
KE Consulting
Knowledge • Experience • Commitment

KE Consulting

Knowledge · Experience · Commitment

GDPR Detailed Assessment – January 2020

Pre-Engagement Meeting

Mario Pinto Ribeiro

KE Consulting

Knowledge · Experience · Commitment

Workshop	Description	Resources
Step 1		
Pre-engagement meeting	**Introduction to the GDPR Detailed assessment, discuss upcoming activities, align expectations and timelines. High level introduction to GDPR. Preview of the GDPR Detailed Assessment questions to help identify the customer representatives that will assist in answering.**	**00 - GDPR Detailed Assessment - Delivery Guide** **01 - GDPR Detailed Assessment – Pre Engagement Presentation**
Step 2		
Engagement Kickoff (on-site)	Kick off meeting to introduce (new) team members, brief the team on upcoming activities. Confirm meeting schedules and locations	00 - GDPR Detailed Assessment - Delivery Guide 02 - GDPR Detailed Assessment – Engagement Kickoff Presentation
GDPR Detailed Assessment	Complete discussion of the questions contained within the GDPR Detailed Assessment	00 - GDPR Detailed Assessment - Delivery Guide 03 - GDPR Detailed Assessment – Detailed Assessment tool
Outcome Analysis and Write-Up	Analyze and document results of the assessment, prepare the close out presentation.	00 - GDPR Detailed Assessment - Delivery Guide 04 - GDPR Detailed Assessment – Closeout Presentation
Step 3		
Close-out presentation	Present the findings from the assessment to the customer and define next steps and if possible a roadmap towards GDPR compliance.	00 - GDPR Detailed Assessment - Delivery Guide 04 - GDPR Detailed Assessment – Closeout Presentation

KE Consulting

Knowledge · Experience · Commitment

Agenda

- Introduction
- Introducing GDPR Detailed Assessment
- Engagement Overview
- GDPR Assessment Tool
- Project Governance

KE Consulting

Knowledge · Experience · Commitment

Step 1 - Objectives / Timeframe:

Workshop	Description	Outcome	Customer attendees	Time	Scheduled time, room
STEP 1					
Pre-Engagement	Present and discuss GDPR concepts and objectives and how KEC can help Customer achieve GDPR compliance.	List of next steps and a roadmap with actionable items and timelines, assisting towards GDPR compliancy	All project team	4 hours	<Time>, <Room>

KE Consulting

Knowledge · Experience · Commitment

We want to address the following questions:

- What is the GDPR?
- What is the perspective on the GDPR?
- What is the GDPR Detailed Assessment?
- What are the goals of the workshop?
- What is the workshop schedule?

KE Consulting

Knowledge · Experience · Commitment

GDPR

The General Data Protection Regulation (GDPR) comes into force in May 2018 and represents a significant overhaul of data protection legislation; the accountability principle will mean that businesses will need to examine how they hold and use data and take steps to demonstrate compliance with the data protection principles.

As businesses hold huge amounts of personal data relating to Customers, Vendors and Employees within their Dynamics NAV systems, currently there is very little functionality in existing or older versions (pre NAV 2018 / 'Tenerife') to support the new legislation.

KEC has spent a considerable amount of time to study and decipher the GDPR legislation, allowing the development of a Solution for GDPR management that will be embedded in your Dynamics NAV application.

KE Consulting

Knowledge · Experience · Commitment

Perspective of GDPR

- Personal / Sensitive data discovery
- Right to be Informed
- Right of Access
- Right to Rectification
- Right to Erasure
- Right to Restrict Processing
- Right to Data Portability
- Automated Encrypt and Destroy
- GDPR activities register.

Discover

Manage

Protect

Report

KE Consulting

Knowledge · Experience · Commitment

GDPR detailed assessment :

- **Identify GDPR compliance gaps**
  - *Identify maturity along key GDPR scenarios*

- **Identify potential data security and compliance challenges**
  - *Determine the current state of personal data security. Discuss and create an actionable data security roadmap for the customer*

KE Consulting

Knowledge · Experience · Commitment

Assessment objectives

➢ Understand customer GDPR compliance objectives

- *Gain a common understanding of compliance objectives and GDPR requirements*

➢ Assess customer GDPR maturity level

- *Assess customer's preparedness to execute on Discover, Manage, Protect, & Report activities*

➢ Create a GDPR compliance roadmap

- *Provide a prioritized and actionable GDPR remediation checklist and roadmap, ready for legal/advisory review*

KE Consulting

Knowledge · Experience · Commitment

Questionnaire of 150+ questions Structured around four vital areas:

- **Discover**, identify what personal data you have and where it resides
- **Manage**, govern how personal data is used and accessed
- **Protect**, establish security controls to prevent, detect, and respond to vulnerabilities and data breaches
- **Report**, execute on data requests, report data breaches, and keep required documentation

Questions have a weighting that counts towards the maturity score and stage

The tool generates recommendations and provides refences to GDPR articles

KE Consulting

Knowledge · Experience · Commitment

Discover

Discover	
D.1: Search for and identify personal data	**Recommended Responder:** Chief Information Security Officer (CISO), Data Protection Officer (DPO), IT Leadership **Related GDPR Reference(s):** Article 15(3)
D1.0	Can the organization generally identify all locations where personal data is stored across the enterprise, including on internal servers or cloud storage, as well as those hosted by any third-party providers?
D.2: Facilitate data classification	**Recommended Responder:** Data Protection Officer (DPO), Processor **Related GDPR Reference(s):** Article 30(2)(b-d); 32(2)
D2.0	Can the organization categorize the types of personal data it uses?
D.3: Maintain an inventory of personal data holdings	**Recommended Responder:** Data Center Leadership, Data Protection Officer (DPO), Marketing/Digital, Processor **Related GDPR Reference(s):** Article 30(1-3)
D3.0	Does the organization have a tool to catalog how and where personal data is used, and is it partially or fully populated?

KE Consulting

Knowledge · Experience · Commitment

Manage

Manage	
M.1: Enable data governance practices and processes	**Recommended Responder:** Chief Information Security Officer (CISO), Data Protection Officer (DPO), HR, Legal **Related GDPR Reference(s):** Article 5(2); 6(1); 8(2); 9(1); (2)(b-h); 10(1); 12(1); 24(2)
M1.0	Does the organization have a data governance program?
M.2: Provide detailed notice of processing activities to data subjects	**Recommended Responder:** Chief Information Security Officer (CISO), Data Protection Officer (DPO), HR, Legal **Related GDPR Reference(s):** Article 7(2); 12(1); 13(1-3); 14(1-4)
M2.0	Does the organization provide data subjects with privacy notices that describe how their data is used?
M.3: Discontinue processing on request	**Recommended Responder:** Data Center Leadership, Data Protection Officer (DPO), Marketing/Digital, Processor **Related GDPR Reference(s):** Article 7(3); 21(1-4); 30(4)
M3.0	When requested by a data subject, can the organization discontinue processing some forms of personal data?
M.4: Collect unambiguous, granular consent from data subjects	**Recommended Responder:** Data Protection Officer (DPO), Legal **Related GDPR Reference(s):** Article 7(1), (4); 8(1); 9(1), (2)(a), (3); 12(6); 16(1); 17(3); 18(2-3)
M4.0	Can the organization obtain consent from data subjects to process their personal data?
M.5: Facilitate communication mechanism between data subject and organization to handle data subject requests	**Recommended Responder:** Data Protection Officer (DPO), IT Leadership **Related GDPR Reference(s)** Article 12(2-5); 15; 16; 17(1), (3); 18(1); 19; 20(1)
M5.0	Does the organization have a published and easily accessible way for data subjects to communicate with the organization on privacy matters?

KE Consulting

Knowledge · Experience · Commitment

Protect

Protect	
P.1: Data protection and privacy by design and default	
Recommended Responder: Chief Information Security Officer (CISO), Data Protection Officer (DPO), IT Leadership, Operations **Related GDPR Reference(s):** Article 25(1-3)	
P1.0	Is the organization planning how to develop its technology, products, processes, and organizational structure with data protection and privacy as key components, and is it aware of the gaps for doing so?
P.2: Secure personal data through encryption	
Recommended Responder: Chief Information Security Officer (CISO), Data Protection Officer (DPO), IT Leadership **Related GDPR Reference(s):** Article 32(1)(a)	
P2.0	Is the organization aware of technologies to encrypt personal data and has it encrypted some personal data, such as government identification numbers, birthdates, or banking numbers?
P.3: Secure personal data by leveraging security controls that ensure the confidentiality, integrity, and availability of personal data	
Recommended Responder: Chief Information Security Officer (CISO), Compliance, Data Protection Officer (DPO), IT Leadership **Related GDPR Reference(s):** Article 29; 32(1)(b-c); (2); 46(1), (2)(a-f), 3(a-b)	
P3.0	Does the organization have an ongoing effort to identify needed people, process, and technology controls to protect the confidentiality, integrity, and availability (CIA) of personal data?
P.4: Prepare for, detect, and respond to data breaches	
Recommended Responder: Chief Information Security Officer (CISO), Compliance, Data Protection Officer (DPO), IT Leadership, Legal **Related GDPR Reference(s):** Article 12(1); 33(1-5); 34(1-2)	
P4.0	Is the organization aware of the potential impacts from breaches of personal data and does it have a response plan in place?
P.5: Facilitate regular testing of security measures	
Recommended Responder: Chief Information Security Officer (CISO), Data Protection Officer (DPO), IT Leadership **Related GDPR Reference(s):** Article 32(1)(d)	
P5.0	Does the organization perform testing of its security measures, whether through technical means, social engineering, or tabletop exercises?

KE Consulting

Knowledge · Experience · Commitment

Report

Report	
R.1: Keep record to display GDPR compliance	**Recommended Responder:** Compliance, Data Protection Officer (DPO), Legal, Operations **Related GDPR Reference(s):** Article 9(4); 23(1-2); 24(3); 30(1-2); 35(4-5); 36(5); 40(3); 42(2), (6); 87; 88(1-2); 90(1)
R1.0	Does the organization maintain records of processing activities with some additional information regarding the purpose or scope of the activities?
R.2: Track and record flows of personal data into and out of the EU	**Recommended Responder:** Compliance, Data Protection Officer (DPO), IT Leadership, Legal, Operations **Related GDPR Reference(s):** Article 45(1); 46(1-2)
R2.0	Does the organization have documentation of ongoing personal data transfers into and out of the EU?
R.3: Track and record flows of personal data to third-party service providers	**Recommended Responder:** Compliance, Data Protection Officer (DPO), IT Leadership, Legal, Third-Party Processors, **Related GDPR Reference(s):** Article 13(1)(f); 14(1)(f); 28 (1-5), (9); 46(1)
R3.0	Does the organization maintain an inventory of processes that transmit personal data to third-party service providers?
R.4: Facilitate data protection impact assessment	**Recommended Responder:** Chief Information Security Officer (CISO), Data Protection Officer (DPO), Project Management **Related GDPR Reference(s):** Article 5(1); 6(4); 25(2); 32(2); 35(1), (3), (7-9), (11); 36(1) (3) ; 39(1)(b-c); 39(2)
R4.0	Can the organization determine risks associated with personal data processing?

KE Consulting

Knowledge · Experience · Commitment

Output assessment :

Executive summary

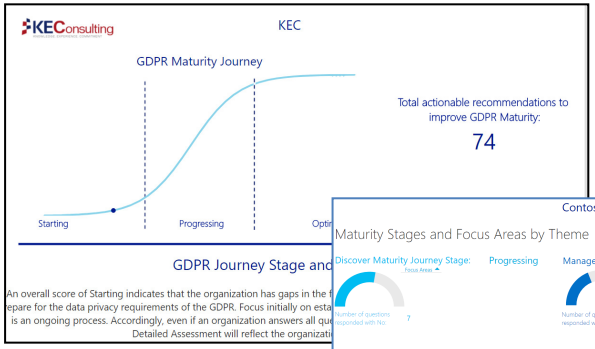
- Aggregated across all four DMPR themes
- Overall maturity of one of three levels: **Starting, Progressing or Optimizing**
- Results per theme and focus area

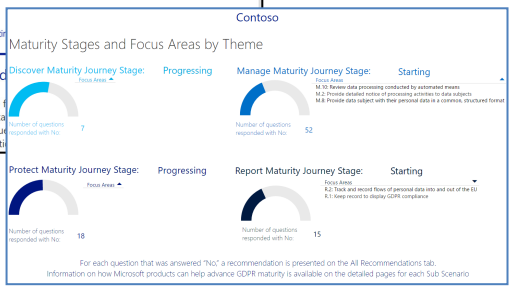
Detailed insights per theme

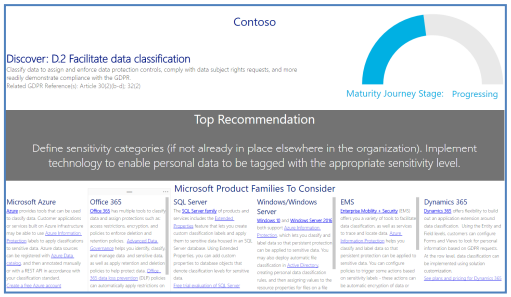
- Maturity index
- Top recommendation per sub scenario
- Microsoft Product suggestions

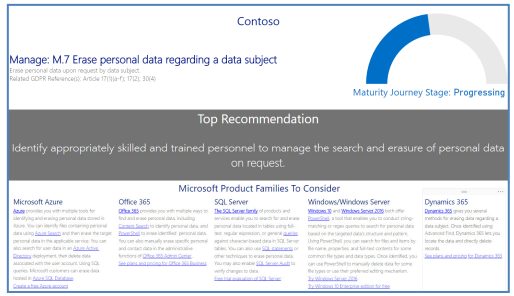
All Recommendations

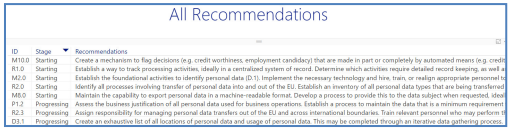
- Comprehensive and actionable list
- Full list of recommendations
- Grouped by sub-scenario and GDPR maturity stage
- For each theme and sub scenario











KE Consulting

Knowledge · Experience · Commitment

Project Governance :

Risk and issues management

- Covering business, technology and project execution
- Describe the escalation path

Date recorded	Risk/Issue description	Probability	Impact	Mitigation plan

Change management

- Describe the change management workflow

Success Criteria

- Discuss and agree on what a successful engagement would look like

KE Consulting

Knowledge · Experience · Commitment

NEXT STEP - 2

Book your Session !!

KE Consulting

Knowledge · Experience · Commitment

Step 2 - Objectives / Timeframe:

Workshop	Description	Outcome	Customer attendees	Time	Scheduled time, room
STEP 2					
GDPR detailed analysis / preparation	Questions / Answers of main GDPR issues, discuss any open items and identified issues.	Ready to move on with completion of the GDPR Detailed Assessment.	All project team	4 hours	<Time>, <Room>
Complete GDPR Detailed Assessment	Answer the remaining questions in the GDPR Detailed Assessment.	Completed GDPR questionnaire	Selected customer responders	1 Day	<Time>, <Room>
Outcome analysis & Write-Up	Review results of GDPR Detailed Assessment, prepare the close out presentation.	Action Plan and Close Out presentation	Compliance Team Partner	4 hours	<Time>, <Room>

KE Consulting

Knowledge · Experience · Commitment

NEXT STEP - 3

Book your Session !!

KE Consulting

Knowledge · Experience · Commitment

Step 3 - Objectives / Timeframe:

Workshop	Description	Outcome	Customer attendees	Time	Scheduled time, room
STEP 3					
Close Out Presentation	Present findings from the assessment and define next steps and roadmap towards GDPR compliance.	List of next steps and a roadmap with actionable items and timelines, assisting towards GDPR compliancy	All project team	4 hours	<Time>, <Room>

KE Consulting

Knowledge · Experience · Commitment

Thank You !

Mario Pinto Ribeiro
Operations Manager
E-mail: marior@keconsuting.co.uk

Laurence Sidney
Head of Project
E-mail: laurences@keconsuting.co.uk