

Microsoft General Data Protection Regulation - Detailed Assessment

Delivery Guide v3 – April 2018

microsoft.com/gdpr

Table of Contents

[Intended usage 3](#_Toc510019569)

[Disclaimer 3](#_Toc510019570)

[Delivering the Microsoft GDPR Assessment 4](#_Toc510019571)

[Microsoft GDPR Detailed Assessment tool overview 5](#_Toc510019572)

[Scope 5](#_Toc510019573)

[Purpose 5](#_Toc510019574)

[Audience 5](#_Toc510019575)

[Overview of the GDPR 6](#_Toc510019576)

[Brief GDPR background 6](#_Toc510019577)

[DMPR themes – Discover, Manage, Protect and Report 6](#_Toc510019578)

[Discover: Identify what personal data you have and where it resides 6](#_Toc510019579)

[Manage: Govern how personal data is used and accessed 7](#_Toc510019580)

[Protect: Establish security controls to prevent, detect, and respond to vulnerabilities and data breaches 7](#_Toc510019581)

[Report: Execute on data requests, report data breaches, and keep required documentation 8](#_Toc510019582)

[Key terms 9](#_Toc510019583)

[Step 1 - Customer pre-engagement meeting 11](#_Toc510019584)

[Determine the appropriate customer responders 12](#_Toc510019585)

[Step 2 – Assessment 14](#_Toc510019586)

[Engagement kick-off meeting. 14](#_Toc510019587)

[GDPR Detailed Assessment 15](#_Toc510019588)

[Walkthrough of how to use the Microsoft GDPR Detailed Assessment 16](#_Toc510019589)

[Compliance manager integration 21](#_Toc510019590)

[Outcome Analysis & Write-Up 26](#_Toc510019591)

[How to use Power BI with the Microsoft GDPR Detailed Assessment 27](#_Toc510019592)

[Update the Close-Out presentation template 33](#_Toc510019593)

[Step 3 – Close Out presentation 34](#_Toc510019594)

[Appendix – Microsoft GDPR Detailed Assessment Toolkit content 35](#_Toc510019595)

[We look forward to your feedback! 35](#_Toc510019596)

# Intended usage

This model is a question-driven assessment tool for preparing for the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). The tool is intended to be used by Microsoft partners to assist customers in identifying where they are on the journey to GDPR readiness. Output from the tool includes identification of gaps in customer readiness and recommendations to consider for closing any gaps. Recommendations are organized into the categories People, Process and Technology.

# Disclaimer

This GDPR Detailed Assessment is intended to assist organizations with assessing their GDPR compliance progress.  This GDPR Detailed Assessment is provided for general public informational purposes only.  Any results, scoring or recommendations produced by the GDPR Detailed Assessment should not be relied upon to determine how GDPR applies to an organization or an organization’s compliance with GDPR, and they do not constitute legal advice, certifications or guarantees regarding GDPR compliance.  Instead, we hope the GDPR Detailed Assessment identifies technologies and additional steps that organizations can implement to simplify their GDPR compliance efforts.  The application of GDPR is highly fact-specific. We encourage all organizations using this GDPR Detailed Assessment to work with a legally qualified professional to discuss GDPR, how it applies specifically to their organization, and how best to ensure compliance.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS GDPR DETAILED ASSESSMENT. Microsoft disclaims any conditions, express or implied, or other terms that use of the Microsoft products or services will ensure the organization’s compliance with the GDPR.  This GDPR Detailed Assessment is provided “as-is.”  Information and recommendations expressed in this GDPR Detailed Assessment may change without notice.

This GDPR Detailed Assessment does not provide the user with any legal rights to any intellectual property in any Microsoft product or service.  Use of the tool is for internal, reference purposes only; however, Microsoft partners may distribute the GDPR Detailed Assessment to their customers for such customers’ internal, reference purposes only. Any distribution of the GDPR Detailed Assessment by a Microsoft partner to its customers must include terms consistent with those set forth in this disclaimer.

© 2017 Microsoft.  All rights reserved

# Delivering the Microsoft GDPR Assessment

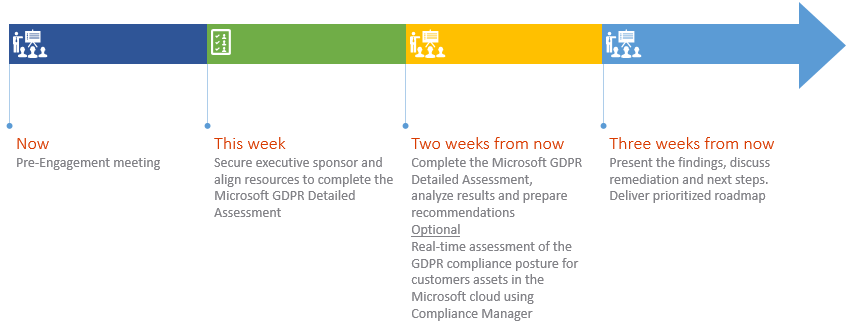
The Microsoft GDPR Detailed Assessment is a three-step process that Microsoft partners will engage in with their customers to assess their overall GDPR maturity. This delivery guide describes the activities for each step, provides execution guidance and tips, discusses resources and deliverables and is focused on a successful engagement and valuable outcome.

The illustration below depicts a high-level overview of the steps and their activities.



The following paragraphs will describe each of the steps in more detail, provide background on de Microsoft DMPR (Discover, Manage, Protect and Report) approach that helps customers on their journey to GDPR compliance and provide guidance on how to use the Microsoft GDPR Detailed Assessment tool.

The overall duration for the engagement is expected to be between 3-4 weeks, while the total effort is estimated to be between 10 and 20 hrs. depending on the complexity of the organization and the number of participants.



# Microsoft GDPR Detailed Assessment tool overview

The Microsoft GDPR Detailed Assessment tool consists of an Excel workbook, a Power BI output file, and a PowerPoint template for customer discussions. The Excel file is made up of yes/no questions, grouped by theme and sub-scenario. The four themes are Discover, Manage, Protect, and Report (DMPR), and the sub-scenarios are more granular activities within those themes. The backend mechanics for how recommendations are generated is hidden by default and can be accessed by unhiding the hidden tabs. Use caution if making any changes to the hidden tabs, as this could break key analysis formulas, as well as the outputs in Power BI.

The Power BI output file is linked to the Excel file and provides high-level visualizations of the end-customers’ maturity overall and within each theme. It also generates recommendations to help customers improve their GDPR maturity within each theme.

Additionally, the GDPR Detailed Assessment tool provides integration with Microsoft Compliance manager, enabling partners to work with their customers on assessing the GDPR compliance posture for the customers assets in the Microsoft cloud, such as Office 365.

## Scope

The Microsoft GDPR Detailed Assessment is intended for use by Microsoft partners to assess their customers’ overall GDPR maturity. It is *not* offered as a GDPR compliance attestation. Customers are responsible for ensuring their own GDPR compliance and are advised to consult their legal and compliance teams for guidance. This tool is *not* to be used to certify compliance, but instead highlights tools and concepts that can be used to support a customer’s journey towards GDPR compliance. It is the distributed responsibility of the customer and their legal and compliance teams to certify their own GDPR compliance.

## Purpose

Partners can use the tool’s questions to help customers assess the maturity of their people, processes, and technology, relevant to the GDPR. Partners can then leverage the tool’s visuals and recommendations to guide customers to appropriate solutions, enabling them to elevate their GDPR maturity.

## Audience

Microsoft GDPR Detailed Assessment users are expected to be familiar with the GDPR. Customer responders are anticipated to have a high-level understanding of their business function and some detailed knowledge of how it is executed. In some cases, this may require multiple individuals from the same department.

# Overview of the GDPR

## Brief GDPR background

The GDPR strengthens the rights of individuals in the European Union (EU) to control their personal data and requires organizations to bolster their privacy and data protection measures. The regulation imposes new organizational requirements, which can include appointing a Data Protection Officer (DPO), carrying out Data Protection Impact Assessments (DPIAs), and protecting personal data by design and default. Data subjects will have significantly enhanced rights, such as to access and receive a copy of their personal data, as well as to have it erased. Notably, organizations who violate the GDPR could face fines up to the greater of €20 million or 4% of annual global turnover (revenue), whichever is greater. The regulation was approved 27 April 2016 and enforcement begins the 25th of May 2018. For more GDPR background, visit [Microsoft.com/GDPR](https://ts.accenture.com/sites/MS-GDPR/Shared%20Documents/GDPR%20Maturity%20Model/Final%20deliverables/How%20to%20Guide/microsoft.com/gdpr).

## DMPR themes – Discover, Manage, Protect and Report

Preparing for the GPDR is complex. Microsoft recommends partners and customers to approach the regulation by focusing on an overall set of key controls and capabilities. These can be summarized by four vital areas: Discover, Manage, Protect, and Report.

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

The first step towards GDPR compliance is to assess whether the GDPR applies to your organization, and, if so, to what extent. This analysis starts with understanding what data you have and where it resides.

#### Does the GDPR apply to my data?

The GDPR regulates the collection, storage, use, and sharing of “personal data.” Personal data is defined very broadly under the GDPR as *any* data that relates to an identified or identifiable natural person.

*Article 4 – Definitions*

*‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; [[1]](#footnote-2)*

If your organization processes such data—in customer databases, in feedback forms filled out by your customers, in email content, in photos, in CCTV footage, in loyalty program records, in HR databases, or anywhere else—or wishes to collect it, and if that data belongs to or relates to a data subject in the Union, then you need to comply with the GDPR. Note that personal data doesn’t need to be stored or processed in the EU to be subject to the GDPR—the GDPR applies to companies, government agencies, non-profits, and other organizations that offer goods and services to people in the EU or that collect and analyze data tied to EU citizens, residents, tourists, and other persons visiting the EU.

#### Building your inventory

To understand whether the GDPR *does* apply to your organization and, if it does, what obligations it imposes, it is important to inventory your organization’s data. This will help you to understand what information is personal data, and to identify the systems where that data is collected and stored, understand why it was collected, how it is processed and shared, and how long it is retained.

### Manage: Govern how personal data is used and accessed

The GDPR provides data subjects—individuals to whom data relates—with more control of how their personal data is captured and used. Data subjects can, for example, request that your organization provides information on the processing of data that relates to them, transfer their data to other services, correct mistakes in their data, or restrict certain data from further processing in certain cases. In some cases, these requests must be addressed within fixed time periods.

#### Data governance

To satisfy your obligations to data subjects, you will need to understand what types of personal data your organization processes, how, and for what purposes. The data inventory discussed previously is a first step to achieving this understanding. Once that inventory is complete, it is also important to develop and implement a data governance plan. A data governance plan can help you define policies, roles, and responsibilities for the access, management, and use of personal data, and can help you ensure your data handling practices comply with the GDPR. For example, a data governance plan can give your organization confidence that it effectively respects data subject demands to delete or transfer data.

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

Organizations increasingly understand the importance of information security—but the GDPR raises the bar. It requires that organizations take appropriate technical and organizational measures to protect personal data from loss or unauthorized access or disclosure.

#### Protecting your data

Data security is a complex area. There are many types of risk to identify and consider—ranging from physical intrusion or rogue employees to accidental loss or hackers. Building risk management plans and taking risk mitigation steps, such as password protection, audit logs, and encryption, can help you ensure compliance.

The Microsoft cloud is specifically built to help you understand risks and to defend against threats, it is more secure than on-premises computing environments in many ways. For example, Microsoft datacenters are certified to internationally recognized security standards; protected by 24-hour physical surveillance; and have strict access controls.

How we secure our cloud infrastructure is only part of a comprehensive security solution and each of our products, either in the cloud or on-premises, have security features to help you secure your data.

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

The GDPR sets new standards in transparency, accountability, and record-keeping. You will need to be more transparent about how you handle personal data and also actively maintain documentation defining your processes and use of personal data.

#### Record-keeping

Organizations processing personal data will need to keep records about the purposes of processing; the categories of personal data processed; the identity of third parties with whom data is shared; whether (and which) countries outside the EU personal data is transmitted to, and the legal basis of such transfers; organizational and technical security measures; and data retention times applicable to various datasets. One way to achieve this is using auditing tools, which can help to ensure that any processing of data—whether it be collection, use, sharing, or otherwise—is tracked and recorded.

# Key terms

These terms are intended to assist the partner in using and understanding the Microsoft GDPR Detailed Assessment. The terms identified below may have different or additional definitions set forth in the GDPR.

**Automatically/automated:** an action or process done by machines/computers with minimal human involvement.

**Binding corporate rules:** one of several lawful means to transfer data from the EU to a third country that has not received an adequacy decision.

**Codes of conduct:** policies or guidelines which, when approved by a European Union Member State and followed by an organization, can be used as an element to demonstrate compliance with the GDPR.

**Confidentiality, integrity, and availability (CIA):** primary objectives of information security. Confidentiality means only authorized individuals may access the information. Integrity means keeping the information accurate and modifiable by only authorized subjects. Availability means intended users can access and use the information, as expected in a timely manner.

**Controller:**the organization that determines the purposes and means of the processing of personal data.

**Controls (noun):** protections that help reduce security risk.

**Data breach notices:** communications informing required recipients personal data has been accessed by unauthorized persons or entities.

**Data governance:** the overall control and management of data’s storage, usage, confidentiality, integrity, and availability.

**Data protection impact assessment (DPIA):** an evaluation of how processing personal data in an organization could pose a high risk to the rights and freedoms of natural person and how to mitigate those risks

**Data Protection Officer (DPO):** a potentially required oversight position for organizations, depending on how they use personal data. DPOs are responsible for helping ensure their organizations comply with data protection requirements.

**Data store:** any technology that maintains or houses data.

**Data subject:** a person whose personal data is processed by an organization.

**First point of contact:** the first time an organization communicates with a data subject.

**Input validation:** a means of ensuring only data of an authorized structure, content, and arrangement/order is maintained in an organization’s data stores.

**Inventory:** a complete list of items.

**Legal justification:** one of several bases upon which an organization may process personal data, such as consent, contract, legitimate interest, and compliance with legal obligations.

**Machine-readable:** something a computer or machine can readily process and understand. For files, this includes types such as .xls and .html.

**Personal data:** any information relating to an identified or identifiable natural person.

**Personnel:** people who perform work for an organization, such as employees or contractors.

**Principle of least privilege:** a concept that users and systems should be granted access to only the amount of data they need to perform their responsibilities.

**Privacy notices:** communications to data subjects about how their personal data is used and what their GDPR data subject rights are (such as to request their personal data be erased).

**Processing:** any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**Processor:** organization that processes personal data on behalf of the controller.

**Pseudonymize:** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, if such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

**Restrict processing of personal data:** limit or reduce how personal data is processed.

**Sub-processors:** entities who process personal data on behalf of an organization’s principal processing partner/contractor.

# Step 1 - Customer pre-engagement meeting

The customer pre-engagement meeting typically is an online meeting organized one to two weeks prior to the actual onsite activities. During this online meeting, the partner will introduce the customer to the Microsoft GDPR Detailed Assessment, discuss the upcoming activities and align expectations and timelines. For customers that have had no prior exposure to the GDPR it is possible to include a high-level introduction explaining the GDPR and its possible impact on the organization.

The partner will also provide a preview of the Microsoft GDPR Detailed Assessment questions to help identify the customer representatives that will assist in answering.

**Objectives**

The objectives for the pre-engagement meeting are to:

* Introduce the engagement and the tools that will be used;
* Align expectations;
* Decide on the starting date for the on-site activities and define timelines;
* Determine the appropriate customer responders that will be interviewed during the assessment

**Resources**

* *<01 - Microsoft GDPR Detailed Assessment - Pre Engagement Presentation.pptx>*

**Preparation**

To prepare for this pre-engagement meeting the partner consultant leading the assessment should:

* Be familiar with the GDPR;
* Become acquainted with the Microsoft GDPR Detailed Assessment;
* Familiarize him/herself with the Microsoft GDPR Detailed Assessment tool;
* Familiarize him/herself with Microsoft Compliance Manager
* Customize the <*01 - Microsoft GDPR Detailed Assessment - Pre Engagement Presentation.pptx>* template with customer specific data and insights.   
  The <*01 - Microsoft GDPR Detailed Assessment - Pre Engagement Presentation.pptx>* template is part of the Microsoft GDPR Detailed Assessment kit and will be used during the pre-engagement meeting.

**Deliverables**

The deliverables of the pre-engagement meeting are:

* An agreed starting date and agreed engagement time lines;
* A list of customer responders (Name, title, contact details).

These deliverables will serve as input to the presentation that will be used during the on-site engagement kick-off.

**Duration**

The typical duration for the on-line pre-engagement meeting is 1-2 hours and the partner consultant preparing for the meeting will need an additional 1-4 hours preparation time depending on his experience with the material at hand.

## Determine the appropriate customer responders

Each sub-scenario in the Microsoft GDPR Detailed Assessment comes with recommended responders, who are described below in detail. Preferably recommended responders are identified with your customer during or shortly after the pre-engagement meeting.

| Recommended responder title | Responder role description |
| --- | --- |
| Chief Information Security Officer (CISO) | A leader responsible for ensuring the organization maintains appropriate information security standards. |
| Compliance | The group responsible for verifying the organization adheres to applicable laws and standards. |
| Data Center Leadership | The group responsible for determining how information is stored, organized, and processed in data centers. |
| Data Protection Officer (DPO) | A potentially required oversight position for organizations, depending on how they use personal data and on the amount of personal data maintained. DPOs are responsible for helping ensure their organizations comply with data protection requirements. |
| Human Resource (HR) | Human Resources is responsible for employee/contractor hiring, benefits, and termination. |
| IT Leadership | A group of leaders responsible for determining the strategic IT vision for the organization, including implementation. This group often includes a Chief Information Officer (CIO). |
| Legal | The group responsible for interpreting and determining how the organization will adopt applicable regulations. It may also help establish policies and procedures to help ensure compliance. |
| Marketing/Digital | The group responsible for analyzing behavioral patterns and interests of an organization’s customers, as well as enticing those customers to purchase products or services. |
| Operations | The group responsible for helping the organization produce better products and services more efficiently. |
| Processor | A person or organization that processes personal data on behalf of another person or organization. |
| Risk Management Office | The group responsible for identifying key risks to highly valued assets within an organization and formulating plans to mitigate or eliminate those risks. |
| Third-Party Processors | A person or organization that processes personal data on behalf of an organization’s principal processing partner/contractor. |

# Step 2 – Assessment

The activities for step 2 are typically conducted on-site at customer premises. During this step the partner consultant will help the customer answer the assessment questions and more important, has the opportunity to provide added value to the customer by sharing insights and background about the journey towards GDPR compliance.

Additionally, the partner can enable Microsoft Compliance Manager and assess the current compliance posture of the customers Microsoft Cloud tenant against data protection regulatory requirements.

## Engagement kick-off meeting.

At the beginning of the day the customer and partner team will gather for a short kickoff meeting. During this meeting, the new team members (if any) will be introduced and the team will be briefed on the upcoming activities and the meeting schedules and location(s) will be confirmed.

**Objectives**

There are two objectives for the kick-off meeting:

* Introduce the new team members (if any) and align expectations;
* Confirm engagement logistics such as interview schedules, rooms & locations, etc.

**Resources**

* *<02 - Microsoft GDPR Detailed Assessment - Kickoff Presentation.pptx>*

**Preparation**

The partner consultant that will be leading the kick-off meeting should:

* Customize and update the <*02 - Microsoft GDPR Detailed Assessment - Kickoff Presentation.pptx>* with customer specific details and the information obtained from the pre-engagement meeting;
* Verify logistics such as meeting room availability and resource availability.

**Deliverables**

There are no deliverables for the kick-off meeting.

**Duration**

The typical duration for the kick-off meeting is 1 to 1½ hrs.

## GDPR Detailed Assessment

Together with the previously identified customer responders the partner consultant(s) will go through each and every question from the Microsoft GDPR Detailed Assessment tool.

**Objectives**

The partner uses the tool’s questions to help the customer assess the maturity of its people, processes, and technology relevant to the GDPR. The answers provided by the customer will be logged into the tool together with relevant remarks and or observations.

For customers considering migrating to the Microsoft cloud or customers that are already using the Microsoft cloud services such as Office 365, the GDPR Detailed Assessment offers additional integration with Microsoft Compliance manager. Compliance manager can be used during the workshop to assess the organizations compliance posture against data protection regulatory requirements. Compliance Manager will provide actionable real-time insights that will help the organization on their journey towards compliance.

**Resources**

* *<03 - Microsoft GDPR Detailed Assessment - Input.xlsx>*
* Compliance Manager <https://aka.ms/compliancemanager>

**Preparation**

To prepare for the detailed assessment the partner consultant should:

* Become familiar with the assessment tool. The upcoming paragraphs will provide detailed guidance and can be used for reference;
* Ensure understanding of all questions from all categories and their relation to the articles of the GDPR.
* Understand Microsoft Compliance Manager (only if applicable)

**Deliverables**

The deliverable for this activity are:

* The completed questionnaire.
* A Compliance Manager assessment of the current compliance posture of the customers Microsoft Cloud tenant against data protection regulatory requirements.

**Duration**

To prepare for the assessment a consultant will typically need 8-12 hours to become familiar with the questions in the tool. This is a one-time activity and is not required for consecutive deliveries of the assessment.

The time needed to answer the assessment questions in the tool heavily depends on the number of customer responders involved and the level of insight they have into people, processes and technology for their organization. The typical duration for the assessment is 6-12 hours for a small to medium sized organization that is well organized and prepared to respond to the assessment.

If Compliance Manager is used to assess the compliance posture of the Office 365 tenant, additional time will need to be added to the overall effort. At the time of this writing, there are 61 customer controls for Office 365 related to the GDPR. If the consultant devotes 15 minutes to review and briefly discuss each control, approximately 16 additional hours should be reserved for this portion of the engagement. Implementation of the customer controls may take considerably more time and should be scoped separately.

### Walkthrough of how to use the Microsoft GDPR Detailed Assessment

The following instructions are intended to help you use the Microsoft GDPR Detailed Assessment.

#### How to answer questions

Each question is designed to have a *“Yes”*, *“No”* or *“N/A”* (not applicable) answer, as selected from the drop-down menu in the “Answer” column cell. If a question has an *and* condition, select *“Yes”* only if each component of the question can be answered *“Yes”.*

***“Knockout”* questions:**

Each sub-scenario has a principal question denoted by an ID ending in .0 (like D1.0) that assesses *foundational* capability for the sub-scenario. If the customer feels close to answering *“Yes”* and is uncertain, err toward answering *“Yes”*.

For example, certain questions ask whether the customer has “some” instances of a foundational capability. If the customer *has* a capability in place that can be improved, lean toward *“Yes”*.

**NOTE: If a customer answers a sub-scenario’s knockout question with *“No”*, answer the rest of the questions for that sub-scenario also with *“No”*.**

**Question Weighting:**

*“Knockout”* questions are weighted more heavily, as they establish a foundational capability. Optimizing stage questions are weighted the least. The rest of the questions are weighted based off criticality of capability to address the sub-scenario. The total of all questions that are answered *“Yes”* determines the stage (starting, progressing, or optimizing) for each sub-scenario, theme, and overall output. Answering *“Yes”* to all questions of a maturity stage moves the customer to the next stage. Question weighting prioritizes customer recommendations and drives the overall maturity scores shown in Power BI.

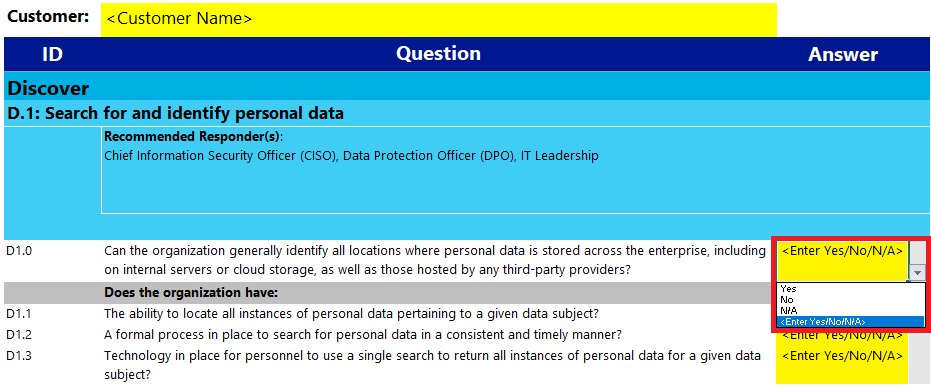
**Assessment Mechanics:**

The mechanics which determine the weighting for each question and the associated maturity stage are completed within a hidden tab within the Microsoft GDPR Detailed Assessment Excel workbook. This tab is used to calculate each weight and provide the associated recommendations for all questions answered *“No”.* Modifying this tab is not recommended and can result in unintended consequences in the Power BI output.

**Choosing an answer from the drop-down menu:**

To select an answer, click on the answer cell next to the applicable question, then click the drop-down arrow button. Finally, select the desired answer (*“Yes”*, *“No”*, or *“N/A”*).

Selecting a desired answer for a question.



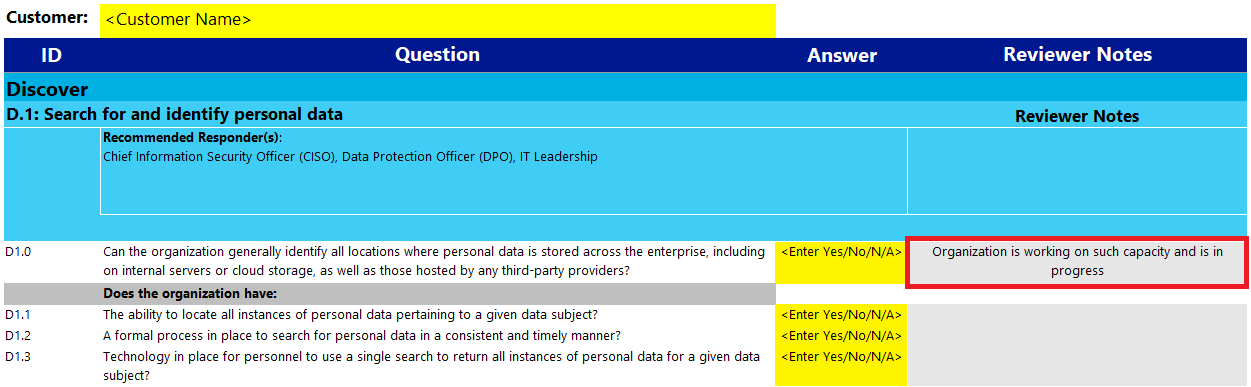
**Consequences of leaving a question unanswered or choosing *“N/A”*:**

If a question is left unanswered or answered as *“N/A”*, it will be excluded from calculations tallying a customer’s overall and specific sub-scenario maturity score.

**Entering *“Reviewer Notes”*:**

For some questions, a responder or the partner interviewing the customer might want to add contextual or follow-up details. These can be entered in the *“Reviewer Notes”* text box.

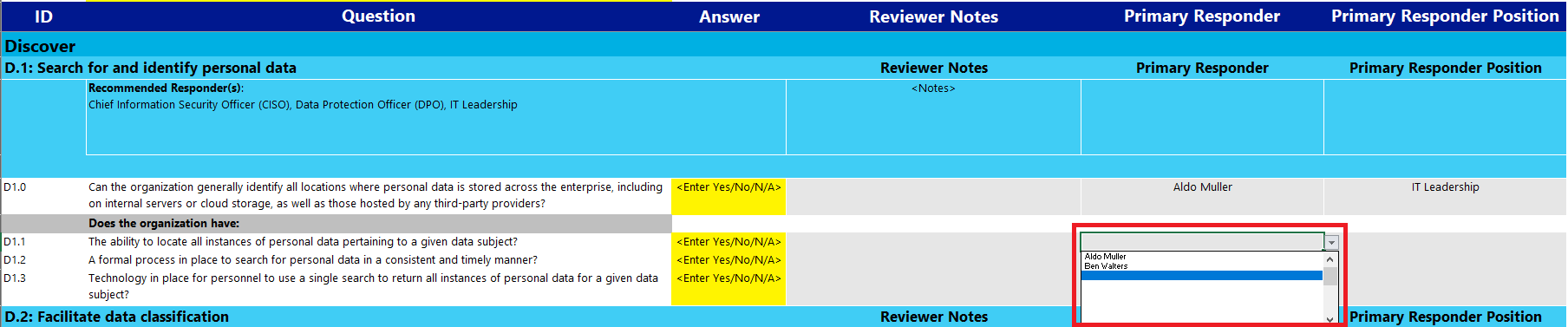
Users can add explanatory or follow-up text for a question in the “Reviewer Notes” field.



**Primary Responders:**

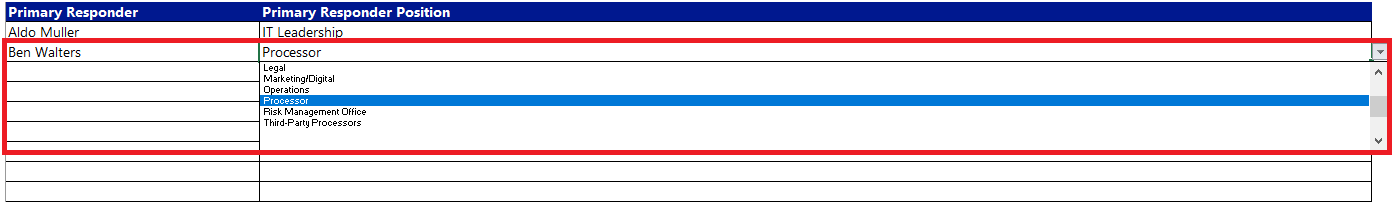
To document the name and title of the principal person answering questions for a sub-scenario, fill in the *“Primary Responder”* and *“Primary Responder Position”* fields. If the name of the *“Primary Responder”* is selected from the drop down list, the *“Primary Responder Position”* is automatically populated. Primary Responder names and positions can be added and updated on the “*Responders worksheet”*.

Fill in the “Primary Responder” and “Primary Responder Position” fields to show who primarily answered sub-scenario questions. The names can be typed in directly or selected from a pre-populated list, if selected from the list, the “Primary Responder Position” will be automatically filled.

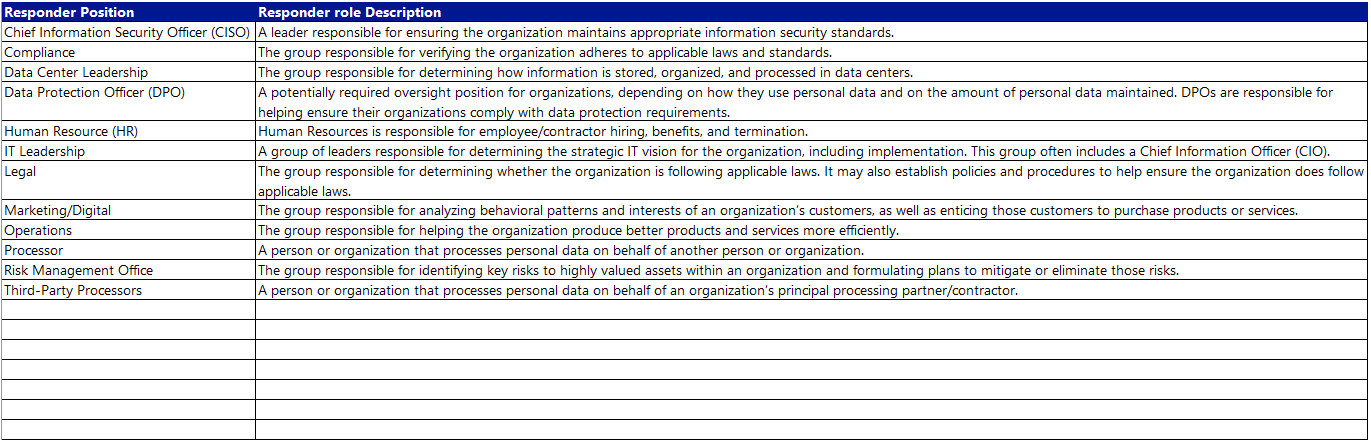


Before starting the assessment, you are advised to populate the list of Primary Responders with the names and positions of the attendees in the workshop. This will speed up data entry while in the process of answering the assessment questions.

Add the workshop attendee names of the “Primary Responder” column and select a position from the list. The Primary Responder Position can be typed in directly or selected from a pre-populated list.



If needed add additional positions to the table to facilitate easy selection from the dropdown list.

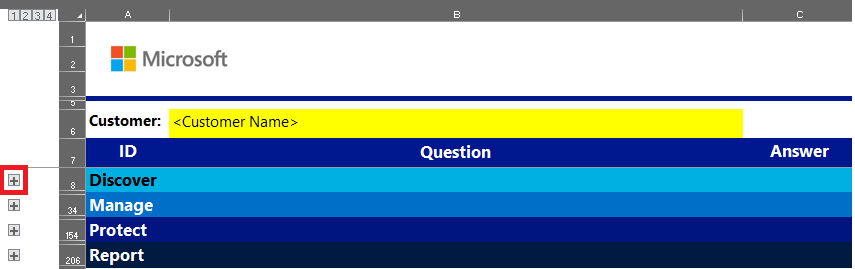


#### How to access questions

**Expanding themes:**

To view and answer questions, first click the group button next to the theme (Discover, Manage, Protect and Report) you want to see. For example, to see questions in the Discover theme, click the group *“+”* button in the cell parallel with Discover.

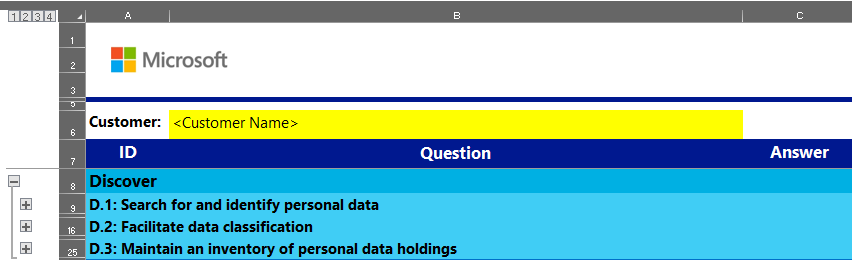
To expand a theme, click the relevant group + button.



**Expanded theme appearance:**

This will expand the theme into its component sub-scenarios:

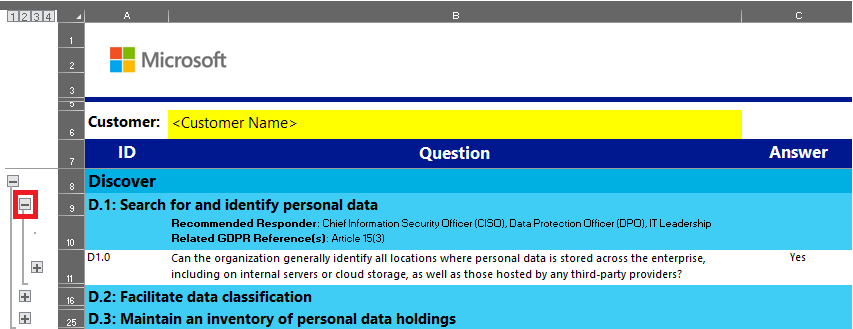
How a theme appears with its sub-scenarios expanded.



**Expanding a sub-scenario:**

Next, click the group *“+”* button adjacent to the sub-scenario you want to expand. This will display the sub-scenario’s 1) Recommended Responder, 2) Related GDPR Reference(s), and 3) principal or *“knockout question*” aligned with it:

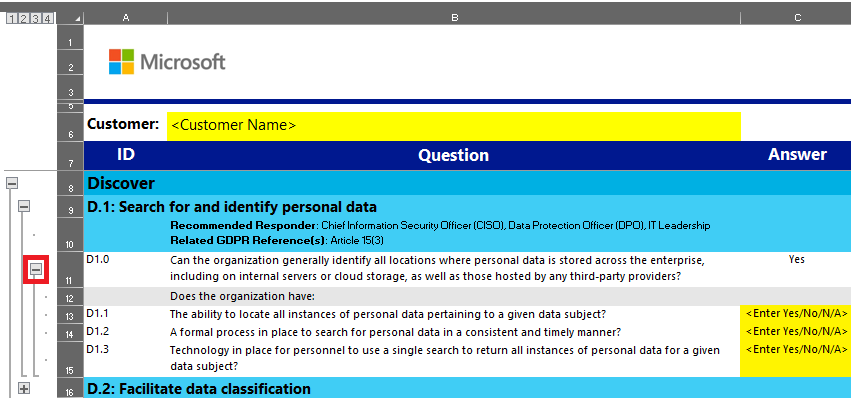
How a sub-scenario appears with its key components expanded.



**Expanding all questions in a sub-scenario:**

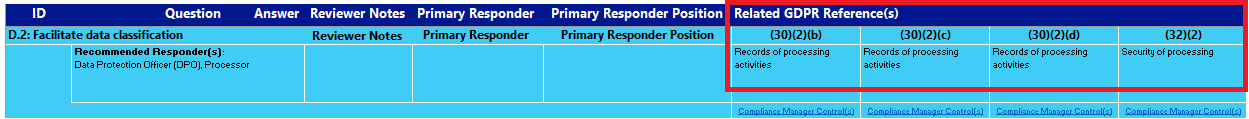
Finally, to display all questions associated with a sub-scenario, click the group *“+”* button adjacent to the principal or *“knockout question”* (it will have an ID numbered .0).

How a sub-scenario appears with all its questions expanded.



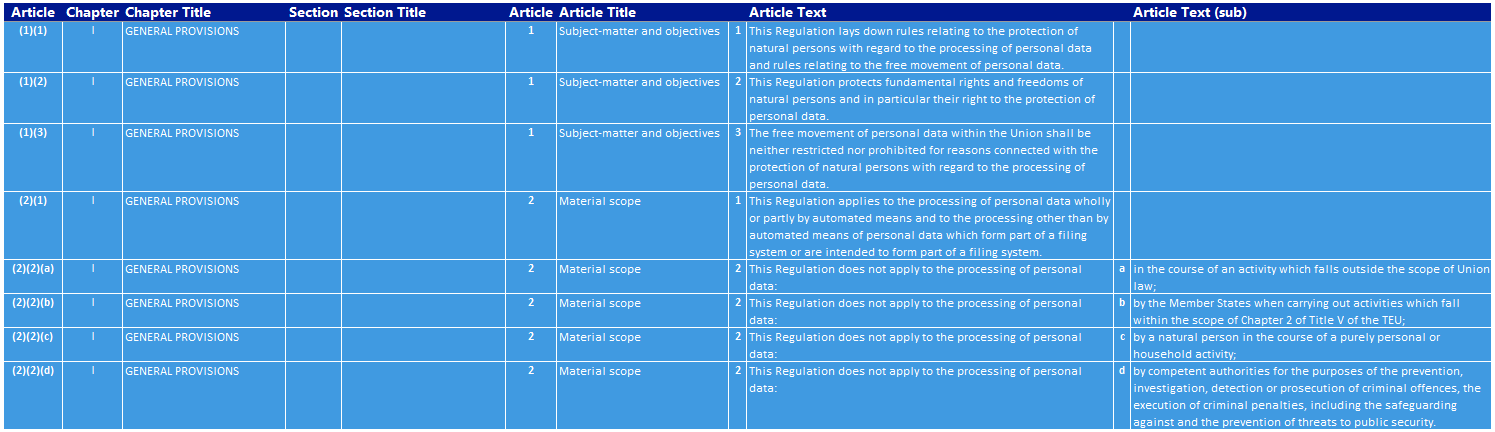
#### GDPR article references

To review the statutory references of the text used to develop the content for a sub-scenario, look for the “Related GDPR Reference(s)” to the right of each sub-scenario.



For your reference, a copy of the GDPR articles can be found on the worksheet “GDPR Articles”, please refer to the official website[[2]](#footnote-3) for the latest and most up to date information.

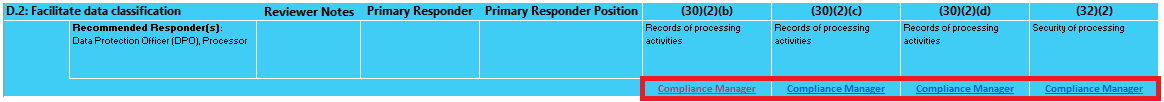
Overview of all GDPR articles, to be used for refence only.



### Compliance manager integration

The GDPR Detailed assessment integrates with Microsoft Compliance Manager. Compliance manager offers actionable insights into both the customer’s and Microsoft’s responsibility to meet compliance standards.

For every statutory reference a link is provided that will open the relevant customer and Microsoft controls when clicked. The controls are assessed in real-time by Compliance Manager and relevant details about required actions, product(s) to implement, settings to configure and test plans to execute are provided.

*Direct links to Compliance Manager controls for every related GDPR Reference.  
*

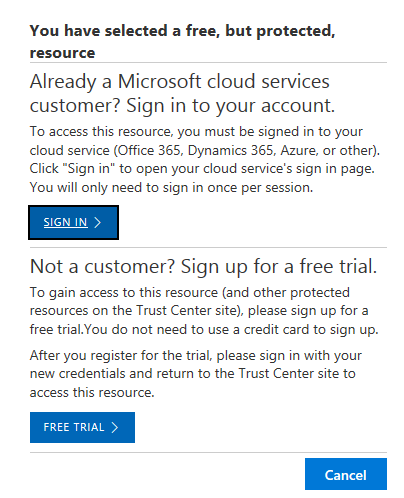
Compliance Manager requires a Microsoft cloud tenant, such as Office 365, and corresponding Azure Active Directory login credentials. Preferably the customer’s production tenant is used because the Compliance Manager assessment will then provide real time insight into the compliance posture of the Microsoft cloud production environment the customer is using. If a customer production tenant is not available, it is possible to use any other Microsoft cloud tenant. In order of preference, it is advised to use one of the following tenants:

1. **Customer Production Tenant**, customer needs to provide administrative credentials for access and configuration of Compliance Manager;
2. **Trial tenant for dedicated use by the customer**. A trial tenant can be setup free-of-charge from the Office 365 product page or via the Compliance Manager sign-in page;
3. **Demo tenant provided by the partner**.The partner can setup a demo tenant on the Microsoft Demos platform (<http://demos.microsoft.com/>) and provide access credentials to the customer.

The first time a link to Compliance Manager is clicked from within the GDPR Detailed Assessment Excel workbook, the user is presented with a sign-in prompt. The sign-in prompt has two options:

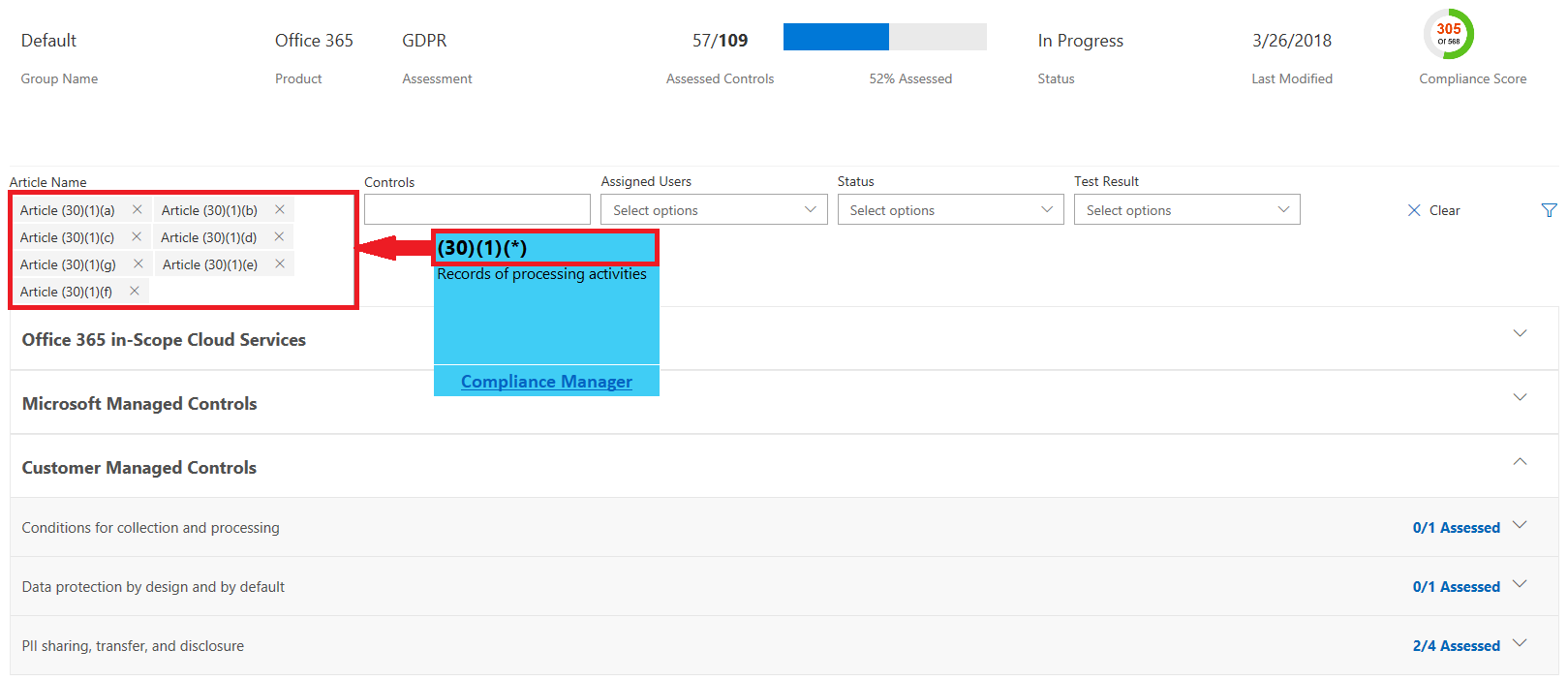
* **Provide credentials for an existing tenant**, this can be a customer production tenant or an existing customer / partner demo tenant;
* **Sign-up for a trial tenant**, if a tenant is not available, selecting this option will allow the user to create a demo tenant with full functionality including Compliance Manager. This demo tenant can, if so desired, be upgraded to a full production tenant.

*Sign in with the appropriate tenant credentials or sign up for a free trial tenant..*



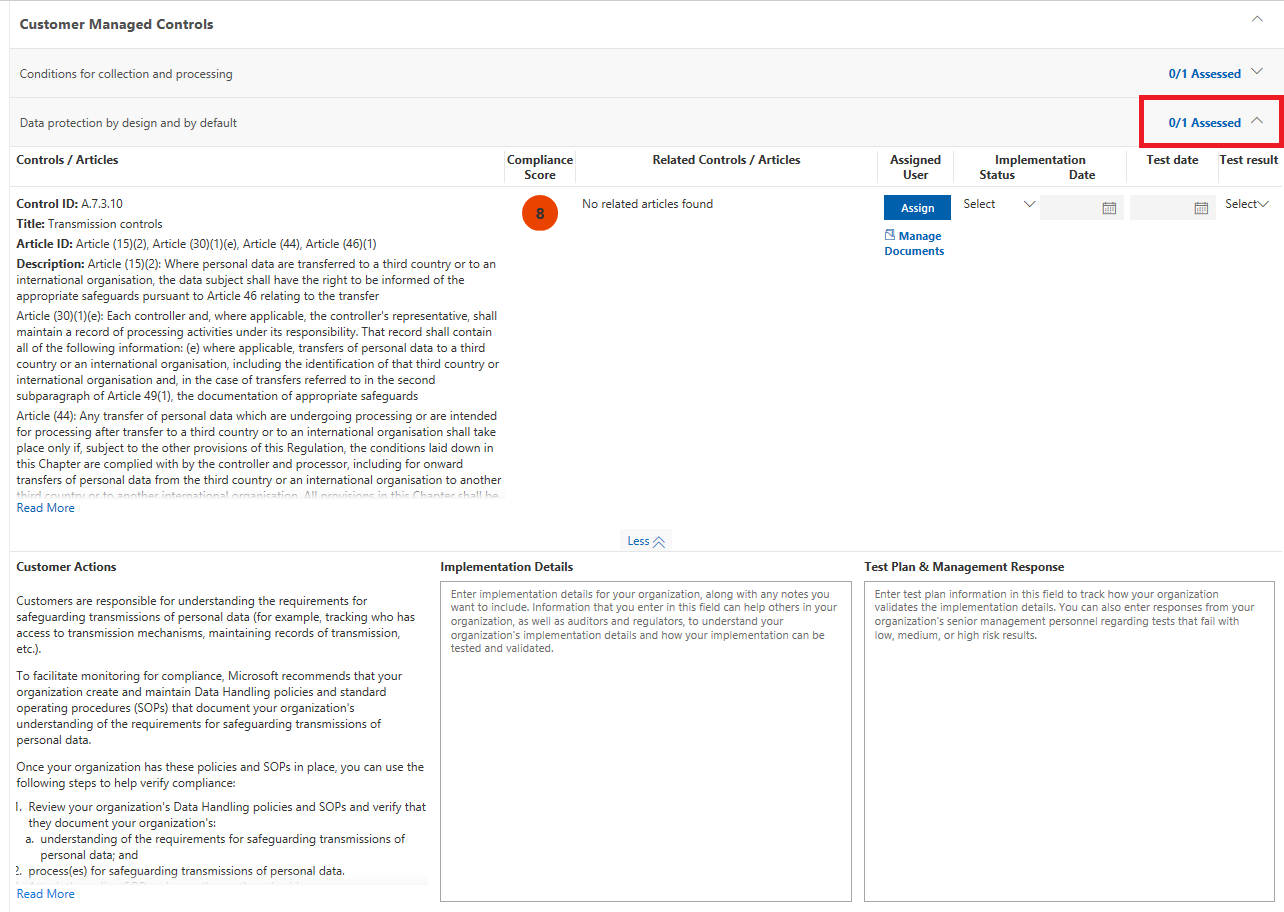
Once the sign-in process is completed, compliance manager will show a detailed overview of all relevant Microsoft and Customer managed controls. The overview is filtered to show only controls that are relevant to the referenced GDPR article(s).

*Clicking the link to Compliance Manager will open the Compliance Manager dashboard with a filtered view of controls relevant to the selected sub-scenario.*



By expanding the control sections below the Microsoft or Customer Managed Controls, additional control details and links to implementation guidance is provided.

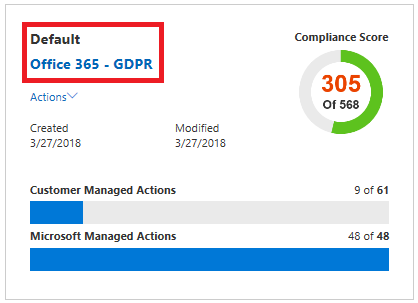
*Detailed view of filtered controls with implementation guidance and background information.*



**Important pre-requisites**

Compliance manager integration is relying on the *Default Office 365 - GDPR* *assessment* that is part of the initial enablement of Compliance Manager.

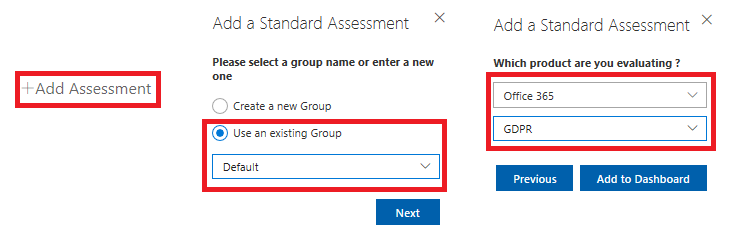
*Verify that the Office 365 GDPR assessment is available in the Default group.*



If the *Default Office 365 - GDPR* *assessment* is not available from the dashboard anymore, it needs to be re-created to enable Compliance Manager integration. Follow the steps outlined below to restore the assessment:

1. From the Compliance Manager Dashboard click **+Add Assessment**
2. Select **Use an existing Group** and select **Default** from the dropdown list.
3. Click **Next**
4. Select **Office 365** from the *product* dropdown list
5. Select **GDPR** from the *certification* dropdown list
6. Click **Add to Dashboard**

*If the assessment is archived and no longer available on the dashboard. Recreate the assessment.*



**Compliance Manager Resources**

* Compliance Manager <https://aka.ms/compliancemanager>
* [Compliance Manager Frequently Asked Questions](https://servicetrust.officeppe.com/ViewPage/FAQ)
* [Use Compliance Manager to help meet data protection and regulatory requirements when using Microsoft cloud services](https://go.microsoft.com/fwlink/?linkid=862109)
* [Service Trust Portal and Compliance Manager white paper](https://resources.office.com/ww-landing-m365e-gdpr-compliance-manager-whitepaper.html?lcid=en-us)
* [GDPR whitepaper featuring Compliance Manager](https://info.microsoft.com/ww-landing-GDPR-M365-Whitepaper-WhitePaper.html)
* [GDPR e-Book featuring Compliance Manager](https://info.microsoft.com/ww-landing-GDPR-and-Microsoft-365-EBook-eBook.html)

## Outcome Analysis & Write-Up

After the customer has completed the questionnaire in the input worksheet, the results will be analyzed and a close out presentation will be created.

Using Microsoft Power BI a summary view and list of recommendations will be automatically generated. The automatically generated views and recommendations will be included in the close-out presentation together with a list of next steps and recommended actions.

The following paragraphs will provide detailed instructions on how to install and use Power BI to generate the various views and how to update the *<Microsoft GDPR Detailed Assessment - Close-Out Presentation.pptx>* template with the output of the Power BI analysis.

**Objectives**

The partner consultant will update the <*Microsoft GDPR Detailed Assessment - Close-Out Presentation.pptx>* template with the outcome of the GDPR Detailed Assessment tool and provide a list of meaningful and actionable next steps that will help the customer defining a roadmap toward GDPR compliancy.

**Resources**

* *<03 - Microsoft GDPR Detailed Assessment – Input.xlsx>*
* *<03 - Microsoft GDPR Detailed Assessment - Results.pbix>*
* *<04 - Microsoft GDPR Detailed Assessment - Close-Out Presentation.pptx>*

**Preparation**

The partner consultant responsible for creating the Close Out presentation should:

* Obtain in deep expertise about the products and solutions from the Microsoft Office 365 product suite that can help customers meet their GDPR requirements;
* Familiarize with the content of the <*04 - Microsoft GDPR Detailed Assessment - Close-Out Presentation.pptx>* template.

**Deliverables**

The main deliverable for this activity is a fully customized and updated Close-Out Presentation that will be presented at the close out meeting.

**Duration**

The typical duration for creating the close out presentation is 2 to 4 hrs.

### How to use Power BI with the Microsoft GDPR Detailed Assessment

Power BI is the principal visualization solution for the Microsoft GDPR Detailed Assessment. The Power BI file that comes with the Microsoft GDPR Detailed Assessment file is an out-of-the-box solution that will automatically generate charts and insights for your customers. The following are instructions for how to use Power BI with the Microsoft GDPR Detailed Assessment, as well as an overview of the Power BI content.

#### Setting up the Power BI file

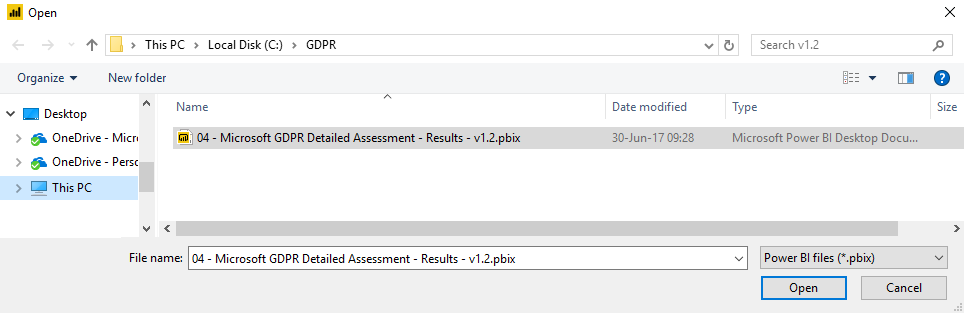
**Download and install Power BI Desktop (if not already installed):**

You will need to have Power BI Desktop installed on your local machine. If you need a copy, you may install the software, free of charge, by downloading it from [this site](https://powerbi.microsoft.com/en-us/desktop/) ([https://Power BI.microsoft.com/en-us/desktop/](https://powerbi.microsoft.com/en-us/desktop/)) and installing it as you would any other application.

**Open your Power BI file:**

Once your Detailed Assessment file is complete and ready for use with Power BI, open Power BI Desktop. Now, open your Power BI file <*03 - Microsoft GDPR Detailed Assessment – Results.pbix>*. **File > Open >** *select and open the Power BI file from where you saved/downloaded it.* (You can also open your Power BI file directly, instead of opening the app first.)

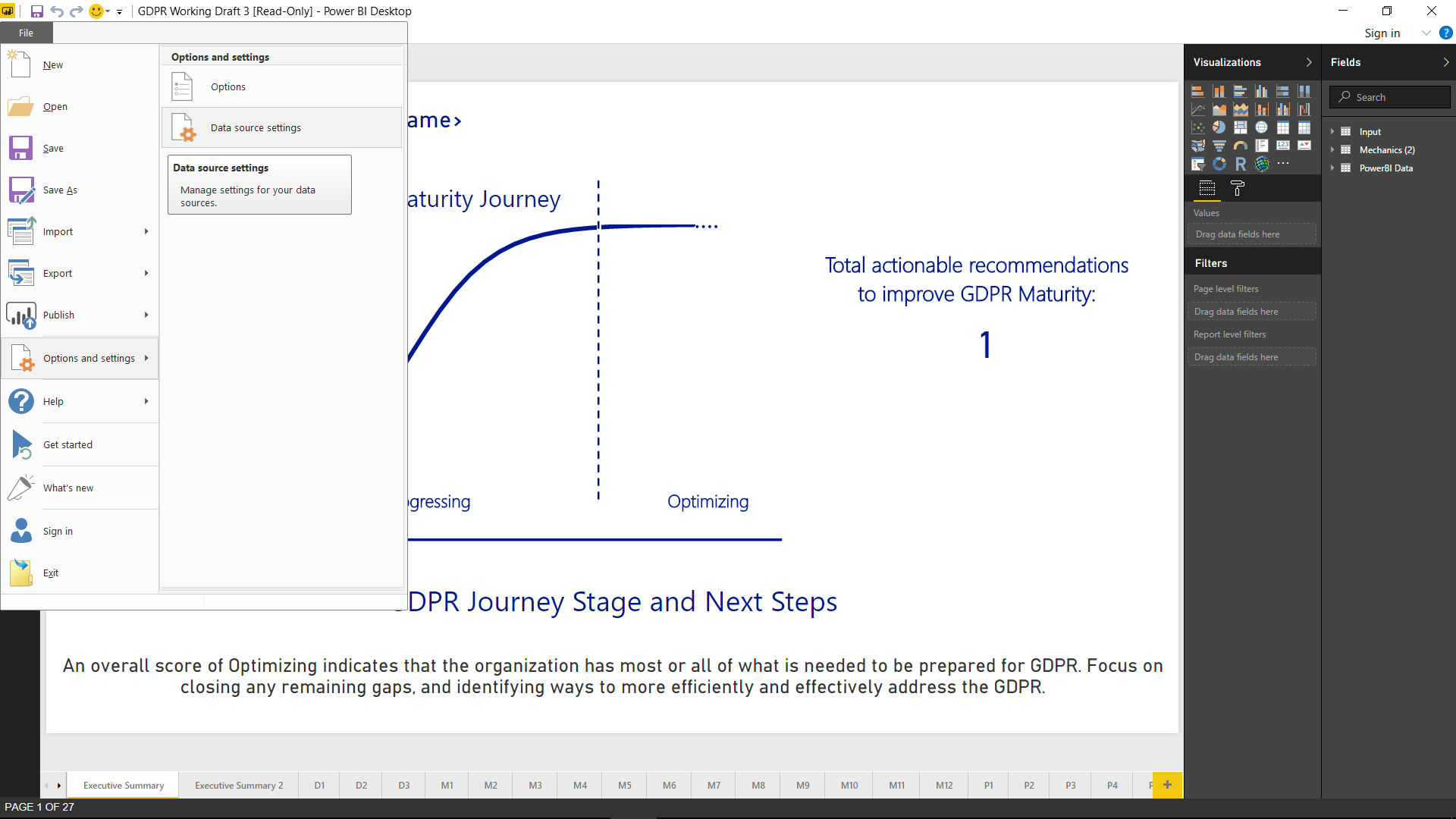
In Power BI Desktop, select the Power BI file by clicking File > Open > [the Power BI file].



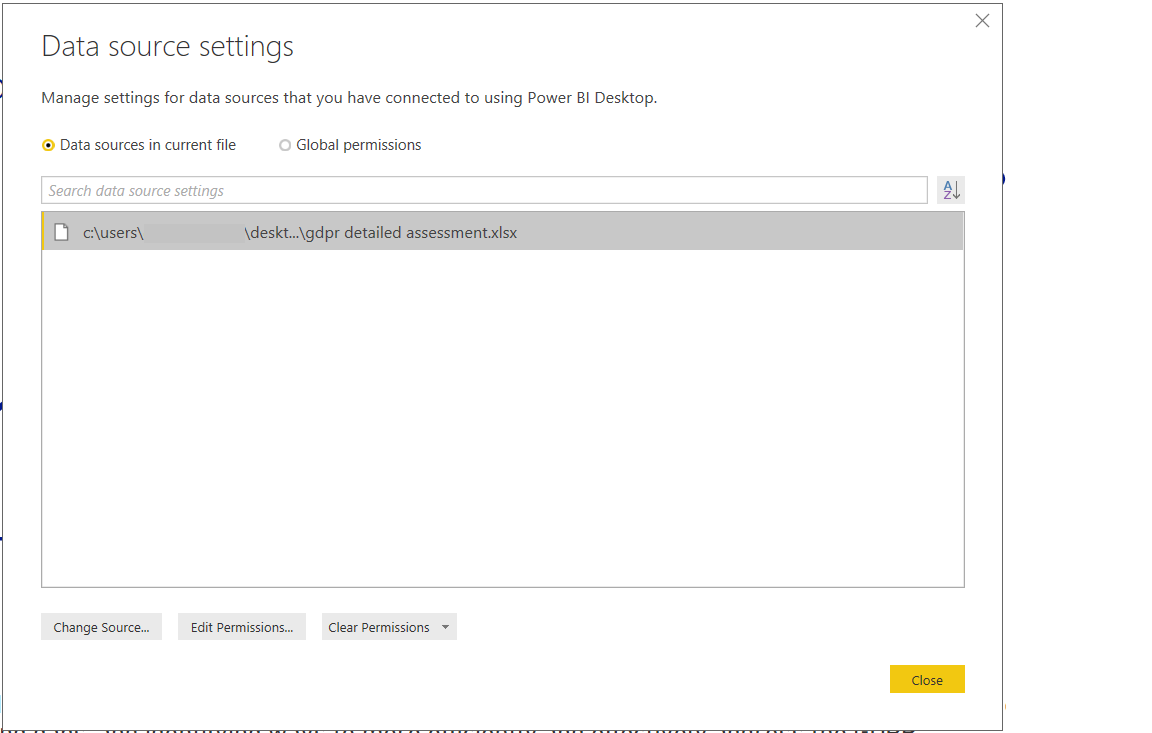
**Load Detailed Assessment data into your Power BI file:**

Next, load into Power BI the data from your Detailed Assessment by clicking **File > Options and settings > Data source settings > Change Source… >** *browse to and open the <Microsoft GDPR Detailed Assessment – Input.xlsx> file (then click Ok and then Close)* **> Apply changes**

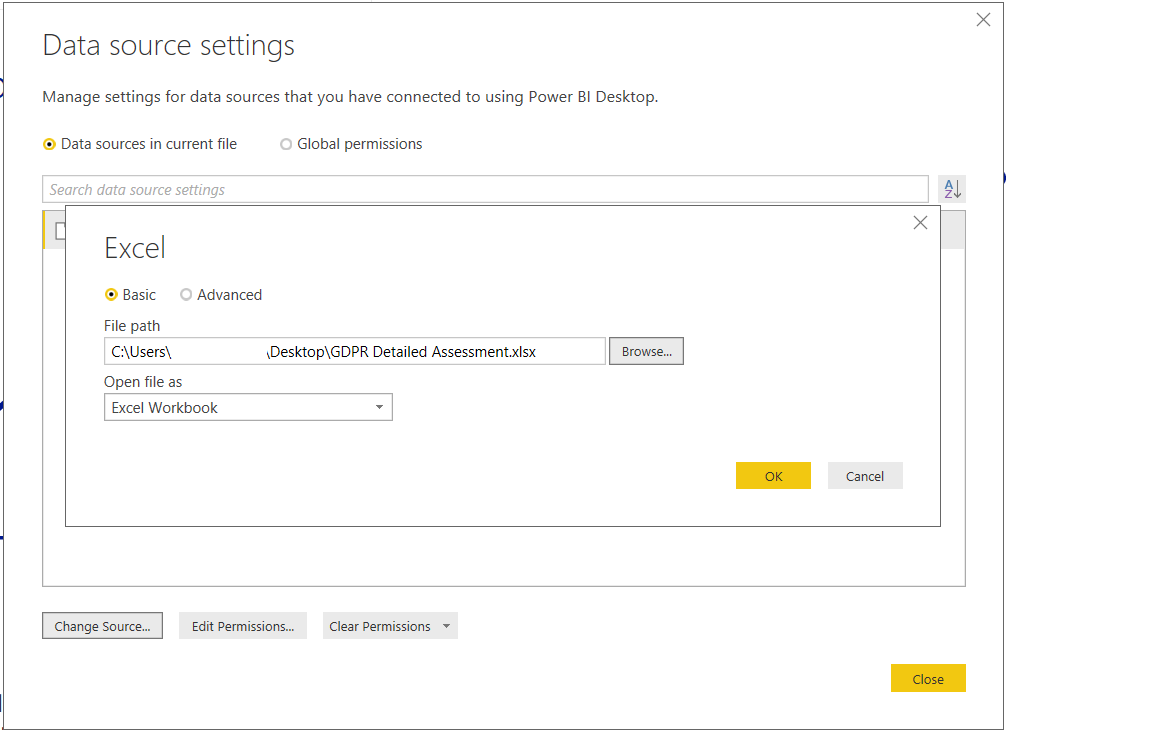
Begin selecting your Microsoft GDPR Detailed Assessment file by clicking File > Options and settings > Data sources settings.



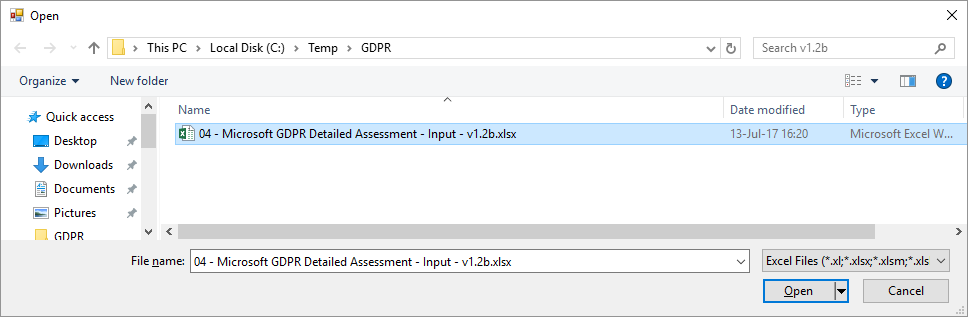
Click Change Source…



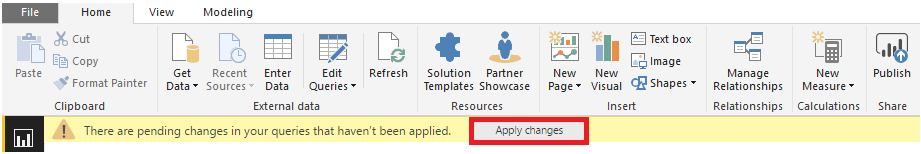
Click Browse...



Click the <Microsoft GDPR Detailed Assessment – Input> file and click Open (then click OK and then Close).



Finally, click Apply changes.



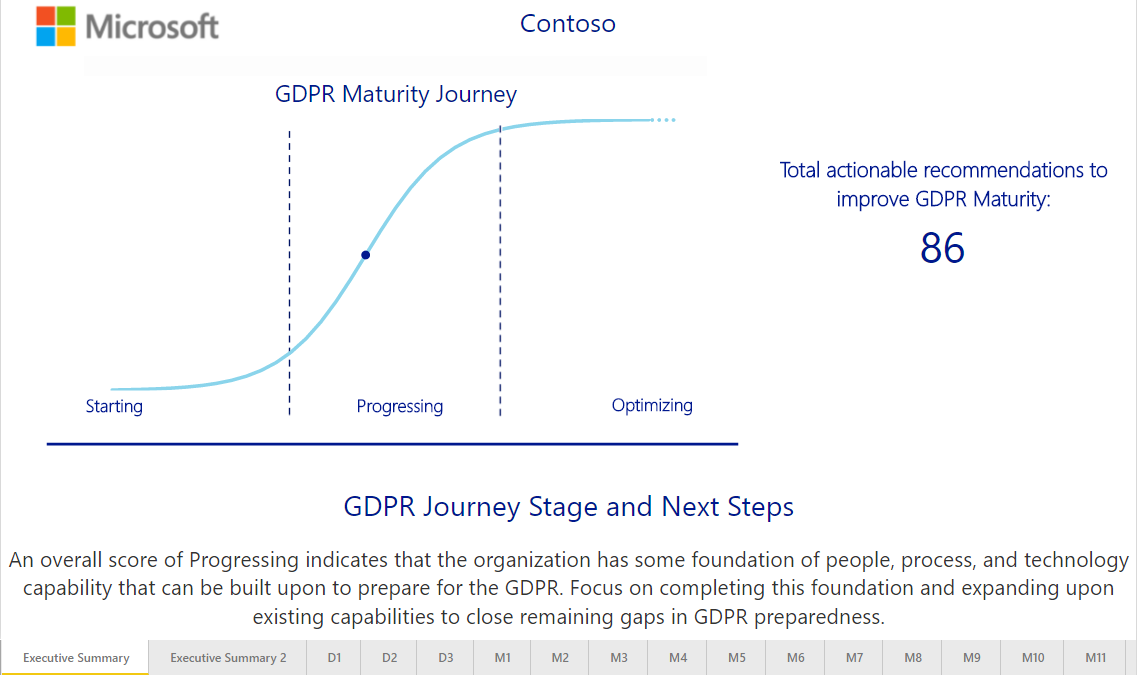
Your Power BI file will now be updated with data from your Detailed Assessment file.

#### Power BI file content overview

**Executive Summary:**

This tab displays 1) the customer’s GDPR maturity in one of three stages, 2) the total number of possible recommendations to follow, and 3) what the customer’s overall maturity stage means.

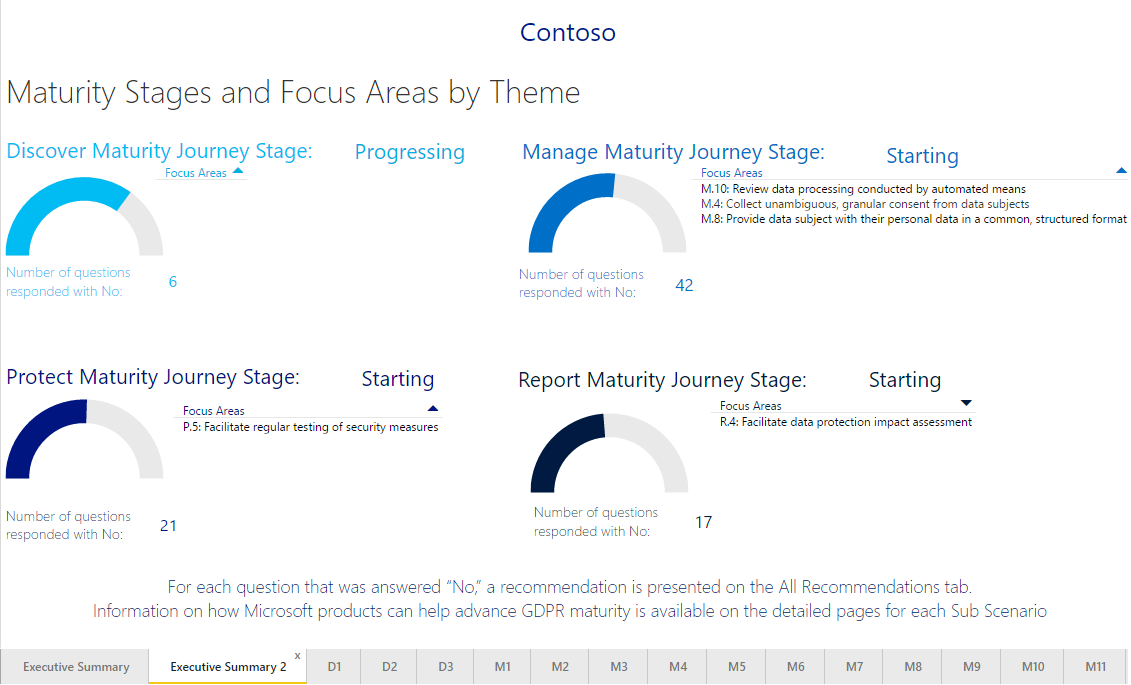
Executive Summary tab.



**Executive Summary 2:**

This tab displays the customer’s GDPR maturity and number of recommendations to follow for each DMPR theme. It also lists the sub-scenarios with foundational capabilities to focus on (“Focus Areas”) and a description of the customer’s maturity stage for each theme.

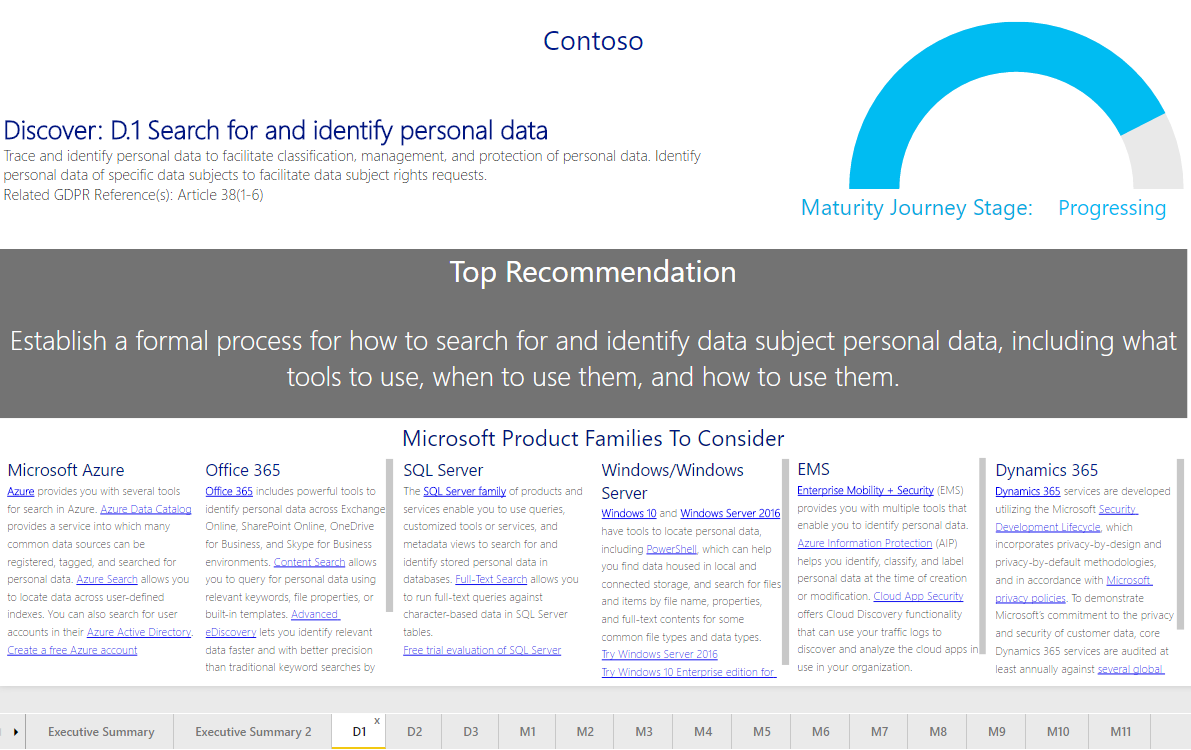
Executive Summary 2



**Sub-scenario tabs:**

These tabs display the customer’s GDPR maturity for a specific sub-scenario of a theme. They also include a description and related GDPR reference(s), as well as the highest priority recommendation and recommended Microsoft products that can help improve maturity for the sub-scenario.

Example of a sub-scenario tab.

****

**All Recommendations tab:**

This tab includes the full list of recommendations for the customer, grouped by sub-scenario and GDPR maturity stage.

All Recommendations tab.



### Update the Close-Out presentation template

The Close Out presentation template <*04 - Microsoft GDPR Detailed Assessment - Close-Out Presentation.pptx>* provided with the Microsoft GDPR Detailed Assessment includes placeholder slides that should be updates with the corresponding BI Views:

* Match the slide title to the corresponding Power BI view
* Open the snipping tool, select “New”, and trace the area of the picture you want to take. Click “Copy” in the snipping tool ribbon
* Open the PowerPoint slide that corresponds to the screenshot taken, and select “Paste”
* Resize the image to take up the entire slide
* Repeat for additional slides

# Step 3 – Close Out presentation

The final activity for the Microsoft GDPR Detailed Assessment is to present the findings from the assessment to the customer and define next steps and if possible a roadmap towards GDPR compliance.

The audience for the closing presentation is not necessarily the same audience that participated in step 2 of the assessment. Consider additionally inviting senior decision makers from the organization that can help defining priorities and initiate next steps.

**Objectives**

The objectives for the close out presentation are to:

* Inform the customer on the outcome the GDPR Detailed Assessment;
* Recommend technologies and services that the customer can leverage towards GDPR compliancy;
* Work with the customer to define next steps and a roadmap with actionable items plotted on a timeline.

**Resources**

* *<04 - Microsoft GDPR Detailed Assessment - Close-Out Presentation.pptx>*

**Preparation**

To prepare for the close out presentation the partner consultant should work with the customer to select the right audience, allocate a conference room and send the invites.

**Deliverables**

The deliverables for the close out presentation are:

* A list of next steps and a roadmap with actionable items and timelines that will assist the customer towards GDPR compliancy

**Duration**

The expected duration for the close out presentation is 1-2 hrs.

# Appendix – Microsoft GDPR Detailed Assessment Toolkit content

The table below lists the files part of the Microsoft GDPR Detailed Assessment Toolkit.

|  |  |
| --- | --- |
| File name | Type |
| 00 - Microsoft GDPR Detailed Assessment - Delivery Guide   (This document) | DOCX Microsoft Word |
| 01 - Microsoft GDPR Detailed Assessment – Pre-Engagement Presentation | PPTX Microsoft PowerPoint |
| 02 - Microsoft GDPR Detailed Assessment - Kickoff Presentation | PPTX Microsoft PowerPoint |
| 03 - Microsoft GDPR Detailed Assessment – Input | XLSX Microsoft Excel |
| 03 - Microsoft GDPR Detailed Assessment – Results | PBIX Microsoft Power BI |
| 04 - Microsoft GDPR Detailed Assessment - Close-Out Presentation | PPTX Microsoft PowerPoint |
| 10 - Microsoft GDPR Detailed Assessment - How to deliver | PPTX Microsoft PowerPoint |
| 20 - Microsoft GDPR Detailed Assessment - Statement of Work template | DOCX Microsoft Word |
| 30 - Microsoft GDPR Detailed Assessment – Datasheet | DOCX Microsoft Word |

# We look forward to your feedback!

Thank you for your continued trust and partnership. We would love to hear about your successes, challenges, and overall feedback from using the tool. Please join the conversation and share your feedback on the Yammer Community Site: <https://aka.ms/gdprcommunity>.

1. From: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN> [↑](#footnote-ref-2)
2. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5419_2016_INIT&from=EN> [↑](#footnote-ref-3)