The GDPR and Its Implications On Cloud Services

September 2017

Norm Barber, Managing Director
(normb@unifycloud.com)
A rapidly growing and successful Redmond, WA-based solutions developer with significant technical resources located in the US and India. Our global focus is on Cloud, Cybersecurity, Compliance (regulatory) and Cost.

Effectively migrating from a traditional, on-premises IT environment to a Hybrid IT environment that may include elements of SaaS, IaaS, and PaaS requires a logical set of steps.

As Gartner has noted, “An organization cannot simply ‘jump’ to the Cloud. There need to be activities that are part of a phased evaluation and plan to move to the Cloud.”

The General Data Protection Regulation (GDPR) impacts the entire Cloud (SaaS, IaaS, PaaS) journey
Disclaimer

This presentation is a commentary on the GDPR, as UnifyCloud LLC 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.

UNIFYCLOUD LLC MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS WHITE PAPER. This presentation is provided “as-is.” information and views expressed in this presentation, including URL and other Internet website references, may change without notice.
Today’s GDPR briefing topics

• What is the GDPR
• How to interpret the GDPR
• Addressing GDPR compliance in the Cloud
• GDPR Baseline approach
• Case Study: Managing GDPR in Azure
Audience poll: GDPR key roles that will impact you

**Controller (from GDPR)**
“...the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.”

**Processor (from GDPR)**
“... a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.”

**Solution Purveyor**
- CSV
- ISV
- Consultant
Poll:
How ready are you?
GDPR key drivers for May 25, 2018 enforcement (in effect as of 5/4/16)

- Updates and modernizes the principles of the 1995 Data Protection Directive
- Sets out the rights of the individual and establishes the obligations of those processing and those responsible for the processing of the data.
- Establishes the methods for ensuring compliance as well as the scope of sanctions for those in breach of the rules.
- Applies to all organizations doing business in the EU regardless of location.
GDPR data definitions regardless of nationality or EU residence

**Personal Data (from GDPR)**

“...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.”

**Examples:**

- Name
- Identification number (e.g., SSN)
- Location data (e.g., home address)
- Online identifier (e.g., e-mail address, screen names, IP address, device IDs)
- Genetic data (e.g., biological samples from an individual)
- Biometric data (e.g., fingerprints, facial recognition)

“The GDPR also requires compliance from non-EU organizations that offer goods or services to EU residents or monitor the behavior of EU residents.”

**Source:** Brief: You Need An Action Plan For The GDPR; Forrester Research; October 2016
GDPR compliance is a challenge for both controllers and processors

“By the end of 2018, over 50% of companies affected by the GDPR will not be in full compliance with its requirements.”

Gartner - *Focus on Five High-Priority Changes to Tackle the EU GDPR; September 30, 2016*

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

- **Enhanced** personal privacy rights
- **Increased** duty for protecting data
- **Mandatory** breach reporting
- **Significant** penalties for non-compliance
Controller’s (or your customer’s) GDPR compliance model

43 GDPR Requirements*

1. Provide notification to data subjects, in clear and plain language.
2. Request and obtain the data subject’s affirmative and granular consent.
3. Discontinue with processing activities if the data subject denies consent.
4. Provide a mechanism for data subjects to withdraw consent.
5. Obtain affirmative consent from a child’s (under age of 16) parent or guardian.

“...organizations must demonstrate that they have implemented appropriate measures to mitigate privacy risks. Even in the absence of a privacy breach or customer complaint, regulators may require firms to exhibit evidence of their compliance and risk management strategies, including a privacy impact assessment (PIA) when appropriate.”

Source: Brief: You Need An Action Plan For The GDPR; Forrester Research; October 2016

* UnifyCloud LLC GDPR interpretation. You are encouraged to complete your own GDPR interpretation.
Controller’s (or your customer’s) GDPR compliance model

43 GDPR Requirements*

1. Provide notice of processing activities at the time personal data is obtained.
2. Provide notice of processing activities if personal data has not been obtained directly.
3. Provide the data privacy notice at all points where personal data is collected.

* UnifyCloud LLC GDPR interpretation. You are encouraged to complete your own GDPR interpretation.
43 GDPR Requirements*

1. Provide mechanism for validating identity of the requesting data subject.
2. Provide mechanism for to request access to their personal data.
3. Provide a mechanism to respond to requests on personal data access.
4. Maintain the technological ability to trace and search personal data.
5. Provide mechanism to request rectification and rectify personal data.
6. Provide a mechanism to request the erasure of personal data.
7. Maintain the technological ability to locate and erase personal data.
8. Track to which additional controllers personal data has been transferred.

* UnifyCloud LLC GDPR interpretation. You are encouraged to complete your own GDPR interpretation
Controller’s (or your customer’s) GDPR compliance model

43 GDPR Requirements*

9. When personal data is made public, contact those entities for data erasure.
10. Provide mechanism to request the restriction of data processing.
11. Maintain the technological ability to restrict processing of personal data.
12. Provide mechanism to request copies and transmit personal.
13. Provide mechanism to respond to data portability requests.
14. Locate personal data and export in structured, machine-readable formats.
15. If processing for direct marketing, provide mechanism to object.
16. Maintain the technological ability to discontinue the data processing.

* UnifyCloud LLC GDPR interpretation. You are encouraged to complete your own GDPR interpretation
Controller’s (or your customer’s) GDPR compliance model

43 GDPR Requirements*

1. Maintain audit trails to demonstrate accountability and compliance.
2. Maintain inventory of data detailing categories of data subjects.
3. Maintain auditable trails of processing activities.
4. Carry out data protection impact assessments of processing operations.
5. Provide the de-identification of personal data for archiving purposes.

* UnifyCloud LLC GDPR interpretation. You are encouraged to complete your own GDPR interpretation
43 GDPR Requirements*

1. Embed privacy controls (in service and development lifecycle).
2. Embed privacy designed to minimize the amount of personal data collected.

* UnifyCloud LLC GDPR interpretation. You are encouraged to complete your own GDPR interpretation.
Controller’s (or your customer’s) GDPR compliance model

1. Provide mechanism to pseudonymize, encrypt, or otherwise secure personal data.
2. Implement security measures in the service.
3. Confirm ongoing confidentiality, integrity, and availability of personal data.
4. Provide mechanism to restore the availability and access to personal data.
5. Facilitate regular testing of security measures.

* UnifyCloud LLC GDPR interpretation. You are encouraged to complete your own GDPR interpretation.
Controller’s (or your customer’s) GDPR compliance model

1. Controllers notify DPA within 72 hours in the event of a data breach incident.
2. Controllers notify affected data subjects of a high-risk data breach incident.
3. Processors notify controllers without undue delay of a data breach incident.

* UnifyCloud LLC GDPR interpretation. You are encouraged to complete your own GDPR interpretation.
Controller’s (or your customer’s) GDPR compliance model

43 GDPR Requirements*

1. Track and record personal data that is forwarded to third-parties.
2. Provide mechanism for tracking and recording data transfers in and out of the EU.
3. Maintain inventory of data transfer contracts with third-parties.
4. Provide appropriate safeguards (e.g., Privacy Shield) for effective legal remedies.

* UnifyCloud LLC GDPR interpretation. You are encouraged to complete your own GDPR interpretation.
Controller’s (or your customer’s) GDPR compliance model

On Premises Compliance

Business Processes & User Controls

Applications & Workload Features

IT Infrastructure Controls

Internal Audit

- GDPR Regulation (261 pages)
- Compliance for Business Processes & User Controls
- Compliance for Applications & Workload Features
- Compliance for IT Infrastructure Controls

Consent (5)
Notice (3)
Data Subject Rights (16)
Data Governance (5)
Privacy by Design (2)
Data Security (5)
Breach Response (3)
Data Transfer (4)
Controller’s (or your customer’s) GDPR compliance model

Cloud Compliance Model

- Business Processes & User Controls
- SaaS Applications & Workload Features
- Internal Audit

GDPR Regulation (261 pages)

- Consent (5)
- Notice (3)
- Data Subject Rights (16)
- Data Governance (5)
- Privacy by Design (2)
- Data Security (5)
- Breach Response (3)
- Data Transfer (4)

Cloud Services

ISO 27018
ISO 27001

UnifyCloud
Controller’s (or your customer’s) GDPR compliance model

Cloud Compliance Model

Business Processes & User Controls

Internal Audit

“So a dashboard through which your team can easily track that (capabilities) will come in handy.”

Source: Brief: You Need An Action Plan For The GDPR; Forrester Research; October 2016
Poll:
How many cloud services providers do you have?
Understanding a Cloud shared responsibility model for GDPR

### Managed by Customer
- Customer Data
- Users and Roles
- Account Management
- Applications
- Firewalls
- Network Configuration
- Guest Operating System

### Managed by AWS
- Virtualization Layer
- Compute Infrastructure
- Storage Infrastructure
- Network Infrastructure
- Facilities Physical Security
- AWS Global Infrastructure

### Responsibility Matrix

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>On-Prem</th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data classification and accountability</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client and end point protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity and access management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application level controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: [Amazon Web Services](https://aws.amazon.com)

Source: [Microsoft](https://microsoft.com)
What “managed by customer” means (from a typical SOC* report)...

Controls and reporting as well as configuration oversight excluded from a CSV platform SOC report

- Controls over account / subscription IDs and passwords and access to applications.
- Compliance with applicable laws/regulations.
- Determining and implementing encryption for data.
- Securing certificates used to access applications.
- Selection of access mechanism for data.
- Determining the Services configurations.
- Backup of data to local / Cloud storage.
- Protection of the secrets associated with accounts.

- Implementing interconnectivity between Cloud and on-premises resources.
- Security Development Lifecycle for applications.
- Application QA prior to moving to Cloud production.
- Monitoring the security of applications.
- Reviewing and applying public security and patch updates (IaaS).
- Reporting the incidents and alerts specific to systems and subscriptions.
- Support timely responses with Cloud platform.
- Implementing redundant systems for hot-failover.

* AICPA Service Organization Control (SOC) Reports (Type I and Type II) formerly Statement on Auditing Standards No. 70: Service Organizations (SAS 70)
An Cloud Service GDPR Baseline should include:

- Cloud Services Compliance Validation (ISO, SOC)
- Services Setting Values
- DevOps Rules for Cloud Services

“However, in terms of security, while few respondents reported a decrease in production security, this is an area where DevOps has not yet contributed significant improvement. (See Figure 9) This may not be the fault of DevOps practices themselves—increasing security requires a deliberate effort—but it could point to an opportunity for tools vendors.”
Case Study: GDPR Baseline Dashboard for Azure

- 130 deployable Azure Services (last count)
- Some Services are candidates for GDPR defined “personal & sensitive data”
  - Blob Storage
  - Data Factory
  - Data lake Store
  - SQL Database
  - SQL Data Warehouse
  - StorSimple
- Some Services are capabilities to help meet GDPR requirements:
  - Azure AD
  - Azure Information Protection
  - Key Vault
  - Multi-factor Authentication
## Azure Services and GDPR compliance roles

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Cloud Service</th>
<th>High Level Description (from Capstone GDPR White paper)</th>
<th>Discover</th>
<th>Manage</th>
<th>Protect</th>
<th>Report</th>
<th>Enabler</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Active Directory</td>
<td>An identity and access management solution in the cloud. It manages identities and controls access to Azure, on-premises, and other cloud resources, data, and applications. With Azure Active Directory Privileged Identity Management, you can assign temporary, Just-In-Time (JIT) administrative rights to eligible users to manage Azure resources.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Key Vaults</td>
<td>It offers an easy, cost-effective way to safeguard keys and other secrets in the cloud by using hardware security modules (HSMs). Protect cryptographic keys and small secrets like passwords with keys stored in HSMs.</td>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>Storage Account (Classic)</td>
<td>An Azure storage account gives you access to the Azure Blob, Queue, Table, and File services in Azure Storage. Your storage account provides the unique namespace for your Azure Storage data objects. By default, the data in your account is available only to you, the account owner.</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>4</td>
<td>Data Factories</td>
<td>It is a managed service which lets you produce trusted information from raw data in cloud or on-premises sources. Easily create, orchestrate and schedule highly-available, fault-tolerant workflows of data movement and transformation activities.</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>5</td>
<td>Multifactor Authentication</td>
<td>It helps prevent unauthorized access to on-premises and cloud applications by providing an additional layer of authentication. Follow organizational security and compliance standards while also addressing user demand for convenient access.</td>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>6</td>
<td>Site Recovery</td>
<td>It helps you protect important applications by coordinating the replication and recovery of private clouds for simple, cost-effective disaster recovery.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>SQL Service</td>
<td>It is a relational database-as-a-service using the Microsoft SQL Server Engine. SQL Database is a high-performance, reliable, and secure database you can use to build data-driven applications and websites in the programming language of your choice, without needing to manage infrastructure.</td>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
# GDPR baseline setting guidance for Azure Services

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Cloud Service</th>
<th>CloudOrigin Functionality</th>
<th>Value</th>
<th>Subject</th>
<th>GDPR Citation</th>
<th>Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Active Directory</td>
<td>-&gt; Integration with local AD -&gt; Domains verified for Directory Sync</td>
<td>1</td>
<td>Data Subject Rights</td>
<td>Art. 15-17</td>
<td>Provide mechanism for validating identity of the requesting data subject.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Provide mechanism for validating identity of the requesting data subject.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Maintain the technological ability to restrict processing of data subjects’ personal data (or for Microsoft customers to do so in accordance with requests of data subjects).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Provide mechanism to pseudonymize, encrypt, or otherwise secure personal data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Activated</td>
<td>Data Security</td>
<td>Art. 32, Sec. 1, Sub. (a)</td>
<td>Provide mechanism for data subjects to request access to their personal data and receive information on the processing activities of their personal data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ACTIVEDIRECTORY_INTEGRATEDAPPLICATIONS_USERSMAYADDINTEGRATEDAPPLICATIONS</td>
<td>No</td>
<td>Data Subject Rights</td>
<td>Art. 15-17</td>
<td>Provide mechanism for validating identity of the requesting data subject.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ACTIVEDIRECTORY_USERACCESS_ALLOWINVITATIONS</td>
<td>Yes</td>
<td>Right to access</td>
<td>Art. 15, Secs. 1 – 2</td>
<td>Provide mechanism for data subjects to request access to their personal data and receive information on the processing activities of their personal data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ACTIVEDIRECTORY_USERACCESS_ALLOWGUESTSTOINVITE</td>
<td>No</td>
<td>Right to access</td>
<td>Art. 15, Secs. 1 – 2</td>
<td>Provide mechanism for data subjects to request access to their personal data and receive information on the processing activities of their personal data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ACTIVEDIRECTORY_USERACCESS_LIMITGUESTACCESS</td>
<td>Yes</td>
<td>Right to access</td>
<td>Art. 15, Secs. 1 – 2</td>
<td>Provide mechanism for data subjects to request access to their personal data and receive information on the processing activities of their personal data.</td>
</tr>
</tbody>
</table>
Creating a GDPR baseline
Creating a GDPR baseline

### Service Management

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Category</th>
<th>Is GDPR</th>
<th>GDPR Stages</th>
<th>GDPR Compliance type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Active Directory</td>
<td>Computer</td>
<td>Yes</td>
<td>NA</td>
<td>Manage NA Protect NA Report NA Enabler NA Target NA Status NA Actions OK De-Activate</td>
</tr>
<tr>
<td></td>
<td>Api Apps</td>
<td>Web + Mobile</td>
<td>No</td>
<td>NA</td>
<td>Manage NA Protect NA Report NA Enabler NA Target NA Status NA Actions OK De-Activate</td>
</tr>
<tr>
<td></td>
<td>API Management</td>
<td>Enterprise Integration</td>
<td>No</td>
<td>NA</td>
<td>Manage NA Protect NA Report NA Enabler NA Target NA Status NA Actions OK De-Activate</td>
</tr>
<tr>
<td></td>
<td>Application Gateways</td>
<td>Networking</td>
<td>Yes</td>
<td>NA</td>
<td>Manage NA Protect NA Report NA Enabler NA Target NA Status NA Actions OK De-Activate</td>
</tr>
<tr>
<td></td>
<td>Application Insights</td>
<td>Developer Tools</td>
<td>Yes</td>
<td>NA</td>
<td>Manage NA Protect NA Report NA Enabler NA Target NA Status NA Actions OK De-Activate</td>
</tr>
<tr>
<td></td>
<td>Audit Logs</td>
<td>Monitoring + Management</td>
<td>Yes</td>
<td>NA</td>
<td>Manage NA Protect NA Report NA Enabler NA Target NA Status NA Actions OK De-Activate</td>
</tr>
</tbody>
</table>
Creating a GDPR baseline
Creating a GDPR baseline

### DevOps Values Management

**Manage** DevOps Recommended Values

- Manage Service Wise: AzureStorage
- OR
- Manage Subscription Wise: Show Values

### AzureStorage Control IDs with Values

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Control ID</th>
<th>Recommended Value</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Azure_Storage_AuthN_Dont_Allow_Anonymous</td>
<td>public</td>
<td>Edit Value</td>
</tr>
<tr>
<td></td>
<td>(The Access Type for containers Must NOT allow public access with anonymous authentication)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Azure_Storage_Audit_Issue_Alt_AuthN_Req</td>
<td>Rules configured</td>
<td>Edit Value</td>
</tr>
<tr>
<td></td>
<td>(Alerts must be issued for authentication request data)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Azure_Storage_Deploy_Use_Geo_Reducant</td>
<td>Zone-redundant</td>
<td>Edit Value</td>
</tr>
<tr>
<td></td>
<td>(A Geo-Reducant Storage Account Type should be used)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Azure_Storage_DP_Encrypt_et_Rest_Blob</td>
<td>TRUE</td>
<td>Edit Value</td>
</tr>
<tr>
<td></td>
<td>(HBI Data at Rest in Azure Storage Blob Services must be encrypted)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Azure_Storage_Audit_Config_Log_AuthN_Req</td>
<td>365 Retention in days</td>
<td>Edit Value</td>
</tr>
</tbody>
</table>
Monitoring a GDPR baseline
## Monitoring a GDPR baseline

### Resource group With GDPR Mapping

<table>
<thead>
<tr>
<th>S.no.</th>
<th>Subscription</th>
<th>Resource Group</th>
<th>Service Type (Count)</th>
<th>Total Services</th>
<th>Journey Stage</th>
<th>GDPR Compliance %</th>
<th>GDPR Ready</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>87654321-541-417-905-218c2170e1 (Contoso 4)</td>
<td>201501newWeek</td>
<td>1</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Recommendation</td>
</tr>
<tr>
<td>2</td>
<td>87654321-541-417-905-218c2170e1 (Contoso 4)</td>
<td>Api-Default-Central-US</td>
<td>1</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Recommendation</td>
</tr>
<tr>
<td>3</td>
<td>87654321-541-417-905-218c2170e1 (Contoso 4)</td>
<td>Api-Default-North-Central-US</td>
<td>1</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Recommendation</td>
</tr>
<tr>
<td>4</td>
<td>87654321-541-417-905-218c2170e1 (Contoso 4)</td>
<td>Api-Default-West-US</td>
<td>1</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Recommendation</td>
</tr>
<tr>
<td>5</td>
<td>87654321-541-417-905-218c2170e1 (Contoso 4)</td>
<td>asCMDBDevNight</td>
<td>1</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Recommendation</td>
</tr>
<tr>
<td>6</td>
<td>87654321-541-417-905-218c2170e1 (Contoso 4)</td>
<td>BCP-PROD-R0</td>
<td>1</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Recommendation</td>
</tr>
</tbody>
</table>
Monitoring a GDPR baseline
Monitoring a GDPR baseline

<table>
<thead>
<tr>
<th>S.no.</th>
<th>Service Type</th>
<th>Total</th>
<th>Discover</th>
<th>Manage</th>
<th>Protect</th>
<th>Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Redis Caches</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• GDPR is in effect now and will be enforced starting on May 25, 2018

• Cloud solutions (IaaS/PaaS and SaaS) will be part of a controller’s compliance model

• Understand / interpret the GDPR requirements and map to processor features / controls

• Consider using a GDPR baseline approach for areas where certifications do not apply

• For vendors...do NOT imply using your solution will directly guarantee GDPR compliance

• Thank you! Any final questions?
The GDPR and Its Implications On Cloud Services

September 2017

Norm Barber, Managing Director
(normb@unifycloud.com)

A copy of this presentation will be made available to you after the session ends. Visit www.cloudatlasinc.com for additional information about our solutions.