

Microsoft General Data Protection Regulation - Detailed Assessment

Statement of Work v3 – March 2018

**TEMPLATE**

**This document is intended to be used as a starting point (template) to help you create a Statement of Work for the GDPR Detailed Assessment.**

**This text box should be removed upon completion.**

**(Select the text box and click delete)**

microsoft.com/gdpr

Table of Contents

[Intended usage 3](#_Toc510103885)

[Disclaimer 3](#_Toc510103886)

[Introduction 4](#_Toc510103887)

[Version History 4](#_Toc510103888)

[Engagement Objectives and Scope 5](#_Toc510103889)

[Objectives 5](#_Toc510103890)

[In scope 5](#_Toc510103891)

[Out of scope 5](#_Toc510103892)

[Project Approach 6](#_Toc510103893)

[Timeline 6](#_Toc510103894)

[Deliverables and work products 7](#_Toc510103895)

[Customer Resource Requirements 8](#_Toc510103896)

[Customer Responsibilities 9](#_Toc510103897)

# 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

# Introduction

The General Data Protection Regulation (GDPR) represents a paradigm shift in global privacy requirements governing how organizations manage and protect personal data while respecting individual choice—no matter where the data is sent, processed, or stored. It introduces new requirements on privacy, security and compliance for organizations that offer goods and services to European Union (EU) residents.

This Statement of Work describes the GDPR Detailed Assessment, a three-step process that Microsoft partners will engage in with their customers to assess their overall GDPR maturity.

The GDPR Detailed Assessment tool that is used during the assessment is built on an Excel workbook (the questionnaire) with over 160 questions that are related to various GDPR scenario’s. The questions are organized around four themes: Discover, Manage, Protect, and Report (DMPR) and describe scenario’s that are impacted by the GDPR and are recognizable by the customer. After completion, the results will be analyzed, and a detailed report will be presented.

The report provides high-level visualizations of the end-customers’ GDPR maturity overall and within each theme. It also provides recommendations and a roadmap with actionable activities to help customers improve their GDPR maturity within each theme.

## Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Author | Changes | Date |
| 0.2 | François van Hemert | Initial Release | February 2018 |
| 3.0 | François van Hemert | Published version | March 2018 |

# Engagement Objectives and Scope

## Objectives

The objectives for the GDPR Detailed Assessment are define as:

* **Understand GDPR compliance objectives**Gain a common understanding of compliance objectives and GDPR requirements
* **Assess GDPR maturity level**Assess the organization’s preparedness to execute on Discover, Manage, Protect, & Report activities
* **Create a GDPR compliance roadmap**Provide a prioritized and actionable list of next steps and roadmap, ready for legal/advisory review

## In scope

The following activities are considered to be in scope for this engagement:

* **Preparation for onsite workshop**
* **Onsite delivery of the assessment workshop**
* **Analysis and write-up**
* **Onsite presentation of the findings and recommendations**

## Out of scope

Any area that is not explicitly listed in the “in-scope” section as “within scope” is out of scope for this engagement. The areas that are out of scope for this engagement include, but are not limited to, the following:

* **Technical designs or product implementations**The activities for the GDPR Detailed Assessment do not include the creation of design documents of any kind or the implementation of products or enablement of services.
* **Proof of concepts or labs  
  The design, installation and operation of test labs and or proof of concepts are not part of the engagement.**
* **Recommendations for non-Microsoft technology**Recommendations for non-Microsoft products and or services are not part of the deliverables for this engagement

# Project Approach

The GDPR Detailed Assessment is a three-step process that Microsoft partners will engage in with their customers to assess their overall GDPR maturity.

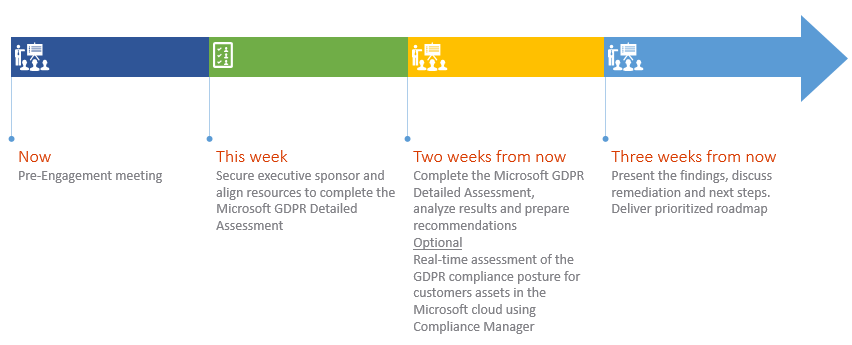
The illustration below depicts a high-level overview of the steps and their activities.



# Timeline

The overall duration for the engagement is expected to be between 3-4 weeks, while the total effort is estimated to be 12-40 hrs. depending on the complexity of the organization and the number of responders participating in the workshop(s).

The illustration below depicts the estimated time line for the GDPR Detailed Assessment.



**Compliance Manager can be used to assess the GDPR compliance posture of the customers assets in the Microsoft Cloud Tenant.**

**Refer to the delivery guide for guidance on additional effort and add relevant details to the sections of this statement of work.**

**(Select the text box and click delete)**

**Total effort**

|  |  |  |
| --- | --- | --- |
| Pre-engagement meeting | 2 | Hrs. |
| On-site assessment + write up | 8-36 | Hrs. |
| Final presentation | 2 | Hrs. |
| **Total** | **12-40** | **Hrs.** |

# Deliverables and work products

The following deliverables and work products are part of the GDPR Detailed Assessment:

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Description | Delivery Date |
| **Pre-engagement meeting** | Work product | An online meeting organized one to two weeks prior to the actual onsite activities. During this online meeting the customer will be introduced to the GDPR Detailed Assessment, discuss the upcoming activities and align expectations and timelines. For customers that have no prior exposure to the GDPR, a high-level introduction explaining the GDPR and its possible impact on the organization will be included.  A preview of the Microsoft GDPR Detailed Assessment questions will be provided to help identify the customer representatives that will assist in answering the questionnaire. | Two weeks prior to onsite workshop delivery. |
| **Confirmed schedule** | Deliverable | An agreed starting date and agreed engagement time lines | Two days after pre-engagement meeting |
| **Confirmed customer responders** | Deliverable | A list of customer responders (Name, title, contact details). | Two days after pre-engagement meeting |
| **Engagement kick-off meeting** | Work Product | 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. | Agreed starting date for on site assessment workshop |
| **GDPR Detailed Assessment workshop** | Work Product | Workshop to assess the maturity of its people, processes, and technology, relevant to the GDPR. The answers provided by the customer will be logged into the assessment tool together with relevant remarks and or observations. | Agreed starting date for on site assessment workshop |
| **Outcome analysis & write up** | Work product | The results of the on site workshop will be analyzed and a close out presentation will be created. | Agreed starting date for on site assessment workshop |
| **Close out presentation** | Work product | The findings from the assessment will be presented to the customer together with suggestions for next steps and if possible a roadmap towards GDPR compliance. | Within 2 weeks after analysis & write up |
| **Close out presentation** | Deliverable | Presentation that summarizes the assessment findings and includes recommended actions and roadmap. | Within 2 weeks after analysis & write up |

The deliverables will be submitted to the Customer for review and approval after the completion of the close out presentation.

Within three business days of the date of submittal, the Customer is required to:

* **Accept the deliverable** by signing, dating, and returning a service deliverable acceptance form, which can be sent by email or by using (or partially using) the deliverable.

Or

* **Reject the deliverable** by notifying Partner in writing; the Customer must include a complete list of reasons for rejection.

Deliverables shall be deemed accepted unless the written rejection notification is received by Partner in the timeframe specified.

If a rejection notification is received, the Partner will correct the problems with a deliverable that are in scope for the project, after which the deliverable is deemed accepted.

# Customer Resource Requirements

This section provides an overview of the resources required for a successful delivery of the GDPR Detailed Assessment.

|  |  |
| --- | --- |
| Resource | Description |
| **Project Executive Sponsor**  **(CPO, CISO, DPO)** | * Executive sponsor who is responsible for driving the strategic vision for the organization & making key decisions * Ultimate authority and accountability for the project and delivery on project objectives * Helps resolve issues escalated by project team * Sponsors communication within the company regarding project goals and deliverables * Provides guidance and clarity regarding overall security strategy, standards and policies for the organization |
| **Project Manager** | * Coordinates partner and working teams engaged in the project * Schedules all meetings with appropriate resources * Is the central point for dissemination of the engagement deliverables * Records and manages project issues, including escalations * Liaises with, and provides updates to, project executive sponsors * Ensures that the on-site requirements are met in time for the 2-day on-site workshops |
| **Enterprise, Compliance and/or Privacy Architects** | * Responsible for compliance and privacy strategy defined by the organization * Analyses and chooses products for the organization that meets business goals * Accountable for creating and maintaining the compliance architecture * Responsible for operation of compliance and privacy products * Provides insights into current and planned compliance and privacy guidelines, requirements and standards for the organization |
| **Privacy & Compliance Specialists** | * Responsible the deployment, operations and maintenance of security solutions * Provides technical knowledge on how existing security controls have been implemented |

# Customer Responsibilities

The customer is responsible to:

* Provide accurate and complete information during the workshop.
* Provide access to people (responders):
  + This includes access to knowledgeable customer personnel, including business user representatives.
* Provide a conference room to be used during the workshop and close out presentation.