

EUROPEAN UNION
GENERAL DATA PROTECTION REGULATION

Microsoft GDPR Journey

Ben Haklai, Attorney
CELA Commercial Lead - Israel

Disclaimer

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

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

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

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

Published November 2017
Version 1.0
© 2018 Microsoft. All rights reserved.

“Make no mistake, the GDPR sets a new and higher bar for privacy rights, for security, and for compliance.

And while your journey to GDPR may seem challenging, Microsoft is here to help all of our customers around the world.”

Brad Smith
President & Chief Legal Officer
Microsoft Corporation



EU General Data Protection Regulation

The **General Data Protection Regulation (GDPR)** imposes new rules on organizations in the European Union (EU) and those that offer goods and services to people in the EU, or that collect and analyze data tied to EU residents, no matter where they are located.

- **Enhanced** personal privacy rights
- **Increased** duty to protect data
- **Mandatory** breach reporting
- **Significant** penalties for non-compliance

Replaces 1995 privacy directive | Regulation passed May, 2016 | Enforcement begins 25 May 2018



What are the key changes to address the GDPR?



Personal privacy

Individuals have the right to:

- Access their personal data
- Correct errors in their personal data
- Erase their personal data
- Object to processing of their personal data
- Export personal data



Controls and notifications

Organizations will need to:

- Protect personal data using appropriate security
- Notify authorities of personal data breaches
- Obtain appropriate consents for processing data
- Keep records detailing data processing



Transparent policies

Organizations are required to:

- Provide clear notice of data collection
- Outline processing purposes and use cases
- Define data retention and deletion policies



IT and training

Organizations will need to:

- Train privacy personnel & employees
- Audit and update data policies
- Employ a Data Protection Officer (if required)
- Create & manage compliant vendor contracts

Getting Ready for GDPR Compliance – Burden to the Business?

GDPR Alignment – Affecting all business aspects...



Data Protection Impact Assessments



Data Subject Requests



Data Breach Notification



Accountability Readiness Checklist

Getting Ready for GDPR Compliance – Burden to the Business?

Aligning Terms with Vendors WW – a Standard Approach

Supplier Number	2327864
-----------------	---------

Omnibus General Data Protection Regulation Addendum

This Omnibus General Data Protection Regulation Addendum (*“Addendum”*) is between **Microsoft Israel Ltd.**, an Israel corporation (*“Microsoft”*), **Byme Technologies Ltd**, an Israel corporation (*“Supplier”*). This Addendum applies to each agreement between Microsoft (or any Microsoft Affiliate) and Supplier (or any Supplier Affiliate) under which Supplier Processes Personal Data as part of performing under that agreement (*“Agreement”*). The Addendum will be effective on the last signature date set forth below (*“Addendum Effective Date”*).

This Addendum consists of

- the terms and conditions below,
- the Agreement, which is incorporated by reference, and
- policies or procedures referenced in this Addendum.

Addresses and contacts for notices

Getting Ready for GDPR Compliance – Burden to the Business?

Aligning Terms with Customers WW – a Standard Approach

Attachment 4 – European Union General Data Protection Regulation Terms

Microsoft makes the commitments in these GDPR Terms, to all customers effective May 25, 2018. These commitments are binding upon Microsoft with regard to Customer regardless of (1) the version of the OST that is otherwise applicable to any given Online Services subscription or (2) any other agreement that references this attachment.

For purposes of these GDPR Terms, Customer and Microsoft agree that Customer is the controller of Personal Data and Microsoft is the processor of such data, except when Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor. These GDPR Terms apply to the processing of Personal Data, within the scope of the GDPR, by Microsoft on behalf of Customer. These GDPR Terms do not limit or reduce any data protection commitments Microsoft makes to Customer in the Online Services Terms or other agreement between Microsoft and Customer. These GDPR Terms do not apply where Microsoft is a controller of Personal Data.

Relevant GDPR Obligations: Articles 28, 32, and 33

1. Microsoft shall not engage another processor without prior specific or general written authorisation of Customer. In the case of general written authorisation, Microsoft shall inform Customer of any intended changes concerning the addition or replacement of other processors, thereby giving Customer the opportunity to object to such changes. (Article 28(2))
2. Processing by Microsoft shall be governed by these GDPR Terms under European Union (hereafter “Union”) or Member State law and are binding on Microsoft with regard to Customer. The subject-matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data, the categories of data subjects and the obligations and rights of the Customer are set forth in the Customer’s licensing agreement, including these GDPR Terms. In particular, Microsoft shall:
 - (a) process the Personal Data only on documented instructions from Customer, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by Union or Member State law to which Microsoft is subject; in such a case, Microsoft shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
 - (b) ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

Getting Ready for GDPR Compliance – Burden to the Business?

iapp

News Connect Train Certify Resources Conferences Join

STORE

The Privacy Advisor



Study: GDPR's global reach to require at least 75,000 DPOs worldwide

Nov 9, 2016

Save This

Getting Ready for GDPR Compliance – Burden to the Business?

- For a WW Service Provider leading with GDPR hiring a DPOs is just the **beginning**...
- PMs,
- Engineers,
- Architects,
- New Product Groups,
- Aligned Products,
- Privacy Professionals...

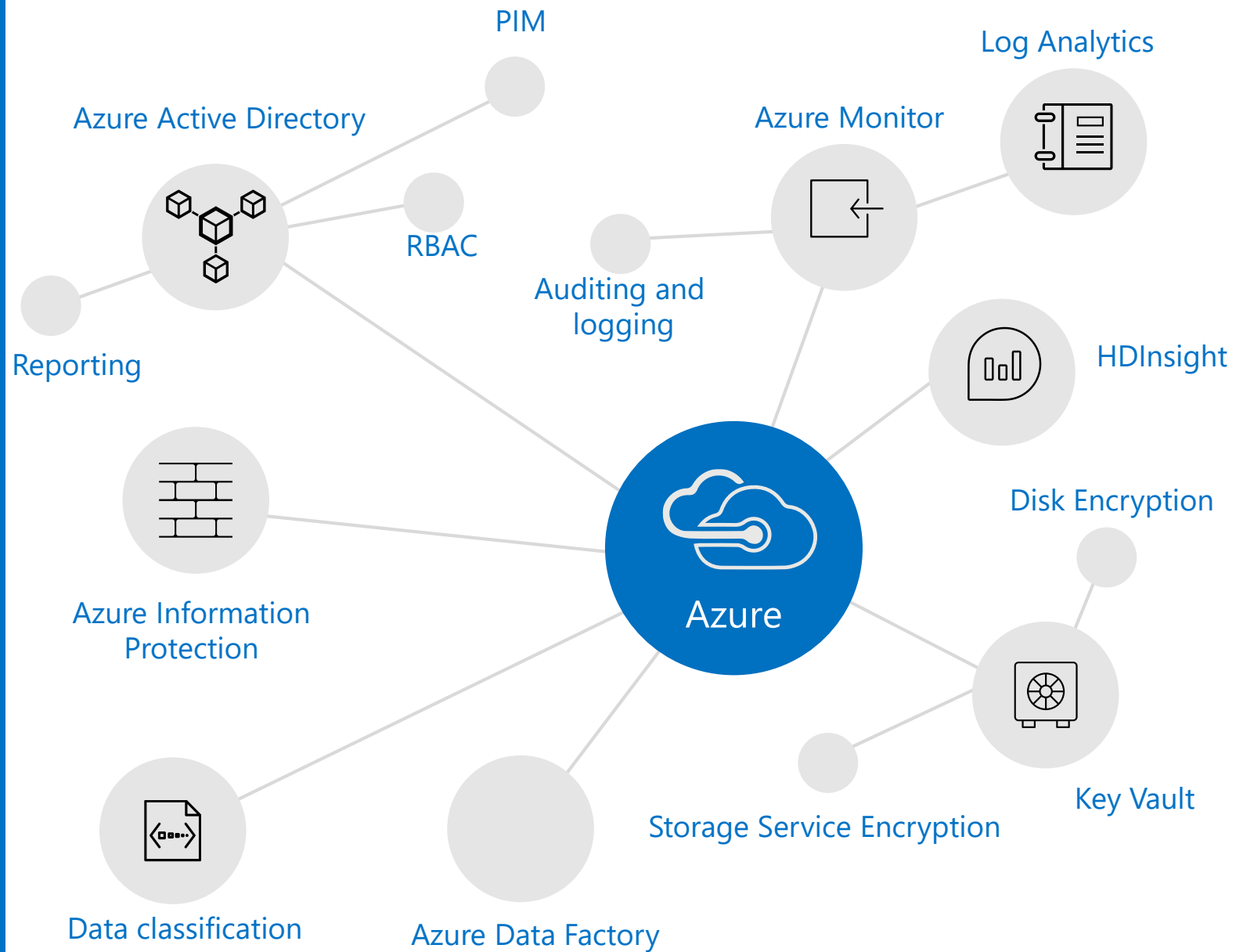
Getting Ready for GDPR Compliance – Burden to the Business?

- GDPR is the new WW Privacy Standard – new GDPR like regulations start appearing...
- California Consumer Privacy Act,
- Israeli Data Protection Regulations,
- Argentina Personal Data Protection Act (July),
- Brazil - The General Data Protection Law, federal law 13.709/2018 (August),
- Moroccan data protection law??
- Coming soon...

Getting Ready for GDPR Compliance – a Business Opportunity !



Solutions to help you prepare for the **GDPR**




Helping our Customers prepare for the GDPR

https://servicetrust.microsoft.com/ViewPage/TrustDocuments?command=Download&docTab=6d000410-c9e9-11e7-9a91-892aae8839ad_AuditedControls

 Dynamics 365 GDPR Control Mapping 8.30.2018	Comprehensive mapping of Microsoft Service Controls to GDPR obligations for Dynamics 365	2018-08-30
 Office 365 GDPR control mapping 5.24.18	Comprehensive mapping of Microsoft Service Controls to GDPR obligations for Office 365	2018-05-24
 Professional Services GDPR control mapping 5.24.18	Comprehensive mapping of Microsoft Service Controls to GDPR obligations for Professional Services	2018-05-24
 Azure GDPR control mapping 5.24.18	Comprehensive mapping of Microsoft Service Controls to GDPR obligations for Azure	2018-05-24

Microsoft 365 GDPR action plan — Top priorities for your first 30 days, 90 days, and beyond

08/15/2018 • 6 minutes to read • Contributors 

This article includes a prioritized action plan you can follow as you work to meet the requirements of the General Data Protection Regulation (GDPR). This action plan was developed in partnership with Protiviti, a Microsoft partner specializing in regulatory compliance. Learn more about how to use this action plan at Microsoft Ignite by attending this session: [Chart your Microsoft 365 compliance path and information protection strategy](#), presented by Maithili Dandige (Microsoft) and Antonio Maio (Protiviti).

The GDPR introduces new rules for companies, government agencies, non-profits, and other organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data for EU residents. The GDPR applies no matter where you or your enterprise are located.

Helping our
Customers
**prepare for the
GDPR**

<https://servicetrust.microsoft.com/ViewPage/GDPRDPIA>



Data Protection Impact Assessments (DPIAs)

How Microsoft helps controllers complete GDPR Data Protection Impact Assessments

How Microsoft can help you prepare DPIAs

Microsoft, as a processor, has a duty to assist controllers in ensuring compliance with the DPIA requirements laid out in the GDPR.

To support our customers, relevant sections of Microsoft's DPIAs are abstracted and will be provided through this section of the Service Trust Portal in future updates with the intent of allowing controllers relying on Microsoft services to leverage the abstracts in order to create their own DPIAs.

Microsoft documentation to support your DPIA compliance

Individually, Microsoft enterprise cloud services provide specific documentation to support your DPIA compliance.

Below are services which provide DPIA compliance information relevant to their Microsoft cloud service, click on a service to get started.

[Office 365](#)

[Azure](#)


[Dynamics 365](#)

[Microsoft Support and Professional Services](#)

Visit <https://aka.ms/DPIAinfo> to learn more.

Helping our Customers prepare for the GDPR

Data Subject Requests for the GDPR


📅 04/13/2018 • ⌚ 2 minutes to read • Contributors 

The General Data Protection Regulation (GDPR) gives rights to people (known in the regulation as data subjects) to manage the personal data that has been collected by an employer or other type of agency or organization (known as the data controller or just controller). Personal data is defined very broadly under the GDPR as any data that relates to an identified or identifiable natural person. The GDPR gives data subjects specific rights to their personal data; these rights include obtaining copies of it, requesting changes to it, restricting the processing of it, deleting it, or receiving it in an electronic format so it can be moved to another controller. A formal request by a data subject to a controller to take an action on their personal data is called a Data Subject Request or DSR. The controller is obligated to promptly consider each DSR and provide a substantive response either by taking the requested action or by providing an explanation for why the DSR cannot be accommodated by the controller. A controller should consult with its own legal or compliance advisers regarding the proper disposition of any given DSR.

These articles discuss [how to use Microsoft products, services, and administrative tools to help you find and act on personal data to respond to DSRs:](#)

- [Office 365](#)
- [Windows](#)
- [Azure](#)
- [Intune](#)
- [Dynamics 365](#)
- [Visual Studio Family](#)
- [Azure DevOps Services](#)
- [Microsoft Support and Professional Services](#)

Breach Notification under the GDPR

📅 04/13/2018 • ⌚ 2 minutes to read • Contributors 

Microsoft takes its obligations under the General Data Protection Regulation (GDPR) seriously. For information about how Microsoft services protect against a personal data breach and how we respond and notify you if a breach occurs, see the following topics:

- [Office 365](#)
- [Windows](#)
- [Azure](#)
- [Dynamics 365](#)
- [Microsoft Support and Professional Services](#)

For more information about how Microsoft detects and responds to a breach of personal data, see [Data Breach Notification Under the GDPR](#) in the Service Trust Portal.

Helping our
Customers
**prepare for the
GDPR**

<https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-breach-notification>

Azure Security and Compliance GDPR Blueprint

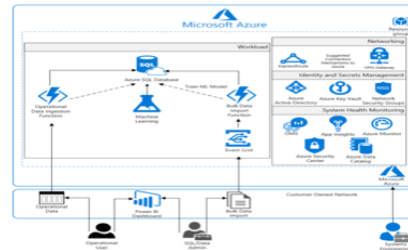
Providing customers supportive solutions for General Data Protection Regulation (GDPR) compliant workloads in Azure.



Helping our Customers prepare for the GDPR

<https://servicetrust.microsoft.com/ViewPage/GDPRBlueprint>

Reference Architectures

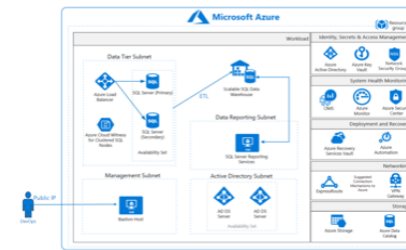


DA

Data Analytics

An SQL-based analytics platform that enables organizations to securely ingest, store, analyze, and interact with personal data while meeting GDPR compliance requirements. This solution includes Machine Learning services, Azure Functions, and Azure Event Grid.

[SEE MORE >](#)

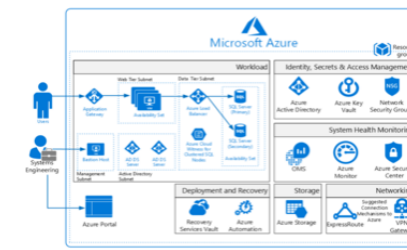


DW

Data Warehouse

An Azure SQL Data Warehouse that enables organizations to securely ingest, stage, store, and interact with personal data while meeting GDPR compliance requirements. This solution includes SQL Server Reporting Services (SSRS) for quick creation of reports from the Azure SQL Data Warehouse.

[SEE MORE >](#)

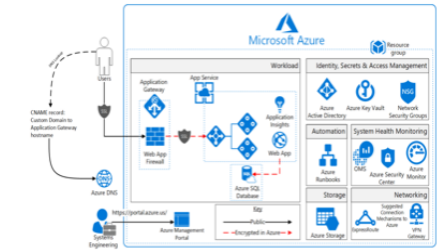


IaaS

Infrastructure as a Service

An IaaS web application with a database backend, including a web tier, data tier, Active Directory infrastructure, application gateway, and load balancer. This solution includes Operations Management Suite (OMS), Azure Monitor, and Azure Security Center for system health monitoring.

[SEE MORE >](#)



PaaS

Platform as a Service

A PaaS web application with an Azure SQL Database backend, including an App Service environment that load balances traffic for the web application across VMs managed by Azure. This solution includes Application Insights which provides real time application performance management and analytics through Operations Management Suite (OMS).

[SEE MORE >](#)

Blueprint Documents

The GDPR Blueprint consists of reference architectures, deployment guidance, GDPR Article implementation mappings, customer responsibility matrices (CRM), and threat models that enable customers to quickly and security implement cloud solutions.

Data Analytics | Data Warehouse | IaaS | PaaS

Document	Description	Report Date
Azure Security and Compliance Blueprint - GDPR Customer Responsibility Matrix	This workbook provides information regarding GDPR requirements in the context of the shared responsibility model for Azure Cloud.	2018-05-14
Azure Security and Compliance Blueprint - GDPR Data Analytics Overview	Provides guidance to deploy a data analytics architecture in Azure that assists with the requirements of the GDPR.	2018-05-04
Azure Security and Compliance Blueprint - GDPR Data Analytics Threat Model	Provides a detailed explanation of the solution boundaries and connections. This is a tm7 file and requires Microsoft Threat Modeling Tool - found here: https://www.microsoft.com/en-us/download/details.aspx?id=49168	2018-05-04
Azure Security and Compliance Blueprint - GDPR Data Analytics Threat Model	Data Analytics threat model illustration.	2018-05-04
Azure Security and Compliance Blueprint - GDPR Data Analytics Reference Architecture	GDPR Data Analytics reference architecture Visio drawing file.	2018-05-04
Azure Security and Compliance Blueprint - GDPR Data Analytics Reference Architecture	GDPR Data Analytics reference architecture illustration.	2018-05-04
Azure Security and Compliance Blueprint - GDPR Data Analytics Implementation Matrix	This control implementation matrix lists all security controls required by GDPR.	2018-05-04