOGINS AND ACCESS MANAGEMENT FOR YOUR B2C APPS: https://azure.microsoft.com/en-us/resources/videos/azure-ad-b2c-how-to-enable-consumer-logins-and-access-management-for-your-b2c-apps/?v=17.23h

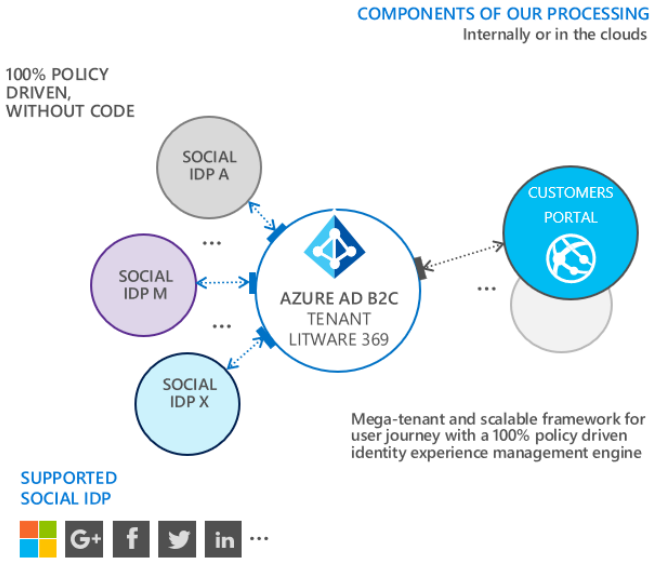


Figure 10. With Azure AD B2C, you can benefit from all the IAM functions for your customers

Allow data subjects to exercise new rights

Identity constitutes the new security plane, in particular in terms of security measures. The efforts made by Litware 369 to rationalize the (customer) identity and access management ((C)IAM) functions for B2E, B2B, and B2C have helped the data subjects (Litware 369 employees (B2E), Litware 369 partners (B2B) and Litware 369 contacts and customers (B2C)) to exercise new rights. The GDPR requires extended rights related to access, rectification, or deletion of erroneous data, erasure of data (also as known as the right to be forgotten), and so on.

Litware 369 can fully benefit from the capacities offered by Azure AD to achieve this capability. The following sections consider this capability, according to the different types of identities: B2E vs. B2B vs. B2C.

Allow Litware 369 employees to exercise their new rights

To manage the identities of its employees, Litware 369 benefits from its previous investment in Microsoft Identity Management (MIM)[71] and the (inter)connection between these identities and the HR solution, the AD technical directory, and other solutions / application silos in the on-premises environment.

MIM simplifies the management of the lifecycle of these identities with automated workflows and company rules, creating a context in which integration with multi-vendor platforms in the on-premises environment or the cloud is easy. Detailed reports illustrate and can be used to keep track of changes to and the history of these identities, and the associated notifications, email messages, and approvals.

An ad hoc internal user portal provides employees with access to their identity information, and enables them to correct or possibly delete incorrect data.

In addition to using LDAP requests sent to AD, the implementation of the portal for the exercise of these rights also uses the Microsoft Graph[72] API that targets the same users in Azure and Office 365 and returns

[71] Microsoft Identity Manager 2016: https://www.microsoft.com/en-us/cloud-platform/microsoft-identity-manager

[72] Microsoft Graph: https://developer.microsoft.com/en-us/graph

the detailed properties of a user, plus enriched contextual information such as any registered devices, the manager's name, whether they are in the office or not, and so on. This same API can be used to update a user's attributes, to deactivate them, or to delete them. (Only HR can use the deactivate and delete functions.)

> **Note** The Azure AD Graph[73] API offers an alternative means of accessing only the Azure AD resources. However, we should point out that development efforts are now focused on Microsoft Graph and that no enhancements are planned for the Azure Graph API. In practice, there are very few scenarios to which the Azure AD Graph API is only suited. For more information, refer to the paper MICROSOFT GRAPH OR THE AZURE AD GRAPH[74].

This portal also integrates the MIM self-service functions, so that users can solve their own identity-related problems, in particular membership of groups, password resets, and so on.

An easy-to-use interface ultimately boosts productivity and satisfaction while also fulfilling the requirements of the GDPR.

Allow Litware 369 partners to exercise their new rights

As mentioned in the section SECURELY MANAGE B2B ACCESS TO DATA, APPLICATIONS, AND OTHER RESOURCES, Litware 369 uses Azure AD B2B Collaboration for authenticated access to the Partners portal. All the duly authorized employees in Litware 369 partner companies have their own Azure AD "guest" account defined.

A section dedicated to this portal provides these external users with rights extending beyond their identity information to include the correction or deletion of incorrect data about them. They can also ask for this data to be erased. Doing so removes their account and, consequently, their access to the Litware 369 Partners portal and to all other resources integrated in Azure AD that Litware 369 makes available to these external users using the existing access control.

The implementation of this part of the Partners portal is based on the Azure AD Graph API (see previous section). Litware 369 also uses the code of the example of a self-service registration portal[75], made available in open source by Microsoft on the GitHub community forge.

Allow Litware 369 contacts and customers to exercise their new rights

The planned processing operation of the storage of collected personal data has two main phases:

- Before the activation of the service
- After the service has been activated

The new rights will be exercised as described in the following paragraphs.

---

[73] AZURE ACTIVE DIRECTORY GRAPH API: https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-graph-api

[74] MICROSOFT GRAPH OR THE AZURE AD GRAPH: https://dev.office.com/blogs/microsoft-graph-or-azure-ad-graph

[75] SELF-SERVICE PORTAL FOR AZURE AD B2B COLLABORATION SIGN-UP: https://aka.ms/b2bselfservice

Before the activation of the service

When the order placed by a contact is confirmed, the confirmation email sent to the contact contains a link that enables the contact to withdraw and cancel the order within 14 days.

This personalized link points to a webpage that describes how the order can be canceled and indicates that no personal data will be kept after the transaction.

After a confirmation request, all the records about this order are deleted from the SQL Server database. Only the order number, the initial order date, and the date and time of cancellation are retained in order to keep a trace of the operations. The order is now displayed as canceled on the Partners portal, without any of the information that appeared previously. The transaction is closed by sending an email message that confirms the deletion of the order and the corresponding personal data.

> **Note** In view of the main steps of our representative processing scenario and the corresponding processing operations, the effective cancellation requires additional coherency checks and, where appropriate, additional operations, depending on the current status of the said processing operation. The goal here is simply to illustrate the principle.

After the service has been activated

As already stated, when the partner company proceeds with the installation in readiness for the complete activation of the service and the purchased options, the Litware 369 Subscriptions entity creates a new customer account:

- A new customer account and a new contract are created in Dynamics 365 in order to invoice the subscription to the connected alarm offer, to manage the contract, and so on.
- A new identity is created in the Azure AD B2C of Litware 369 via the Azure AD Graph API for access to the Customer portal (see previous section SECURELY MANAGE B2C ACCESS TO DATA, APPLICATIONS, AND OTHER RESOURCES).

  The identifier is the email address sent previously that was used in the exchanges so far. A temporary password is created. The telephone number is stored in the attributes of the B2C account. It will be used for multi-factor authentication in the various user journeys and experiences offered on the portal: finalization of registration when the customer logs on for the first time, with explicit consent, sign-in, profile edit, password reset, and so on.

A confirmation email is sent to the customer that contains all the connection information (identifier and password) required to manage the subscription and any related requests from the Customer portal.

Customers must identify themselves with their email address to access the Customer portal and their customer accounts. When they sign in for the first time, users can use a social identity for (the bootstrap of) the authentication process instead of this email address.

After they have signed in, customers can access their customer account for the alarm service along with their profile. Information about the contract and their personal information can be accessed and edited, if necessary. The Microsoft Dynamics 365 Web Services[76] and the Azure AD Graph API are used to provide this functionality.

These same web services and APIs are used to grant the right to erase data (also known as the right to be forgotten), plus the possibility to delete all the information that does not have to be imperatively retained.

---

[76] USING THE MICROSOFT DYNAMICS 365 Web Services: https://msdn.microsoft.com/en-us/library/mt608128.aspx

This concludes the examples used to illustrate the capacities for the governance of personal data within the scope of our scenario.

Examples of solutions

The classification and labeling of personal data and the management of identities and roles in our representative processing scenario show how Azure Information Protection, Azure AD, Azure AD B2B Collaboration, and Azure AD B2C contribute to reinforce the governance of personal data.

This governance of personal data in general, and not only within the restricted framework of our scenario and the resulting plan, can also take advantage of other products and cloud services from Microsoft, in addition to the examples given here.

> **Note** The white paper THE START OF YOUR ROAD TO COMPLIANCE WITH THE GENERAL REGULATION ON DATA PROTECTION[77] contains examples of actions that you can take with Microsoft right away to get started on your way to GRDP compliance. This white paper contains an illustration of the measures to be taken in this context for the management of personal data, and of how Microsoft products and cloud services can contribute to the execution (or the effective expression) of these measures.

[77] THE START OF YOUR ROAD TO COMPLIANCE WITH THE GENERAL REGULATION ON DATA PROTECTION: https://aka.ms/gdprwhitepaper

Protect - Prevent, detect, and respond to any vulnerabilities and personal data breaches

Like in the previous management step (see section MANAGE - CONTROL THE WAY PERSONAL DATA IS ACCESSED AND USED), this step of protecting personal data corresponds to a series of activities in the **DO** phase (of the PDCA model) of the GDPR program suggested in the white paper GDPR – GET ORGANIZED AND IMPLEMENT THE RIGHT PROCESSES FOR COMPLIANCE WITH THE GDPR. These activities and the corresponding actions consist of improving the security of personal data processing.

In view of the results of the preliminary study, and to limit the risks of information leaks or unauthorized access to personal data, the decision was taken to reinforce protection by taking advantage of the encryption capabilities of the systems on which they are stored.

The following sections illustrate how these actions take shape, using some examples of Microsoft products and cloud services.

Protect data at rest

Data at rest is protected essentially by encryption.

Encrypt data at rest

Data encryption is one of the technical measures explicitly mentioned by the GDPR. This section considers what is feasible in the representative processing scenario.

Encrypt the orders on the Windows Server file server

In the processing of new orders, an extract of the internal SQL database is done on a daily basis in the form of .CSV files stored on a Windows Server file server. Even if this server is located on Litware 369 premises, the company wants to be sure that personal data contained in the .CSV files on the hard drives of the server are encrypted when at rest.

To do this, Litware 369 decided to use BitLocker technology. The BitLocker disk encryption technology, which is natively present in Windows Server, provides a professional-quality encryption functionality to protect personal data if a disk is lost or stolen. BitLocker entirely encrypts the disks of a computer to prevent unauthorized users from accessing your data.

BitLocker covers the risk of access to the operating system disk and the data disks when a computer is lost or stolen, or when a disk is decommissioned or recycled.

> **Note** BitLocker offers maximum protection when used in conjunction with TPMs (Trusted Platform Modules) that are present in most recent configurations. For even greater security, a PIN code can be required when starting a server if it is not connected to the corporate network by activating the unlock network function.
>
> For more information, refer to the articles OVERVIEW OF THE ENCRYPTION OF BITLOCKER DEVICES[78] and BITLOCKER: HOW TO ENABLE NETWORK UNLOCK[79], and the white paper PROTECTING YOUR DATA WITH WINDOWS 10 BITLOCKER[80].

[78] Overview of the encryption of BitLocker devices: https://technet.microsoft.com/en-us/library/cc732774(v=ws.11).aspx

[79] BITLOCKER: HOW TO ENABLE NETWORK UNLOCK: https://docs.microsoft.com/en-us/windows/device-security/bitlocker/bitlocker-how-to-enable-network-unlock

[80] PROTECTING YOUR DATA WITH WINDOWS 10 BITLOCKER: https://www.microsoft.com/en-us/download/details.aspx?id=53006

Note For more information on the security of the Windows platform, refer to the presentation of Windows Server 2016 Security[81] and Windows 10 Security[82].

Encrypt orders in the internal SQL Server database

In the initial phase of the order-taking process by customers on the Litware 369 institutional website, the information associated with the order, including the customer's personal data, is stored in the internal SQL Server database. Data at rest is natively protected by the transparent data encryption (TDE) functionality of the SQL Server database.

Transparent data encryption protects data at rest by encrypting the database, the corresponding backups, and the transaction log files on the physical storage level. This mode of encryption is transparent for the institutional site and uses hardware acceleration to improve performance.

Note For more information, refer to the article TRANSPARENT DATA ENCRYPTION (TDE)[83].

Litware 369 wants to reinforce protection by using its own encryption keys for Transparent Data Encryption and by protecting these keys in the Azure Key Vault service (see section ENCRYPT THE CUSTOMER FORMS IN THE SHAREPOINT ONLINE LIBRARY later in this paper). To this end, the SQL connector for Azure Key Vault integrates the internal SQL Server database and the Azure Key Vault service.

Note The SQL Server connector is an extensible key management (EKM) provider that enables SQL Server to use Azure Key Vault as a vault for the protection and management of SQL encryption keys. This means that you can use your own keys for SQL Server encryption, and then protect them in Azure Key Vault. In addition to providing the transparent data encryption (TDE) that interests us at this point, the SQL Server connector can also configure column-level encryption (CLE) and the encryption of backups.

For more information, refer to the paper SQL SERVER CONNECTOR FOR AZURE KEY VAULT IS GENERALLY AVAILABLE[84].

Encrypt the mailboxes in Exchange Online

In the processing, after the new orders have been stored as .CSV files on the internal file server, an email is automatically sent to each partner by an Outlook add-in. Each email contains the data that relates directly to the customer (order number) and the links used to keep track of the order, cancel the order, and so on. Later in the processing, after the partner has installed the connected alarms for the customer, other email messages are sent that contain the login information specific to each customer. Therefore, it is important that the mailboxes containing these email messages are protected in the place where they are stored – that is, the Office 365 Exchange Online messaging system.

Exchange Online natively offers **encryption functionality of each user's mailbox** to protect all the content in the mailbox with a different key. This service-level encryption prevents a system administrator or an indiscreet operator of the cloud service from accessing the customer content, and therefore provides more protection than the BitLocker volume-level encryption that is applied to the disk volumes for the Exchange Online cloud service.

---

[81] IMPROVING SECURITY WITH WINDOWS SERVER 2016: https://www.microsoft.com/en-us/cloud-platform/windows-server-security

[82] PROTECTION AGAINST THE NEW THREATS TO: https://www.microsoft.com/en-us/WindowsForBusiness/Windows-security

[83] TRANSPARENT DATA ENCRYPTION (TDE): https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption-tde

[84] SQL SERVER CONNECTOR FOR AZURE KEY VAULT IS GENERALLY AVAILABLE: ttps://blogs.msdn.microsoft.com/sqlsecurity/2016/06/13/sql-server-connector-for-azure-key-vault-is-generally-available/

In line with the steps taken to encrypt the data in the internal SQL Server database, Litware 369 also wants to use its own keys to encrypt the mailboxes and, in the same way, to use the Azure Key Vault to store and protect its keys (see section ENCRYPT THE CUSTOMER FORMS IN THE SHAREPOINT ONLINE LIBRARY below).

This process consists of implementing the BYOK (bring your own key) functionality, which offers additional guarantees to Litware 369. This functionality can be used to configure Exchange Online so that this cloud service uses the keys in an Azure Key Vault to protect the content of the mailboxes.

> **Note** For more information, refer to the white paper CONTENT ENCRYPTION IN MICROSOFT OFFICE 365[85].

Encrypt the customer forms in the SharePoint Online library

At the end of the processing, each day, the completed orders are extracted and Word forms are automatically generated and stored in a Litware 369 SharePoint Online library. These Word forms contain personal data about customers (the order file with the technical characteristics of the installation). Therefore, they must be protected in the SharePoint library.

No particular action is necessary because the SharePoint Online cloud service (or the OneDrive Enterprise storage service) offers **file-level encryption of data at rest** by default.

> **Note** Each file is divided into one or more parts, depending on the size of the file, and each part is encrypted using its own unique key. The keys are then encrypted and stored in an online SharePoint content database with the map showing the distribution of the parts of the files, which is used to rebuild the files when access is required.
>
> For more information, refer to the white paper CONTENT ENCRYPTION IN MICROSOFT OFFICE 365[86].

Litware 369 benefits from the recent integration with Azure Key Vault at this point, too.

> **Note** For more information, refer to the paper NEW MICROSOFT 365 FEATURES TO ACCELERATE GDPR COMPLIANCE[87].

Store and protect the encryption keys in Azure Key Vault

Azure Key Vault[88] is an Azure vault service for keys and secrets that protects encryption keys, secret data (such as passwords), and the certificates that protect the data.

> **Note** For more information, refer to the article WHAT IS AZURE KEY VAULT?[89], view the webinar INTRODUCTION TO MICROSOFT AZURE KEY VAULT[90] and following the Microsoft Virtual Academy (MVA) online training AZURE KEY VAULT IN PRACTICE[91].

---

[85] CONTENT ENCRYPTION IN MICROSOFT OFFICE 365: http://aka.ms/Office365CE

[86] Ibid

[87] NEW MICROSOFT 365 FEATURES TO ACCELERATE GDPR COMPLIANCE: https://cloudblogs.microsoft.com/microsoftsecure/2017/09/25/new-microsoft-365-features-to-accelerate-gdpr-compliance/

[88] Azure Key Vault: https://azure.microsoft.com/en-us/services/key-vault/

[89] WHAT IS AZURE KEY VAULT?: https://docs.microsoft.com/en-us/azure/key-vault/key-vault-whatis

[90] INTRODUCTION TO MICROSOFT AZURE KEY VAULT: https://youtu.be/5p2dQdTsUvE

[91] AZURE KEY VAULT in practice: https://mva.microsoft.com/en-us/training-courses/azure-key-vault-en-pratique-fr--16572?l=svn7dFdgC_1205192797

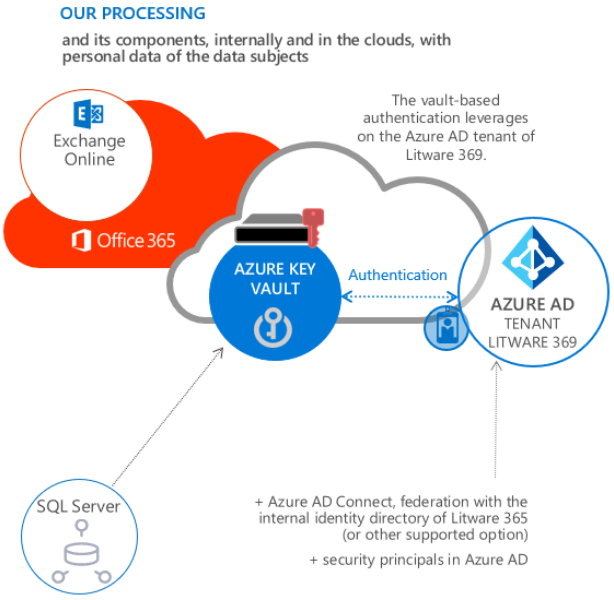


Figure 11. Manage encryption keys with Azure Key Vault

With the integration between Azure Key Vault and an increasing number of Microsoft products and cloud services, such as SQL Server, Exchange Online, and SharePoint Online in our example, you can benefit from a distinct and centralized key management system and the option to use hardware security modules (HSM) in the cloud for your key vault.

> **Note** The use of hardware security modules allows the implementation of the BYOK (bring your own key) functionality to import your own keys from your internal environment into a key vault instead of generating them in the vault.
>
> For more information, refer to the white paper BRING YOUR OWN KEY (BYOK) WITH AZURE KEY VAULT FOR OFFICE 365 AND AZURE[92].

Azure Key Vault is designed to control keys and, consequently, data in particular to guarantee that Microsoft does not have access to the keys and cannot extract them.

Moreover, Litware 369 can monitor and audit the use of its stored keys using the Azure logs and import the logs into Azure HDInsight or its security information and event management (SIEM) system to conduct additional analyses and detect threats.

This approach enables Litware 369 to ensure that the roles of key management and data management are kept separate.

Litware 369 can simply withdraw the use of its encryption keys in the access policies of the key vaults to make inaccessible all the data encrypted with the corresponding keys. This capability will be particularly useful if Litware 369 stops using certain services in the future.

[92] BRING YOUR OWN KEY (BYOK) WITH AZURE KEY VAULT FOR OFFICE 365 AND AZURE: http://download.microsoft.com/download/F/6/3/F63C9623-053F-44DD-BFA8-C11FA9EA4B61/Bring-Your-Own-Key-with-Azure-Key-Vault-for-Office-365-and-Azure.docx

Protect data in mobile devices and mobile applications

This section considers the processing scenario of orders, email messages, and other personal data that pertain to email messages.

As described earlier in the processing scenario, orders for connected alarms are registered by the customers themselves on the institutional website (see section TAKE ORDERS). Orders can also be registered directly by a Litware 369 salesperson when meeting a prospect or at a trade show.

The sales reps in the Litware 369 sales force use mobile terminals, consisting mainly of Windows 10 tablets, plus a few iPads. A mobile application has been developed for both platforms using Xamarin technology, which enables the salespeople to take orders in an attractive interface that is well adapted to these terminals, with additional functions that allow them to work offline or to manage customer dossiers.

Consequently, the sales force's mobile devices contain personal customer data and, in the event of loss or theft, can lead to leaks of personal data without the data breach even being detected. Therefore, protection is required against this serious risk by imposing security policies, such as the fact that the device is a company asset, that its disk must be encrypted, that six-character PIN codes are compulsory, and so on.

It should be noted that these criteria can be used to impose conditional access to the mobile application and the associated cloud services.

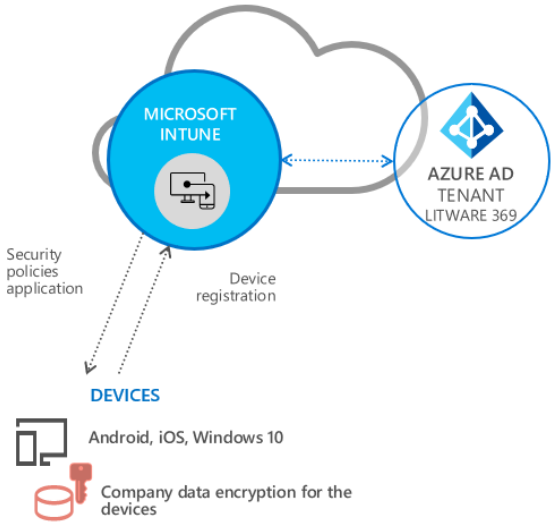


Figure 12. Secure data on mobile devices with Microsoft Intune

Litware 369 decided to use Microsoft Intune[93] to manage its mobile devices to achieve this level of security.

Microsoft Intune protects data that may be stored on personal computers and mobile devices. You can control access, encrypt the devices, selectively scan the data, and control the applications that store and share personal data. Microsoft Intune helps to inform users of their management options by publishing a personalized declaration of non-disclosure and terms of use. It can also rename and delete devices.

[93] Microsoft Intune: https://www.microsoft.com/en-us/cloud-platform/microsoft-intune

Note For more information, refer to the online documentation MICROSOFT INTUNE DOCUMENTATION[94] and the short videos COMMUNICATION FROM THE MICROSOFT INTUNE TEAM – WELCOME TO THE NEW INTUNE ON AZURE EXPERIENCE[95] and UPDATES TO MICROSOFT INTUNE ON MICROSOFT AZURE[96].

In practice, all the sales force's mobile devices must be registered in Microsoft Intune in advance to subsequently install the mobile order and customer management application. Registration starts the security policies application that imposes the previously mentioned security requirements, such as the encryption of the device and the use of a PIN code.

Note Microsoft Intune proposes a self-service enterprise portal for users where they can register their own devices and install enterprise applications using the most common mobile platforms. It protects company data by limiting access to email messages in Exchange Online, to Outlook email messages, and to documents in SharePoint Online or OneDrive Enterprise when a user attempts to access the resources from a device that is not registered or compliant, according to the policies defined by the administrator.

In addition to protecting the device itself in the event of loss or theft, Microsoft Intune also enables the salespeople to inform the Litware 369 administrator, who can then immediately and completely erase the data on the device to prevent any leaks. It should be noted that Microsoft Intune now uses Azure, is accessible from the Azure portal, and can be integrated with conditional access control.

Finally, for the sales force's Windows 10 devices that are registered in Microsoft Intune, as well as the disk encryption using the BitLocker technology mentioned earlier, additional protection can be activated using the Windows Information Protection functionality.

Windows Information Protection takes over at the point where BitLocker stops. BitLocker protects the entire disk of a device, and Windows Information Protection separates personal data from corporate data with additional file-level encryption of the latter, plus a mechanism to prevent information leaks. Corporate data cannot be copied into applications that are not deemed to be trusted, and users cannot transfer corporate files to insecure storage devices, such as a Dropbox share or a personal Box.

In this respect it should be noted that, in our scenario, the .CSV order files that are protected as company files cannot be copied to external destinations if the Windows Information Protection functionality is implemented.

[94] MICROSOFT INTUNE DOCUMENTATION: https://docs.microsoft.com/en-us/intune/

[95] COMMUNICATION FROM THE MICROSOFT INTUNE TEAM – WELCOME TO THE NEW INTUNE ON AZURE EXPERIENCE: http://intunedin.net/2017/04/communication-from-the-microsoft-intune-team-welcome-to-the-new-intune-on-azure-experience/

[96] UPDATES TO MICROSOFT INTUNE ON MICROSOFT AZURE: http://intunedin.net/2017/04/updates-to-microsoft-intune-on-microsoft-azure-new-microsoft-mechanics-video/

Note For more information, refer to the article PROTECT YOUR ENTERPRISE DATA USING WINDOWS INFORMATION PROTECTION (WIP)[97], the blog posts INTRODUCING WINDOWS INFORMATION PROTECTION[98] and WINDOWS INFORMATION PROTECTION EXPLAINED – WINDOWS 10 CREATORS UPDATE[99], and view the webinar KEEP WORK AND PERSONAL DATA SEPARATE AND SECURE USING WINDOWS INFORMATION PROTECTION IN WINDOWS APPS[100].

Enforce the data protection policies

This section attempts to show how consistent protection and automatic protection against the risk of accidental disclosure can be provided. In this context, the following components of our processing scenario are concerned:

- The Windows Server file server, with the .CSV order files to be processed.
- The email messages generated by the Outlook add-in and the other email messages sent from Outlook and Exchange Online.
- The SharePoint Online cloud service, with the library of Word files (order files with the technical characteristics of the installation).

Permanently protect files containing personal data with Azure Information Protection

In addition to offering the capacity to classify and label data (see section CLASSIFY AND LABEL PERSONAL DATA), Azure Information Protection[101] contributes to secure personal data according to its type and sensitivity – a key requirement of the GDPR – and regardless of its storage location and how it is shared. With the Azure Rights Management protection service, Litware 369 can protect (encrypt) new or existing data and share it in complete confidence with others inside or outside the company and with partner companies.

In practice, Azure Information Protection provides a holistic data protection platform that is sufficiently agile, complete, and flexible for today's organizations.

Note For more information, view the webinar LEARN HOW CLASSIFICATION, LABELING, AND PROTECTION DELIVERS PERSISTENT DATA PROTECTION[102].

Define the policies to prevent sensitive documents (orders) from being used by unauthorized users

Litware 369 must protect sensitive data, and in particular personal data mentioned in this white paper. Therefore, it must prevent its accidental disclosure.

---

[97] PROTECT YOUR ENTERPRISE DATA USING WINDOWS INFORMATION PROTECTION (WIP): https://docs.microsoft.com/en-us/windows/threat-protection/windows-information-protection/protect-enterprise-data-using-wip

[98] INTRODUCING WINDOWS INFORMATION PROTECTION: https://blogs.technet.microsoft.com/windowsitpro/2016/06/29/introducing-windows-information-protection/

[99] WINDOWS INFORMATION PROTECTION EXPLAINED – WINDOWS 10 CREATORS UPDATE: https://blogs.technet.microsoft.com/cbernier/2017/05/19/windows-information-protection-explained-windows-10-creators-update/

[100] KEEP WORK AND PERSONAL DATA SEPARATE AND SECURE USING WINDOWS INFORMATION PROTECTION IN WINDOWS APPS: https://www.youtube.com/watch?v=AbOgWvRxQf8

[101] Azure Information Protection: https://www.microsoft.com/en-us/cloud-platform/azure-information-protection

[102] LEARN HOW CLASSIFICATION, LABELING, AND PROTECTION DELIVERS PERSISTENT DATA PROTECTION: https://youtu.be/ccBus_Yx69g

In this context, and as mentioned earlier, Azure Information Protection can be used to define and implement policies to classify and label data, and to permanently protect it, no matter where it resides or where it goes. With the application of this protection, Azure Information Protection monitors the use of protected personal data and can even deny remote access. Azure Information Protection also includes enhanced log and reporting functionality to monitor the distribution of the data, and options to manage and control your encryption keys using Azure Key Vault.

As mentioned previously, the functionality for protection against data loss of the Office 365 Compliance and Security Center also identifies, monitors, and automatically protects the sensitive data in Office 365. This functionality is integrated with Azure Information Protection and, by default, benefits from the protection mechanisms of Azure Information Protection for the definition and implementation of protection policies for email messages and files that contain personal data.

Notes For more information, refer to the article OVERVIEW OF PROTECTION POLICIES AGAINST DATA LOSS[103], view the webinar PROTECT YOUR SENSITIVE INFORMATION WITH OFFICE 365 DATA LOSS PREVENTION[104], and follow the Microsoft Virtual Academy (MVA) online training DATA LOSS PREVENTION IN OFFICE 365[105].

The Cloud App Security policies also benefit from the same integration with the protection mechanisms of Azure Information Protection to protect files that contain personal data.

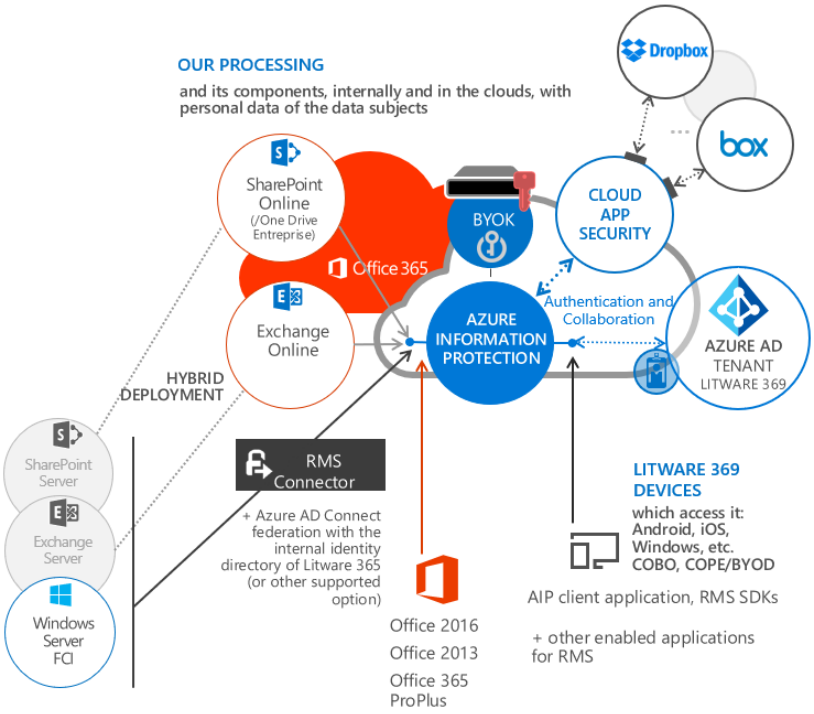


Figure 13. Permanently protect files containing personal data with the Azure Rights Management protection service of Azure Information Protection

[103] OVERVIEW OF PROTECTION POLICIES AGAINST DATA LOSS: https://support.office.com/en-us/article/Overview-of-data-loss-prevention-policies-1966b2a7-d1e2-4d92-ab61-42efbb137f5e

[104] PROTECT YOUR SENSITIVE INFORMATION WITH OFFICE 365 DATA LOSS PREVENTION: https://youtu.be/EFBXY-YYI9Y

[105] DATA LOSS PREVENTION IN OFFICE 365: https://mva.microsoft.com/en-us/training-courses/data-loss-prevention-in-office-365-8390?l=KgwSPyIz_2304984382

Impose conditional access to data

As already stated, cyberattacks always target accounts and their passwords, which are the best way of breaking into a corporate network without being detected. Therefore, they attempt to steal credentials.

Controlling and protecting identities must be the first line of defense in a typical defense-in-depth approach. Since most cybersecurity attacks can be traced back to user credentials that are lost, weak, or compromised, it is obviously necessary to reach a level of security that passwords alone cannot offer.

Protect personal data with risk-based conditional access and privileged identity management

The following part of our processing scenario concerns both the Litware 369 Partners portal and the administration / management of Azure, Office 365, and Dynamics 365 subscriptions along with the associated resources. The following paragraphs examine how to define the conditions to protect access.

Set-up conditional access with Azure AD

One of the essential aspects of a suitable security system is that it is almost invisible to legitimate users. Excessive friction is an obstacle to productivity, and legitimate users will always find ways of circumventing measures in place that reduce their productivity, thereby creating additional risks.

Even if you can impose multi-factor authentication (MFA) on every user, every time they log in – and this will be the case for Litware 369 partners – maximizing productivity ideally involves allowing legitimate users to do their job with few interruptions, while keeping out ill-intentioned individuals. Conditional access in Azure AD[106] does precisely that.

Previously, you would have had to impose restrictions such as "no access from outside the corporate network" or "no access from personal devices." Now, access can be granted or denied conditionally. For example, in our scenario, a conditional access policy for the mobile application and the corresponding mobile back-end in Azure can be based on the requirement to use a device that is previously registered for use by the Litware 369 sales force.

[106] CONDITIONAL ACCESS IN AZURE ACTIVE DIRECTORY: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access

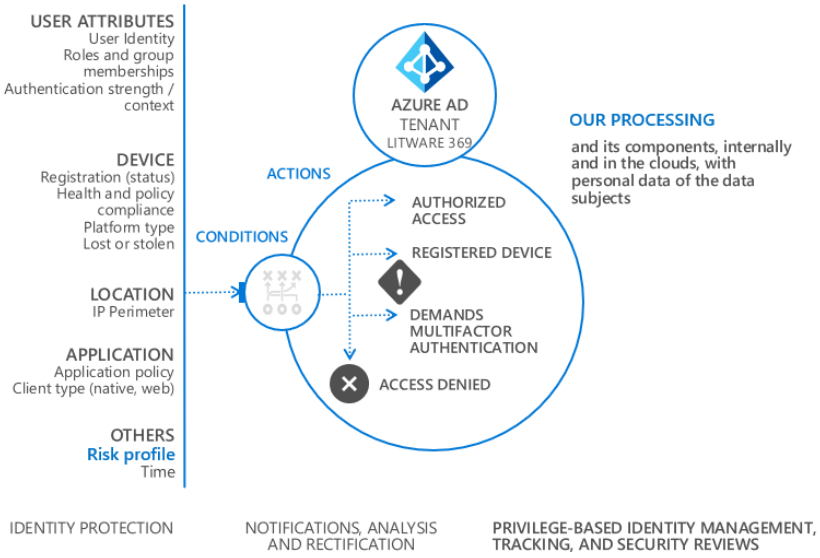


Figure 14. Control conditional access with Azure AD Premium (P1 or P2)

Conditional access in Azure AD is an Azure AD Premium (P1 or P2)[107] capacity. All users accessing applications or devices that are restricted by conditional access policies must have an Azure AD Premium license.

This conditional access continues with a conditional session in SharePoint Online. Furthermore, the recently announced proxy capacity in Cloud App Security can be integrated with the conditional access policies in Azure AD to extend this type of feature to other applications in the cloud, or wherever they reside, and to make sure that the possible actions in an application depend on the context of access after access has been granted. (Such applications must be based on the SAML-P 2.0 protocol.)

However, these conditional access policies are not limited to Litware 369 employees.

Note For more information, refer to the article UNLICENSED USAGE REPORT[108].

With Azure AD B2B Collaboration, Litware 369 can implement multi-factor authentication policies[109] (MFA) for the "guest" users (B2B) for Litware 369 partner companies. These policies can be applied to tenants, applications, or individual users. (They can also be activated for the full-time employees of Litware 369.) This type of policy is implemented for the Partners portal in our scenario.

[107] Azure AD Premium (P1 or P2): http://www.microsoft.com/identity

[108] UNLICENSED USAGE REPORT: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-unlicensed-usage-report

[109] CONDITIONAL ACCESS FOR B2B COLLABORATION USERS: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-mfa-instructions

Important note "Guest" users with Azure AD B2B Collaboration hold a license via the Azure AD licenses. Like the conditional access policies, this is a paid Azure AD feature extended to "guest" users, thanks to the Azure B2B collaboration capacity, and requires a paid Azure AD license. In practice, Litware 369 receives five "guest" user rights with each paid Azure AD license. In other words, every paid Azure AD license that includes the rights to use the paid Azure AD feature for one Litware 369 employee, also includes the same user rights of the same feature for five other "guest" users working in Litware 369 partner companies.

For more information, refer to the article GUIDE TO AZURE ACTIVE DIRECTORY B2B COLLABORATION LICENSING[110].

Set-up risk-based conditional access with Azure AD Identity Protection

As the preceding figure shows, the notion of a risk profile (access from an anonymizing browser, from improbable places, several unsuccessful authentication attempts, and so on) can be integrated in the conditional access policies.

Azure AD Identity Protection[111] can be used to define conditional access policies that mitigate the risk of potentially dangerous connections by blocking them or by imposing multi-factor authentication. These policies are made possible by the Microsoft Intelligent Security Graph[112], constituted by the accumulated intelligence collected not only from all Microsoft products, cloud services, and internal teams but also from external sources. We use this data to calculate the risk level of an individual user or of an attempt to sign in. Azure AD Identity Protection reports any suspicious behavior and helps to investigate the situation and to take automated measures, such as locking out attempted connections or initiating a password reset.

In more general terms, Azure AD Identity Protection is a capacity of the Azure AD Premium P2 edition that can be used to:

- Detect potential vulnerability affecting identities in the organization.
- Configure automatic responses to detected suspicious actions relating to the identities in the organization.
- Examine suspicious incidents and take the appropriate measures to resolve them.

Note For more information, view the webinars AZURE AD AND IDENTITY SHOW: IDENTITY PROTECTION PREVIEW[113] and RESPOND TO ADVANCED THREATS WITH AZURE ACTIVE DIRECTORY IDENTITY PROTECTION[114].

Manage privileged identities in the cloud with Azure AD Privileged Identity Management (PIM)

The more elevated a user's privileges are, the more serious is the potential damage if their account is compromised. By providing greater visibility of these privileged identities, Azure AD Privileged Identity Management[115] (PIM) is a capacity of the Azure AD Premium P2 edition that helps to reduce the

---

[110] GUIDE TO AZURE ACTIVE DIRECTORY B2B COLLABORATION LICENSING: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-licensing

[111] AZURE ACTIVE DIRECTORY IDENTITY PROTECTION: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-identityprotection

[112] THE BILLIONS OF DATA POINTS THAT MAKE THE DIFFERENCE: https://www.microsoft.com/en-us/security/intelligence

[113] AZURE AD AND IDENTITY SHOW: IDENTITY PROTECTION PREVIEW: https://channel9.msdn.com/Series/Azure-AD-Identity/Azure-AD-and-Identity-Show-Identity-Protection-Preview

[114] RESPOND TO ADVANCED THREATS WITH AZURE ACTIVE DIRECTORY IDENTITY PROTECTION: https://youtu.be/rpmjqFERIvI

[115] WHAT IS AZURE AD PRIVILEGED IDENTITY MANAGEMENT?: https://azure.microsoft.com/en-us/documentation/articles/active-directory-privileged-identity-management-configure/

risk associated with administrator-based access privileges using controls, access management, and reports on these critical administrator roles.

Azure AD Privileged Identity Management (PIM) allows a better hygiene by enabling just-in-time (JIT) administration and just-enough administration. The goal is to enable the temporary granting of just-in-time privileged access or withdrawing permanent privileged access and making it a standard day-to-day activity. This capacity is now combined with the Azure Role-Based Access Control (RBAC) for resources management in Azure like, in the case of Litware 369, the institutional website and the customer and partners portals.

Note For more information, view the webinar INTRODUCTION TO AZURE AD PRIVILEGED IDENTITY MANAGEMENT (PIM)[116].

Reducing the time of privileges' exposure and increasing the visibility of their use help Litware 369 in its efforts to secure privileged access, as described in the section MANAGE ROLES AND RESPONSIBILITIES.

Note For more information, refer to the article SECURING PRIVILEGED ACCESS[117].

Manage internal privileged identities with Privileged Access Management (PAM)

In addition to the privileged identities for the Azure, Office 365, and Dynamics 365 subscriptions, Litware 369 also wants to grant just-in-time (JIT) privileges for its existing implementation of its on-premises AD. The Privileged Access Manager (PAM)[118] solution can achieve this goal by restricting privileged access in an existing AD environment.

PAM serves two purposes:

1. It restores the control of a compromised AD environment, while keeping a distinct known bastion environment that is not affected by malicious attacks.
2. It isolates the use of privileged accounts to reduce the risk of theft of the related credentials.

PAM is an instance of PIM that is implemented using Microsoft Identity Manager (MIM).

As well as doing away with permanent administrators, Litware 369 also wants to internally reproduce the principles of just-enough administration, like with PIM for the cloud. To do this, and to reduce the number of accounts with domain administration privileges and the corresponding risk of exposure, Litware 369 uses the so-called JEA (just-enough administration) functionality of Windows PowerShell to perform all its routine maintenance operations on the domain controllers. JEA technology is a PowerShell toolbox that defines a series of commands to perform privileged activities, and a terminal point where the administrators can be granted the suitable authorization(s) to execute these commands. JEA technology authorizes certain users to perform specific administrative tasks on the servers (such as the domain controllers), without granting any administrator rights.

---

[116] INTRODUCTION TO AZURE AD PRIVILEGED IDENTITY MANAGEMENT (PIM): https://channel9.msdn.com/Blogs/Concretement/Episode-27-Azure-AD-PIM

[117] SECURING PRIVILEGED ACCESS: https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access

[118] PRIVILEGED IDENTITY MANAGEMENT FOR ACTIVE DIRECTORY DOMAIN SERVICES: https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services

Note For more information, refer to the article JUST ENOUGH ADMINISTRATION[119].

Reinforce the security of access to customer accounts (the data subjects)

This section considers the processing scenario of the Litware 369 Customer portal.

As noted earlier (see section SECURELY MANAGE B2C ACCESS TO DATA, APPLICATIONS, AND OTHER RESOURCES), Azure AD B2C provides the ability to remove the need of using the accounts database in SQL Server to manage customer access and to create suitable user journeys.

By defining these journeys, Litware 369 benefits from the possibility of imposing strong authentication for its customers through the definition/configuration of the corresponding application policies for the Customer portal. This strong authentication uses the multi-factor authentication mentioned earlier.

This capability enables Litware 369 to benefit from its knowledge of its customers' phone numbers, which are part of the personal data collected in the representative processing scenario. An information notice in this processing operation informs users when collecting and recording their explicit consent.

While offering its customers the flexibility of using a social identity, such as Facebook, Google, Microsoft, or Twitter, which is a common practice on B2C-oriented sites and portals, Litware 369 at the same time reinforces the security of access to the accounts of its customers and standardizes the practice adopted for the employees of its partner companies for the B2B part.

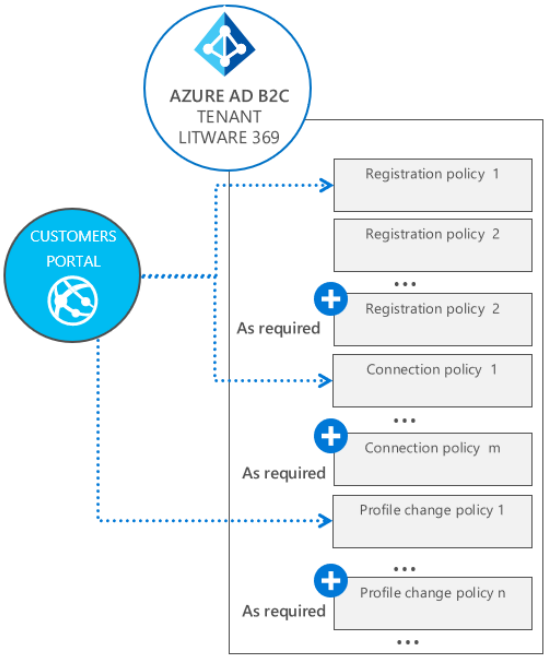


Figure 15. Implement adapted user journeys with Azure AD B2C

Adopt an "Assume personal data breaches" posture

The programmatic approach on the journey to GDPR compliance is governed by risks, and their circumstantial analysis helps to set the correct priorities and in particular, as illustrated by our

[119] JUST ENOUGH ADMINISTRATION: https://msdn.microsoft.com/powershell/jea/overview

representative processing scenario, to identify the appropriate technical measures in terms of security controls.

Then there is the "**Assume personal data breaches**" posture. What does this mean?

Protect the processing environment

In addition to the analysis and assessment of risks, the key requirements of the GDPR regarding the security of personal data are based on two pillars:

- Prevention and protection.
- Surveillance and detection.

These two pillars now require us to accept the troubling fact that personal data breaches are inevitable, despite all the measures we take to mitigate the risks identified in the preliminary study of the processing.

The assumption of personal data breaches allows us to take this fact into consideration and represents a major change that consists of **thinking that digital defenses are vulnerable at a given point of a processing**.

We live in a world where attacks and the attack vectors can come from anywhere. Every day, current events unfortunately show that attacks are becoming more and more sophisticated, that the attackers are better organized, and so on. It is a boundless and dynamic world that is constantly changing.

But adopting an "assume personal data breaches" posture is not a submission: it means that you have taken the first step toward mitigating the risks facing all your (personal) data in the digital age, as testified by the article ASSUMPTION OF BREACH: HOW A NEW MINDSET CAN HELP PROTECT CRITICAL DATA[120].

So what is plan B? What is the plan to detect intrusions? How to react to this type of incident?

This posture entails shifting from a simple **Protect and Recover** model to a new strategy and a more global posture that today includes at least the three aspects mentioned in the following diagram:

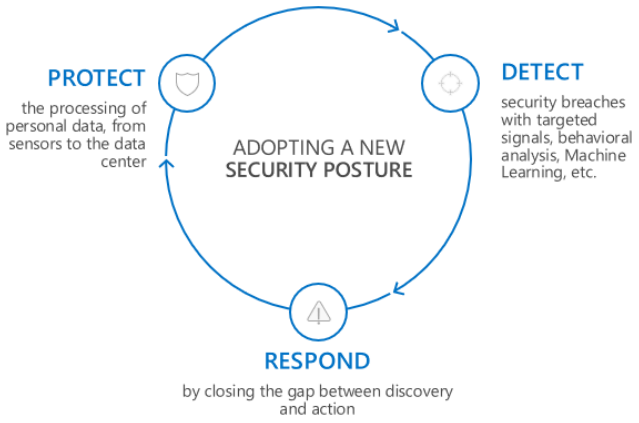


Figure 16. Adopt a new security posture

This strategy to protect the processing environment takes the form of a need to proactively prevent threats – which is what we previously meant by protection – to which the need to quickly detect and

[120] ASSUMPTION OF BREACH: HOW A NEW MINDSET CAN HELP PROTECT CRITICAL DATA: http://searchsecurity.techtarget.com/tip/Assumption-of-breach-How-a-new-mindset-can-help-protect-critical-data

respond to threats must be added. The three phases – protect, detect, and respond – constitute a continuum, as noted earlier.

Therefore, detecting an ongoing attack can prevent personal data leaks, and therefore a breach according to the GDPR, if these two new dimensions are taken into consideration properly.

In terms of detection, this consideration entails moving toward a more behavioral model in which breaches are detected by observing behavior (of the attack vector in the case of intrusion) using targeted signals, behavior analytics, and machine learning. For example, the detection of an attack in progress in a timely manner can prevent personal data exfiltration and, therefore, a breach, as per the GDPR.

The response presupposes the dynamic application of security controls in response to detection in order to fill the gap between the discovery and the reactive action. This application entails a radical change in the manner of reacting.

The next section explores how these dimensions can be applied to our processing scenario with the products and cloud services that Microsoft recommends for supporting this ongoing transformation.

Proactively prevent and detect, and quickly respond to threats

To begin with, our processing scenario concerns the Litware 369 institutional site and the Partner and Customer portals, plus associated Azure resources.

Help to prevent, detect, and respond to the threats facing personal data in Azure with Azure Security Center

Azure Security Center[121] provides visibility and control of Litware 369 Azure resources. It continually monitors the resources, provides useful security recommendations, and helps to prevent, detect, and respond to threats. The integrated advanced analysis functionality of Azure Security Center helps to identify the attacks that might not be detected, to understand them in depth, and to take the right steps to break the kill chain in time.

> **Note** For more information, refer to the article INTRODUCTION TO THE AZURE SECURITY CENTER[122] and view the webinar USE AZURE SECURITY CENTER TO PREVENT, DETECT, AND RESPOND TO THREATS[123].

[121] Azure Security Center: https://azure.microsoft.com/en-us/services/security-center/

[122] PRESENTATION OF THE AZURE Security Center: https://docs.microsoft.com/en-us/azure/security-center/security-center-intro

[123] USE AZURE SECURITY CENTER TO PREVENT, DETECT, AND RESPOND TO THREATS: https://youtu.be/iqwaja4NCso

Note For more information about security in Azure, view the presentation AZURE SECURITY SERVICES AND TECHNOLOGIES[124].

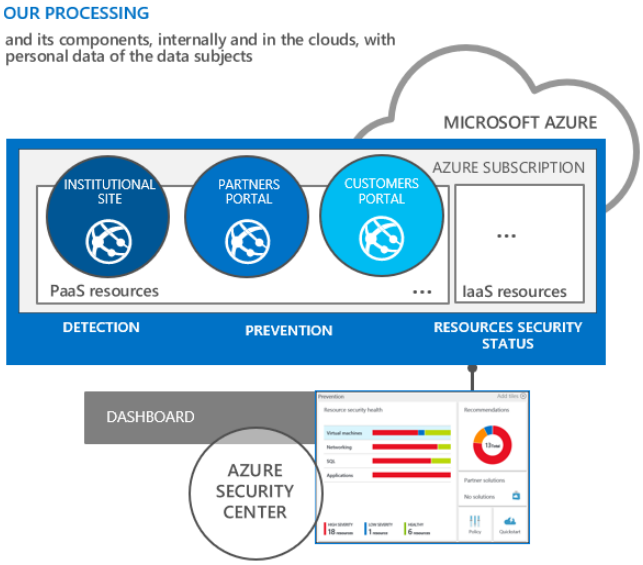


Figure 17. Help to prevent, detect, and respond to threats with increased visibility using Azure Security Center

Help to prevent, detect, and respond to the threats that face internal personal data with Advanced Threat Analytics (ATA) or Azure Advanced Threat Protection (ATP)

Our processing scenario now focuses on the internal infrastructure, that is, Active Directory and the SQL Server databases. The goal here is to protect the identities that access personal data and the resources that pertain to SQL Server, and to raise alerts in the event of suspicious activities.

In this context, Advanced Threat Analytics (ATA)[125] proposes a platform for the internal environment of companies like Litware 369 that helps to identify advanced security threats and attacks before they cause any damage.

Advanced Threat Analytics (ATA) helps locate breaches and identify the attackers using innovative anomaly detection and behavioral analytics technologies. ATA is deployed on-premises and operates with the existing implementation of Active Directory at Litware 369. It uses machine learning and behavioral analytics of users, and corresponding interactions, to find advanced and persistent threats and detect suspicious activity, or even malicious attacks used by cybercriminals, by identifying breaches before they do any harm. An easy-to-use chronological analysis with in-depth investigation capabilities is available, plus the dispatch of alerts in near real-time.

[124] Azure security services and technologies: https://docs.microsoft.com/en-us/azure/security/azure-security-services-technologies

[125] Advanced Threat Analytics (ATA): https://www.microsoft.com/en-us/cloud-platform/advanced-threat-analytics

Note For more information, refer to the article WHAT IS ADVANCED THREAT ANALYTICS?[126] and view the webinar USE AZURE SECURITY CENTER TO PREVENT, DETECT, AND RESPOND TO THREATS[127].

The recently announced Azure Advanced Threat Protection (ATP) service now offers similar capabilities, but in the form of a managed service in Azure.

Note For more information, refer to the paper INTRODUCING AZURE ADVANCED THREAT PROTECTION[128].

Analyze and score the security of an Office 365 subscription with Secure Score

Our processing scenario now focuses on the Office 365 collaboration services, which in this case are Exchange Online and SharePoint Online. In particular, this focus concerns the SharePoint Online cloud service, with the library of Word files (order files with the technical characteristics of the installation).

Secure Score is a tool that analyzes the security of the Office 365 services. Available at https://securescore.office.com, this tool scores the Litware 369 environment based on the current security parameter settings, in comparison with all the available and applicable parameters. A chronology is provided showing the progression of the security level of the environment, with a comparison of the average measure amongst all other Office 365 customers.

Remediation suggestions are provided to mitigate the security risks and eventually improve the score.

Note For more information, refer to the article INTRODUCING THE OFFICE 365 SECURE SCORE[129] and view the webinar AN INTRODUCTION TO OFFICE 365 SECURE SCORE[130].

Consequently, Litware 369 receives relevant suggestions about controls and security settings that can reduce the risk of attack against personal data and can track the progression of the global security level.

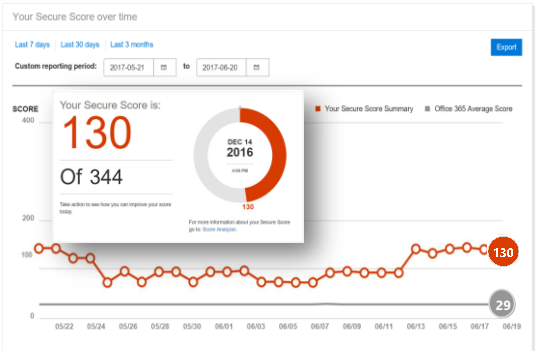


Figure 18. Analyze and rate the security of an Office 365 subscription with Secure Score

[126] WHAT IS ADVANCED THREAT ANALYTICS?: https://docs.microsoft.com/en-us/advanced-threat-analytics/what-is-ata

[127] USE AZURE SECURITY CENTER TO PREVENT, DETECT, AND RESPOND TO THREATS: https://youtu.be/iqwaja4NCso

[128] INTRODUCING AZURE ADVANCED THREAT PROTECTION: https://cloudblogs.microsoft.com/enterprisemobility/2017/09/27/introducing-azure-advanced-threat-protection/

[129] INTRODUCING THE OFFICE 365 SECURE SCORE: https://support.office.com/en-US/article/Introducing-the-Office-365-Secure-Score-c9e7160f-2c34-4bd0-a548-5ddcc862eaef?ui=en-US&rs=en-US&ad=US/

[130] AN INTRODUCTION TO OFFICE 365 SECURE SCORE: https://www.youtube.com/watch?v=h__nxWlm5Nc&feature=youtu.be

Protect and manage compliance for all Litware 369 data with the Office 365 Compliance and Security Center

At this point, our processing scenario is the same as in the previous section – that is, the Office 365 collaboration services.

Display and manage advanced security alerts

The availability of threat intelligence helps to proactively discover advanced threats and to protect Litware 369 resources in Office 365. Precise intelligence about the threats provided by Microsoft worldwide presence, the Intelligent Security Graph mentioned earlier, and information from cybernetic threat hunters helps to quickly and efficiently raise alerts and deploy dynamic policies and security measures.

> **Note** For more information, refer to the paper APPLYING INTELLIGENCE TO SECURITY AND COMPLIANCE IN OFFICE 365[131].

Audit and monitor the activity of Litware 369 Office 365 users

Advanced Security Management (ASM) identifies high risks or abnormal usages and informs Litware 369 administrators of potential breaches. It can also be used to define activity policies to keep track of and respond to actions that incur high levels of risk.

> **Note** For more information, refer to the paper GAIN ENHANCED VISIBILITY AND CONTROL WITH OFFICE 365 ADVANCED SECURITY MANAGEMENT[132] and view the webinar INTRODUCING ADVANCED SECURITY MANAGEMENT FOR OFFICE 365[133].

Help to prevent, detect, and respond to the threats facing personal data in Dynamics 365

The final portion of this section is about the Dynamic 365 cloud service.

As has already been stated several times, controlling access to personal data is a key aspect of data protection and security.

Dynamics 365 relies on the security of the identities in Azure AD and can be used to manage and control access to data in several ways:

- **Role-based security** in Dynamics 365 groups together a number of privileges to limit the tasks that can be performed by a given user. This is crucial functionality, especially when users change roles in a company; for example, in our case, for Litware 369 employees who join as an internal move to the Subscriptions entity or employees who leave it.
- **Records-based security** in Dynamics 365 limits access to specific records.
- **Field-level security** in Dynamics 365 limits access to specific high-impact fields, such as personally identifiable information (PII).

---

[131] APPLYING INTELLIGENCE TO SECURITY AND COMPLIANCE IN OFFICE 365: https://blogs.office.com/2016/09/26/applying-intelligence-to-security-and-compliance-in-office-365/

[132] GAIN ENHANCED VISIBILITY AND CONTROL WITH OFFICE 365 ADVANCED SECURITY MANAGEMENT: https://blogs.office.com/2016/06/01/gain-enhanced-visibility-and-control-with-office-365-advanced-security-management/

[133] INTRODUCING ADVANCED SECURITY MANAGEMENT FOR OFFICE 365: https://www.youtube.com/watch?v=gWTSTqNHgSg

Dynamics 365 also has the capacity to keep track of activities.

Note For more information, refer to the dedicated blog[134] and view the webinar DYNAMICS 365 FOR OPERATIONS – TECH TALK: REPORTING OPTIONS[135].

Examples of solutions

Generally speaking, and beyond the restricted framework of our illustration, the protection of personal data and the "assume personal data breaches" approach can also take advantage of other products and cloud services from Microsoft, in addition to the examples mentioned in this paper.

Note The white paper THE START OF YOUR ROAD TO COMPLIANCE WITH THE GENERAL REGULATION ON DATA PROTECTION[136] contains examples of actions that you can take with Microsoft right away to get started on your way to GDPR compliance. This white paper contains an illustration of the measures to be taken in this context for the protection of personal data, and of how Microsoft products and cloud services can contribute to the execution (or the effective expression) of these measures.

Report - Maintain the required documentation and handle requests pertaining to personal data and notification of breach

The path to compliance with the GDPR inevitably leads to the reporting stage and everything to do with the necessary documentation.

Similar to previous steps, this step corresponds to a series of activities in the **CHECK** phase (of the PDCA model) of the GDPR program suggested in the white paper GDPR – GET ORGANIZED AND IMPLEMENT THE RIGHT PROCESSES FOR COMPLIANCE WITH THE GDPR. In particular, these activities and actions aim to produce and maintain over time the documentation pertaining to compliance with the GDPR.

The following paragraphs illustrate how these actions take shape, using some examples of Microsoft products and cloud services.

Produce the documentation pertaining to compliance with the GDPR

There are a number of aspects to produce the documentation required to prove compliance and manage the exercise of new rights and breach notification.

In the context that interests us, and in support of these activities, the goal consists of defining the tools used to guarantee that the processing of personal data is monitored and recorded in documents or logs, for data collection, use, transfer, and so on.

---

[134] Blog Microsoft Dynamics 365: https://community.dynamics.com/b/msftdynamicsblog

[135] DYNAMICS 365 FOR OPERATIONS – TECH TALK: REPORTING OPTIONS: https://youtu.be/NzZONjKs5xA

[136] THE START OF YOUR ROAD TO COMPLIANCE WITH THE GENERAL REGULATION ON DATA PROTECTION: https://aka.ms/gdprwhitepaper

Produce the documentation pertaining to data processors

In this section, our representative processing scenario concerns the Azure, Office 365, and Dynamics 365 subscriptions.

A number of legitimate questions can and must be asked with the GDPR:

Who has access to your data? Where is it? What does Microsoft do to protect it? How can you make sure that Microsoft fulfills its commitments?

These questions are answered in the complete documentation in the Microsoft Trust Center[137] on compliance, security, and privacy. In particular, this documentation contains the service offering descriptions, the compliance audit reports for the certifications and accreditations held, plus a body of documents comprising FAQs, white papers, compliance guides, security analyses, and penetration tests.

Microsoft is committed to compliance with the GDPR for Microsoft cloud services, as testified by Brendon Lynch, Microsoft Privacy Officer, in the video MICROSOFT COMMITMENTS TO GDPR[138]. This video is a reflection of how Microsoft operates its cloud services, by adopting high ethical standards that provide transparency on the way services are designed and operated, and how we protect customer data.

Provide non-falsifiable and trustworthy information based on activity logs

In addition to the production of the documentation as described, our processing scenario covers the use of the resources of the Azure, Office 365, and Dynamics 365 subscriptions, namely:

- The Litware 369 institutional website, and the Partner and Customers portals
- Exchange Online, including mailboxes and email messages
- SharePoint Online, including the library of Word files (order files with the technical characteristics of the installation)
- Dynamics 365 and the customer accounts, contract numbers, and so on

The goal is to provide non-falsifiable and trustworthy information based on activity logs that pertain to the processing.

Azure provides configurable audit and logging options that can help to identify any gaps in the security policies, so that they can be fixed to prevent breach.

For example, Azure Log Analytics[139] helps collect and analyze the data produced by the resources in your cloud environment or on-premises. It delivers information in real time that can be used in integrated searches and personalized dashboards to rapidly analyze millions of records on the workloads and servers, no matter where they are located physically in a hybrid cloud context.

Note For more information, refer to the article PRESENTATION OF LOG ANALYTICS[140] and view the webinar COMBATING CORPORATE SECURITY THREATS: GETTING STARTED WITH LOG ANALYTICS[141].

[137] The Microsoft Trust Center: http://www.microsoft.com/en-us/trustcenter

[138] MICROSOFT'S COMMITMENTS TO GDPR: https://aka.ms/GDPRCommitmentVideo

[139] Azure Log Analytics: https://azure.microsoft.com/en-us/services/log-analytics/

[140] PRESENTATION OF LOG ANALYTICS: https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-overview

[141] COMBATING CORPORATE SECURITY THREATS: GETTING STARTED WITH LOG ANALYTICS: https://youtu.be/1bDj0lSAvTY

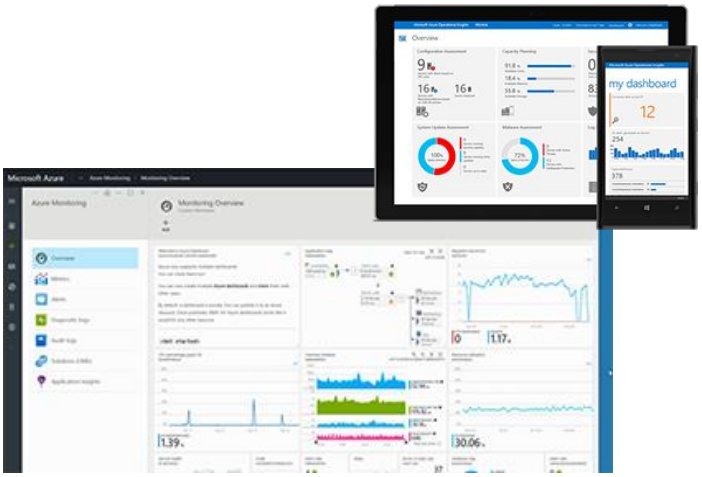


Figure 19. Provide non-falsifiable and trustworthy information pertaining to the processing with Azure Monitor/Azure Log Analytics

Similarly, Office 365 audit trails[142] can be used to monitor and track the activities of users and administrators on Litware 369 Office 365 workloads to contribute to the advanced detection and examination of issues related to security and compliance.

Note For more information, view the webinar OWN YOUR DATA AND SERVICE – MONITOR AND INVESTIGATE WITH OFFICE 365 AUDITING, INSIGHTS AND ALERTS[143].

Provide a compliance management dashboard

Finally, and in addition to the previous examples, it is important to highlight the Compliance Manager, now in public preview, that is designed to help you manage your compliance posture for all Microsoft cloud services from a single point.

Compliance Manager will enable you to assess the risks to Microsoft cloud services in real time by producing a score that reflects your performance in terms of compliance with the various regulatory requirements that pertain to data protection.

You will also be in a position to manage the integrated controls and reporting tools to improve and monitor your compliance posture.

[142] SEARCH THE AUDIT LOG IN THE OFFICE 365 Security & Compliance Center: https://support.office.com/en-us/article/Search-the-audit-log-in-the-Office-365-Security-Compliance-Center-0d4d0f35-390b-4518-800e-0c7ec95e946c

[143] OWN YOUR DATA AND SERVICE - MONITOR AND INVESTIGATE WITH OFFICE 365 AUDITING, INSIGHTS AND ALERTS: https://youtu.be/CEeOCoV863U

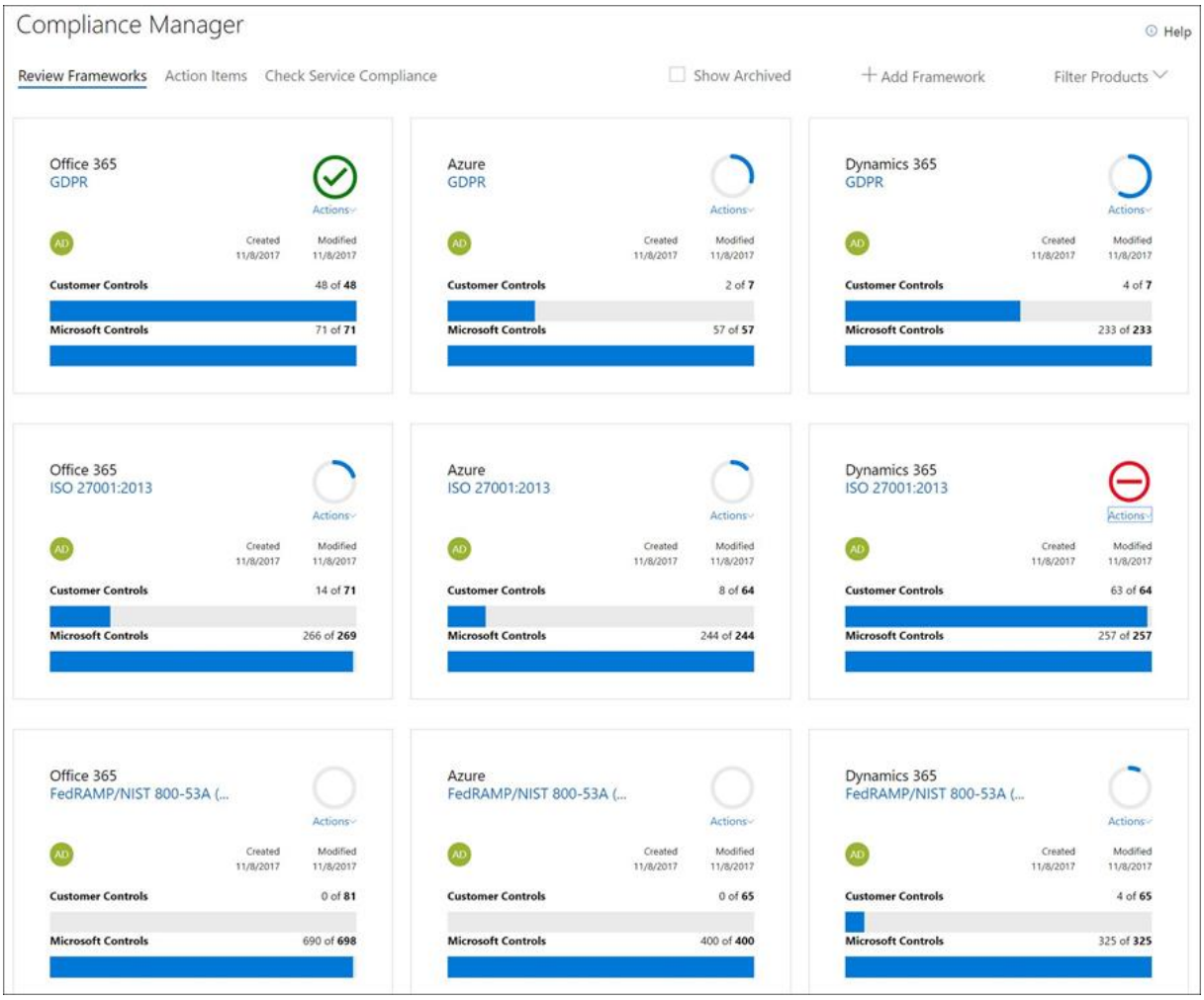


Figure 20. Example of a Compliance Manager dashboard

Important note Recommendations from Compliance Manager should not be interpreted as legal guidance or a guarantee of compliance.

Note For more information, learn more from the Tech Community blog.[144]

Note You can sign up for the Compliance Manager trial by visiting https://aka.ms/compliancemanager.

Examples of solutions

The activity logs offered by Microsoft cloud services help to produce non-falsifiable and trustworthy information about the processing. This information is one part of the documentation to be produced and maintained, like the documentation about the data processor which, for the Litware 369 use of cloud services, is Microsoft.

[144] MANAGE YOUR COMPLIANCE FROM ONE PLACE – ANNOUNCING COMPLIANCE MANAGER PREVIEW PROGRAM: https://aka.ms/compliance-manager-blog

Generally speaking, and not only within the restricted framework of our scenario, the production and maintenance overtime of the necessary documentation can also take advantage of other products and cloud services from Microsoft, in addition to the examples mentioned here.

Note The white paper THE START OF YOUR ROAD TO COMPLIANCE WITH THE GENERAL REGULATION ON DATA PROTECTION[145] contains examples of actions that you can take with Microsoft right away to get started on your path to compliance with the GDPR. You can refer to this white paper for an illustration of the actions to be taken in this context, to produce and keep your documentation on the processing operations up to date over time, and of how Microsoft products and cloud services can help you achieve compliance.

[145] THE START OF YOUR ROAD TO COMPLIANCE WITH THE GENERAL REGULATION ON DATA PROTECTION: https://aka.ms/gdprwhitepaper

Conclusion

As stated in the introduction to this white paper, Microsoft is by your side to help you on the path to compliance with the GDPR:

- Microsoft cloud services, such as Azure, Office 365, and Dynamics 365, to mention only those used in our representative processing scenario, enable you to facilitate the processes that you must implement to achieve compliance with the GDPR, thanks to artificial intelligence (AI), innovation, and collaboration.
- Microsoft on-premises solutions and cloud services help you to locate and catalog personal data in your systems' processing operations, to build a more secure hybrid environment, and to simplify the management and monitoring of personal data. We hope that the illustrations provided by our representative processing scenario will enable you to better appreciate their benefits.
- Microsoft is investing in additional functionality and capacities to help organizations meet their GDPR requirements, some of which were mentioned in this paper as we made our way through the main steps on the path to compliance with the GDPR.
- Finally, we share our own experts' best privacy practices.

We hope that this white paper provides you the opportunity to start your journey along the path to compliance with the GDPR if you have not already done so. The regulation will take effect on May 25, 2018.

References

Useful links in the Microsoft Trust Center

- About Microsoft services and products on microsoft.com/GDPR:
  - Microsoft Azure
  - Microsoft Dynamics 365
  - Microsoft Enterprise Mobility + Security (EM+S)
  - Microsoft Office and Office 365
  - Microsoft SQL Server and Azure SQL Database (database as a service)
  - Windows 10 and Windows Server 2016
- e-books and white papers:
  - An Overview of the General Data Protection Regulation[146]
  - Accelerate your GDPR compliance with the Microsoft Cloud[147]
  - Beginning your General Data Protection Regulation (GDPR) journey[148]
  - Discover how to start your journey toward GDPR compliance while using Microsoft Dynamics 365 applications[149]
  - How Microsoft Azure Can Help Organizations Become Compliant with the GDPR[150]
  - Supporting Your EU GDPR Compliance Journey With Enterprise Mobility + Security[151]
  - Accelerate your GDPR compliance journey with Microsoft 365[152]
  - Guide to enhancing privacy and addressing GDPR requirements with the Microsoft SQL Platform[153]
  - Accelerate GDPR with Windows 10[154]

---

[146] An Overview of the General Data Protection Regulation: https://aka.ms/GDPROverview

[147] Accelerate your GDPR compliance with the Microsoft Cloud: https://aka.ms/gdprebook

[148] Beginning your General Data Protection Regulation (GDPR) journey: https://aka.ms/gdprwhitepaper

[149] Discover how to start your journey toward GDPR compliance while using Microsoft Dynamics 365 applications: https://info.microsoft.com/GDPRAssessmentResponses-Registration.html

[150] An Overview of the General Data Protection Regulation: https://aka.ms/GDPROverview:

[151] Supporting your EU GDPR compliance journey with Microsoft EMS: https://aka.ms/emsgdprwhitepaper

[152] Accelerate your GDPR compliance journey with Microsoft 365: https://resources.office.com/ww-landing-M365EGDPR-accelerate-your-GDPR-compliance-whitepaper.html?LCID=EN-US

[153] Guide to enhancing privacy and addressing EU GDPR requirements with the Microsoft SQL platform: http://aka.ms/gdprsqlwhitepaper

[154] Accelerate GDPR with Windows 10: https://aka.ms/WindowsGDPRwhitepaper

Some papers (on the key scenarios covered by Microsoft Enterprise Mobility + Security):

- How Microsoft EMS can support you in your journey to EU GDPR compliance[155].
- Azure Information Protection[156] – How to persistently protect personal data locally and in the cloud.
- Azure Active Directory[157] – How to grant or restrict access to personal data.
- Cloud App Security[158] – How to protect personal data in mobile devices and applications.
- Intune[159] – How to heighten visibility and control personal data in cloud applications.
- Advanced Threat Analytics[160] – How to detect vulnerability before it causes any damage

[155] How Microsoft EMS can support you in your journey to EU GDPR compliance – Part 1: https://blogs.technet.microsoft.com/enterprisemobility/2017/05/24/how-microsoft-ems-can-support-you-in-your-journey-to-eu-gdpr-compliance/

[156] How Microsoft EMS can support you in your journey to EU GDPR compliance – Part 2: https://blogs.technet.microsoft.com/enterprisemobility/2017/06/06/how-microsoft-ems-can-support-you-in-your-journey-to-eu-gdpr-compliance-part-1/

[157] How Microsoft EMS can support you in your journey to EU GDPR compliance – Part 3: https://blogs.technet.microsoft.com/enterprisemobility/2017/06/27/how-microsoft-ems-can-support-you-in-your-journey-to-eu-gdpr-compliance-part-3/

[158] How Microsoft EMS can support you in your journey to EU GDPR compliance – part 4: https://blogs.technet.microsoft.com/enterprisemobility/2017/07/07/how-microsoft-ems-can-support-you-in-your-journey-to-eu-gdpr-compliance-part-4/

[159] How Microsoft EMS can support you in your journey to EU GDPR compliance – Part 5: https://blogs.technet.microsoft.com/enterprisemobility/2017/07/13/how-microsoft-ems-can-support-you-in-your-journey-to-eu-gdpr-compliance-part-5/

[160] How Microsoft EMS can support you in your journey to EU GDPR compliance – Part 6: https://blogs.technet.microsoft.com/enterprisemobility/2017/08/07/how-microsoft-ems-can-support-you-in-your-journey-to-eu-gdpr-compliance-part-6/

Microsoft France
39 Quai du Président Roosevelt
92130 Issy-Les-Moulineaux