

# The GDPR and Its Implications On Cloud Services

September 2017

Norm Barber, Managing Director  
([normb@unifycloud.com](mailto:normb@unifycloud.com))



# UnifyCloud LLC – General Background

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**.



CloudAtlas

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.**”

Discover

Assess

Target

Migrate

Monitor

← 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)

**European data protection for the digital era**

**Better protection for personal data**

- Clear consent required to process data
- Right to move data from one service provider to another
- More and clearer information about processing
- Right to rectify and remove data, including the 'right to be forgotten' for data collected as a child
- Limits on the use of automated processing of data to make decisions, for example in the case of 'profiling'
- Easier access to personal data
- Right to notification if data is compromised
- Stricter safeguards for transfers of personal data outside the EU

**More opportunities for business**

- Level playing field for all EU and non-EU businesses offering goods and services to persons in the EU
- One set of rules for the whole EU
- Rules that allow businesses, especially SMEs, to get the most out of the Digital Single Market
- Risk-based approach, matching obligations of controllers to the level of risk of the processing

**More consistent application and effective enforcement**

- Individuals and businesses can have their cases dealt with by a data protection authority and a court close to them
- A one-stop shop for individuals and businesses in cross-border cases thanks to the cooperation of national data protection authorities

**Fines** € up to €20 million OR 4% of global annual turnover

- 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

---

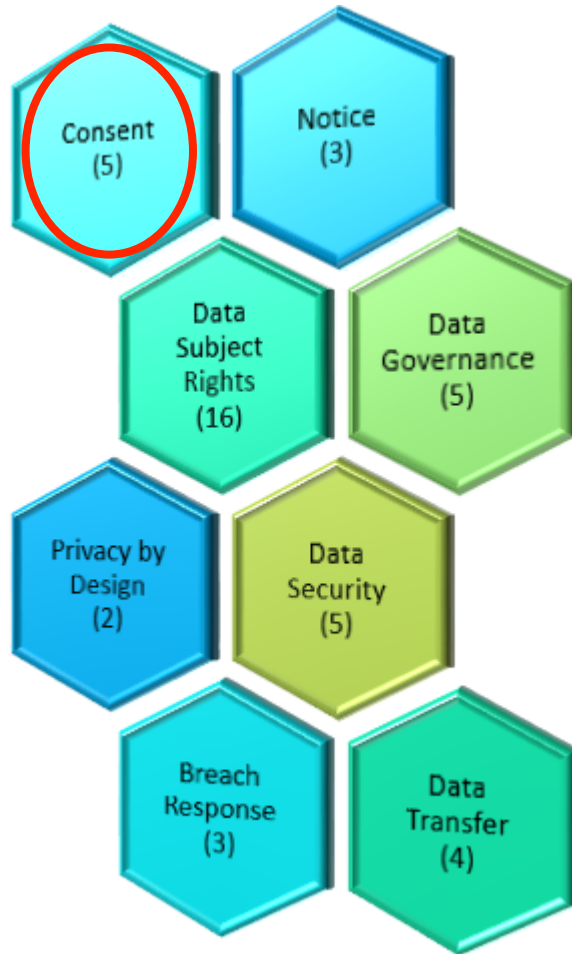
- **Significant** penalties for non-compliance

# Controller's (or your customer's) GDPR compliance model

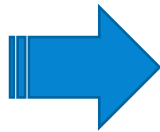


European Council  
Council of the European Union

43 GDPR Requirements\*



GDPR Regulation (261 pages)



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.  
 "...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."

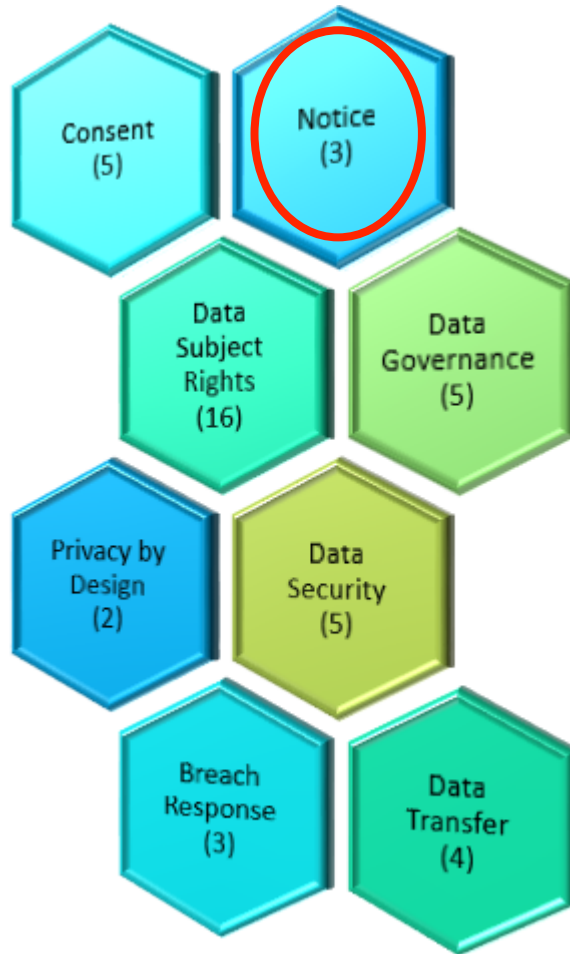
5. Obtain affirmative consent from a child's (under age of 16) parent or guardian.

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

# 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.

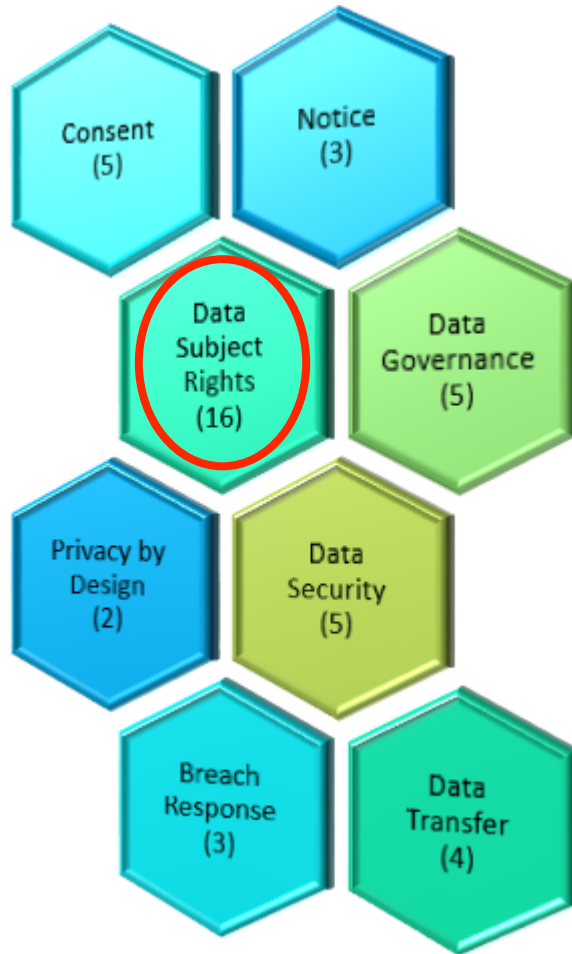
GDPR Regulation (261 pages)

# Controller's (or your customer's) GDPR compliance model



European Council  
Council of the European Union

43 GDPR Requirements\*



GDPR Regulation (261 pages)

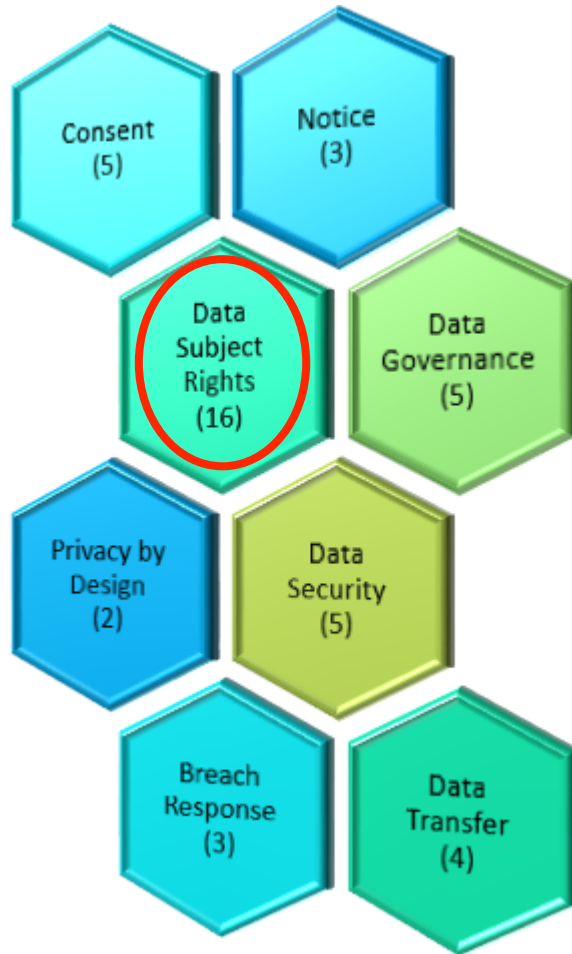
1. Provide mechanism for validating identity of the requesting data subject.
2. Provide mechanism for to request access to their personal data.
3. Provide a mechanism to respond to requests on personal data access.
4. Maintain the technological ability to trace and search personal data.
5. Provide mechanism 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.

# Controller's (or your customer's) GDPR compliance model



European Council  
Council of the European Union

## 43 GDPR Requirements\*



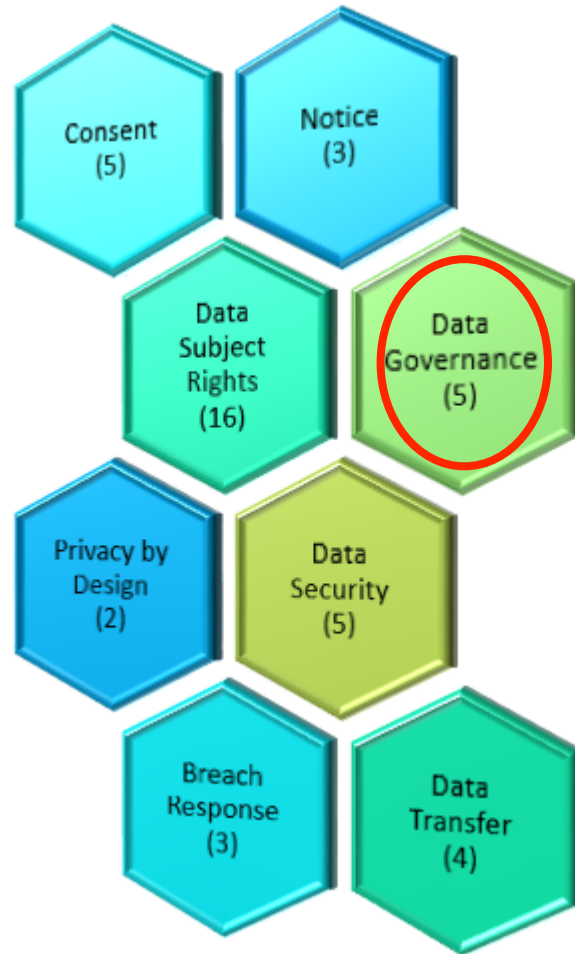
GDPR Regulation (261 pages)

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.

# 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.

GDPR Regulation (261 pages)

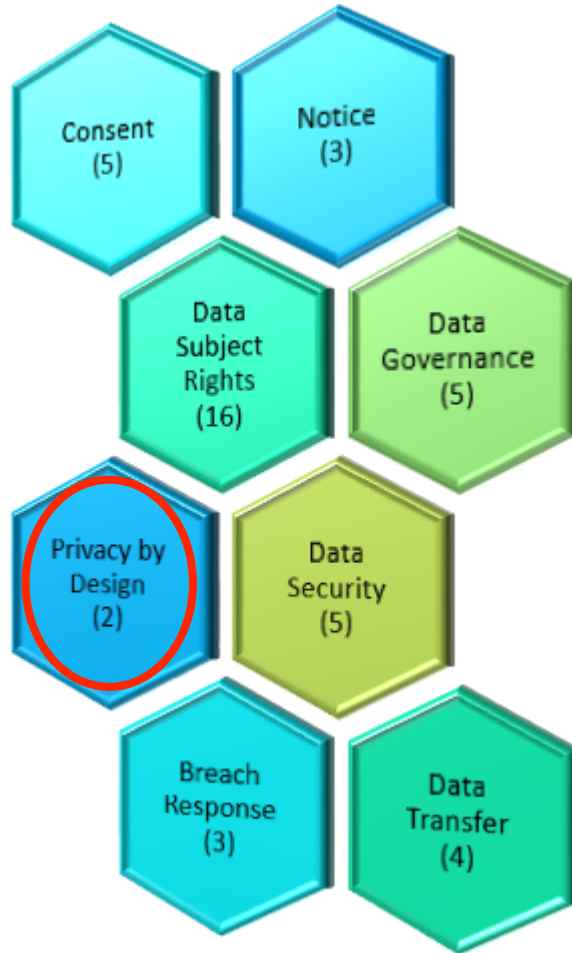
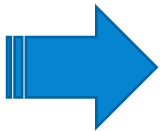
\* UnifyCloud LLC GDPR interpretation. You are encouraged to complete your own GDPR interpretation

# Controller's (or your customer's) GDPR compliance model



43 GDPR Requirements\*

GDPR Regulation (261 pages)



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

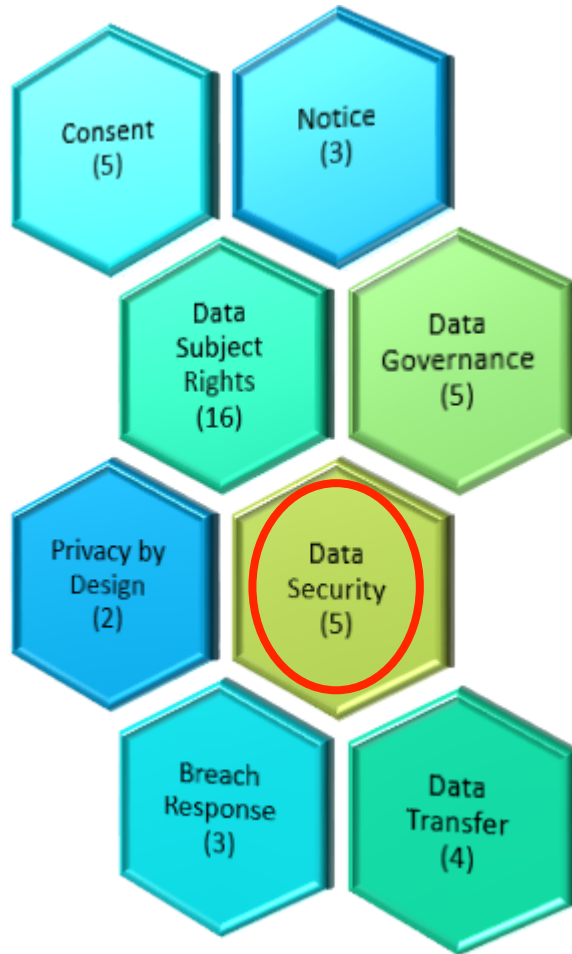


# Controller's (or your customer's) GDPR compliance model



European Council  
Council of the European Union

43 GDPR Requirements\*



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.

GDPR Regulation (261 pages)

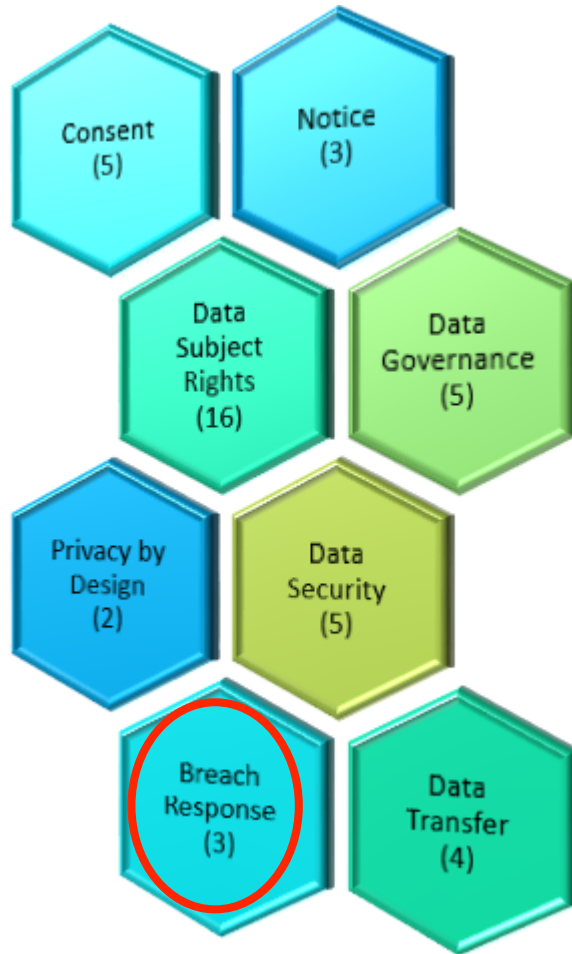


# Controller's (or your customer's) GDPR compliance model



European Council  
Council of the European Union

43 GDPR Requirements\*



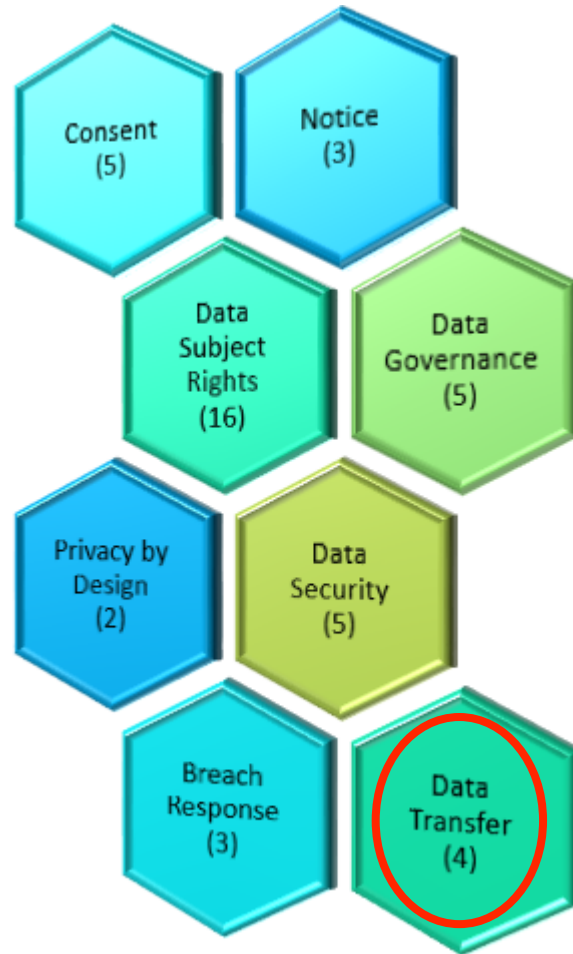
GDPR Regulation (261 pages)

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.

# 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.

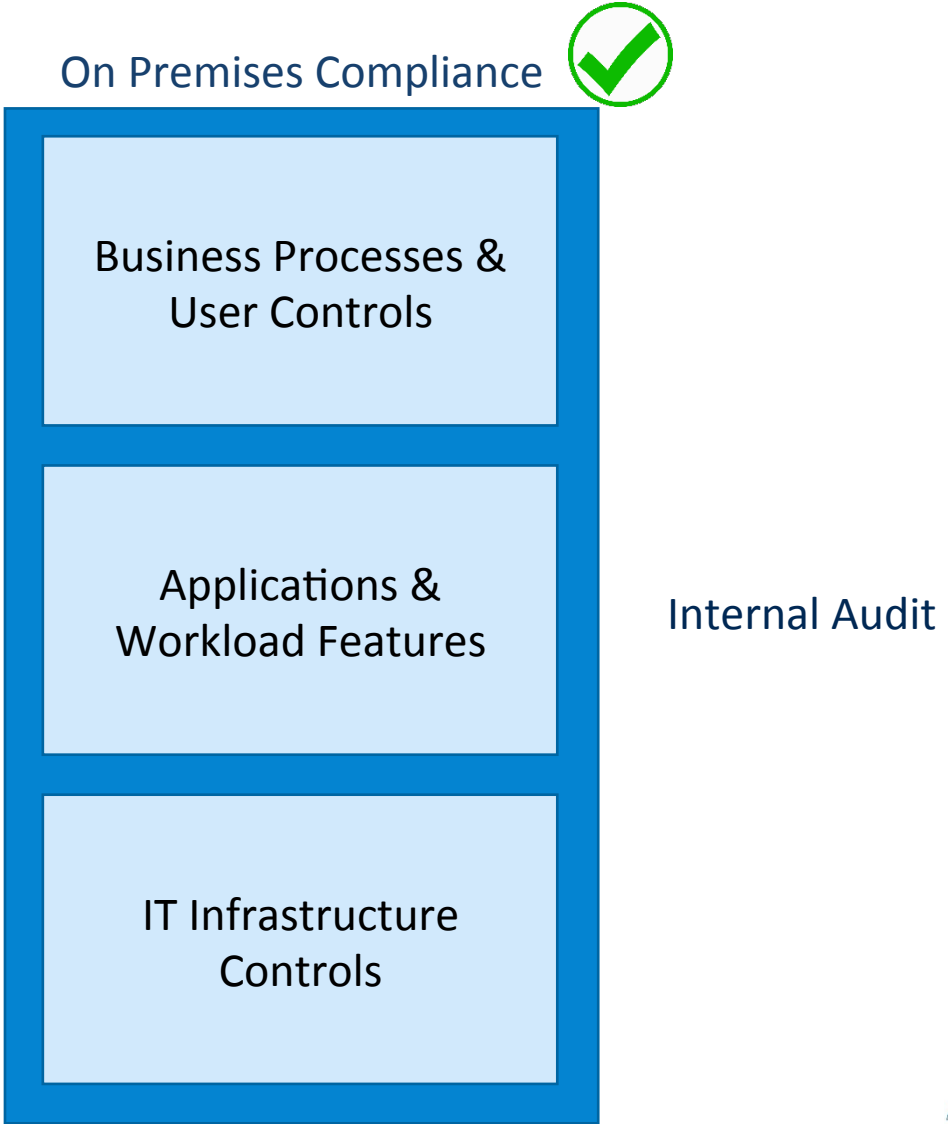
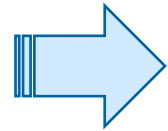
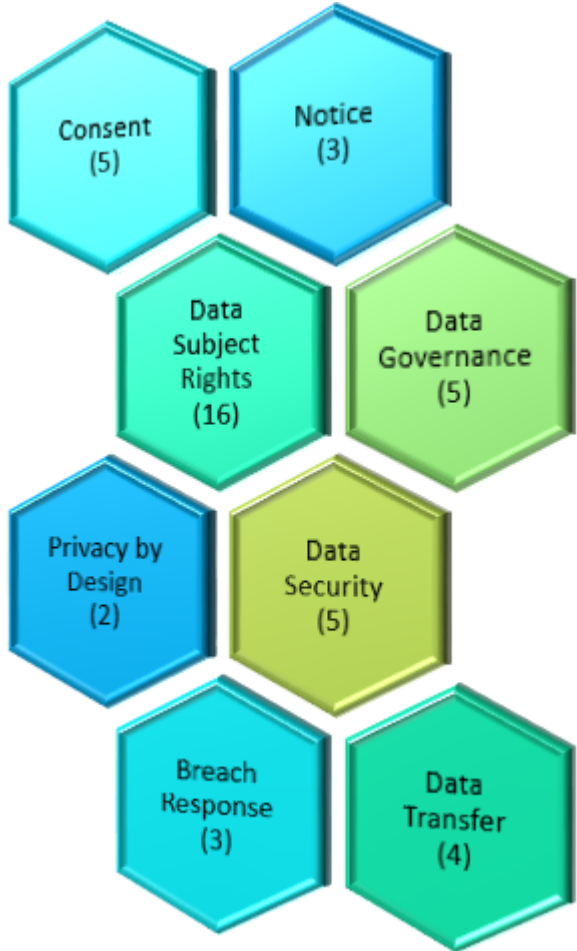
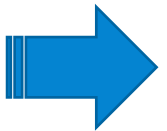
GDPR Regulation (261 pages)

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

# Controller's (or your customer's) GDPR compliance model



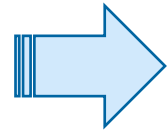
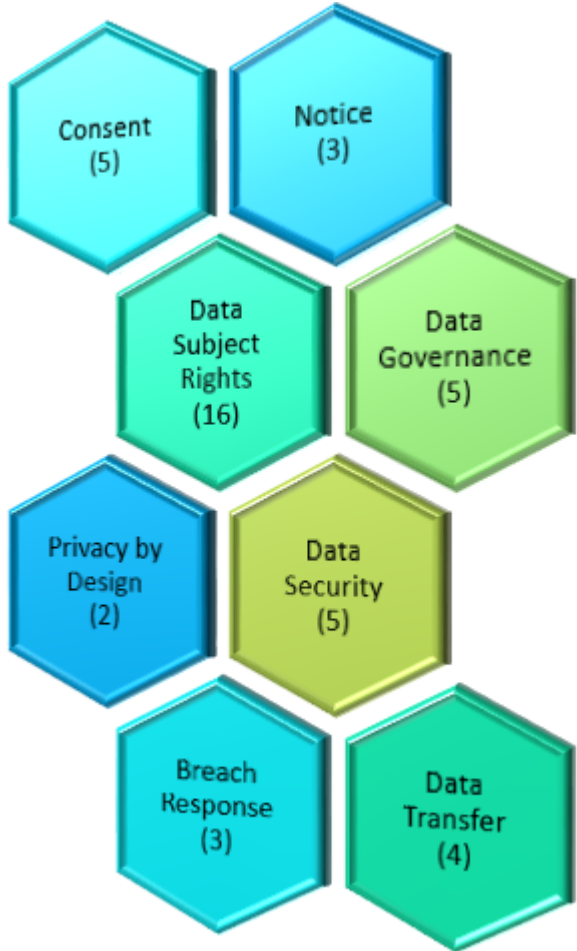
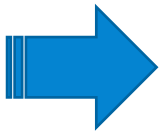
GDPR Regulation (261 pages)



# Controller's (or your customer's) GDPR compliance model



GDPR Regulation (261 pages)

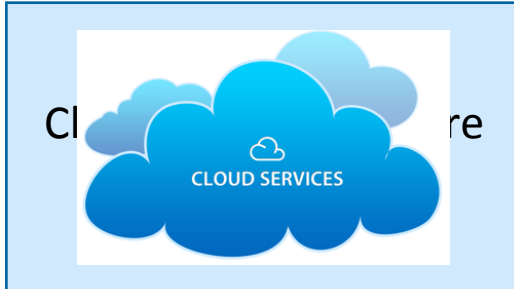


## Cloud Compliance Model



Business Processes & User Controls

SaaS Applications & Workload Features



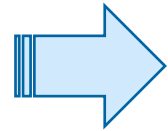
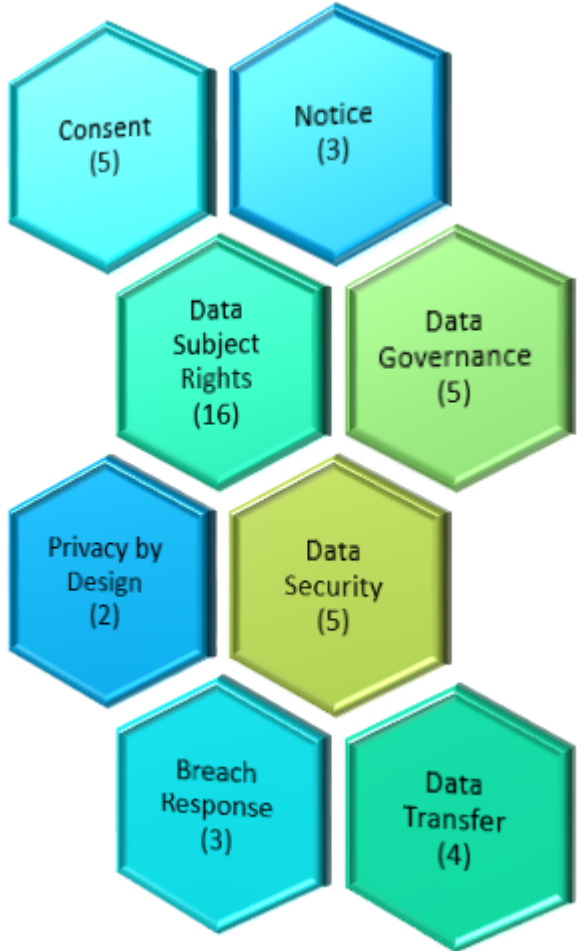
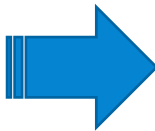
Internal Audit



# Controller's (or your customer's) GDPR compliance model



GDPR Regulation (261 pages)



## 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



SOC 2 Type 2    SOC 1 Type 2

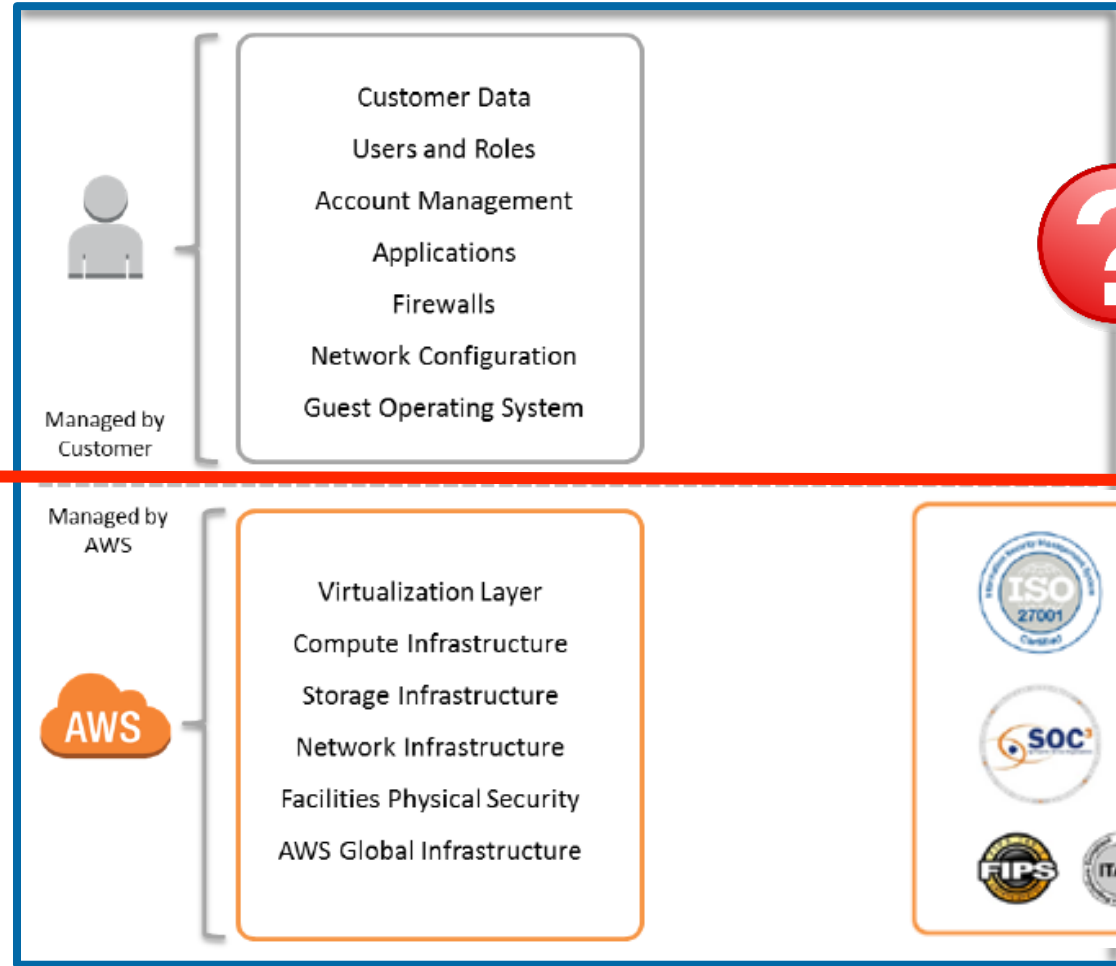


ISO 27018    ISO 27001



**Poll:**  
**How many cloud services providers  
do you have?**

# Understanding a Cloud shared responsibility model for GDPR



Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification and accountability	Cloud customer	Cloud customer	Cloud customer	Cloud customer
Client and end point protection	Cloud customer	Cloud customer	Cloud customer	Cloud customer
Identity and access management	Cloud customer	Cloud customer	Shared	Shared
Application level controls	Cloud customer	Cloud customer	Shared	Cloud provider
Network controls	Cloud customer	Cloud customer	Shared	Cloud provider
Host security	Cloud customer	Cloud provider	Cloud provider	Cloud provider
Physical security	Cloud customer	Cloud provider	Cloud provider	Cloud provider

Legend: ■ = Cloud customer, ■ = Cloud provider

Source: Amazon Web Services

Source: Microsoft

# 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.

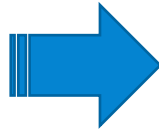
\* AICPA Service Organization Control (SOC) Reports (Type I and Type II)  
formerly Statement on Auditing Standards No. 70: Service Organizations (SAS 70)



# Using a GDPR baseline approach

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.

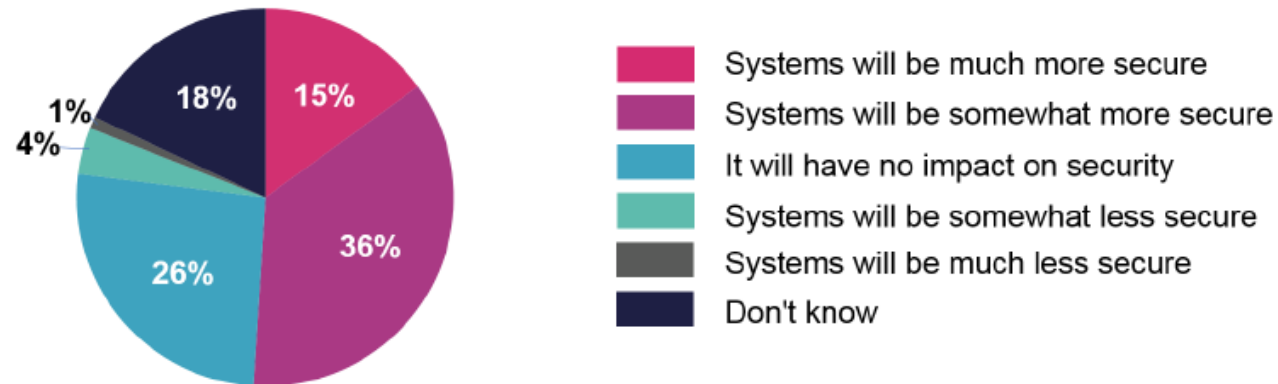


An Cloud Service GDPR Baseline should include:

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

## Impact on Security

What impact will DevOps have on the security of production systems?



Base: 237 respondents who have adopted or plan to adopt DevOps  
Data: UBM survey of 300 IT professionals involved in applications, January 2017

Figure 9

“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

## The Azure Periodic Table

Explore the power and possibilities of Azure

 DATA FACTORY									 TRAFFIC MANAGER	
 STREAM ANALYTICS	 EVENT HUBS					 SQL DATABASE	 SQL DATA WAREHOUSE	 DOCUMENTDB	 AZURE SEARCH	 EXPRESSROUTE
 MACHINE LEARNING	 HDINSIGHT	 VIRTUAL MACHINES	 CLOUD SERVICES	 BATCH	 REMOTEAPP	 STORAGE	 STORSIMPLE	 AZURE REDIS CACHE	 VIRTUAL NETWORK	
 AZURE AD	 MULTI-FACTOR	 BACKUP	 SITE RECOVERY	 SERVICE BUS	 BIZTALK SERVICES	 SCHEDULER	 AUTOMATION	 OPERATIONAL INSIGHTS	 DNS	
 WEB APPS	 MOBILE APPS	 NOTIFICATION HUBS	 API MANAGEMENT	 MOBILE ENGAGEMENT	 APP SERVICES	 API APPS	 LOGIC APPS	 KEY VAULT	 APPLICATION GATEWAY	
 VISUAL STUDIO	 APPLICATION INSIGHTS	 MEDIA SERVICES	 MEDIA INDEXER	 MEDIA ENCODING	 MEDIA PROTECTION	 MEDIA PLAYER	 MEDIA STREAMING	 CDN	 VPN GATEWAY	

- 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

S.No.	Cloud Service	High Level Description (from Capstone GDPR White paper)	Journey Stage				Compliance	
			Discover	Manage	Protect	Report	Enabler	Target
1	<b>Active Directory</b>	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.		Yes	Yes		Yes	
2	<b>Key Vaults</b>	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.			Yes		Yes	
3	<b>Storage Account (Classic)</b>	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.		Yes				Yes
4	<b>Data Factories</b>	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 work flows of data movement and transformation activities.		Yes				Yes
5	<b>Multifactor Authentication</b>	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.			Yes		Yes	
6	<b>Site Recovery</b>	It helps you protect important applications by coordinating the replication and recovery of private clouds for simple, cost-effective disaster recovery.			Yes		Yes	
7	<b>SQL Service</b>	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.		Yes	Yes			Yes

# GDPR baseline setting guidance for Azure Services

S.No.	Cloud Service	CloudOrigin Functionality	Value	Subject	GDPR Citation	Issue
1	Active Directory	Active Directory -> Integration with local AD -> Domains verified for Directory Sync	1	Data Subject Rights	Art. 15-17	Provide mechanism for validating identity of the requesting data subject.
		Active Directory -> Integration with local AD -> Domains planned for Single Sign-On	0	Data Subject Rights	Art. 15-17	Provide mechanism for validating identity of the requesting data subject.
		Active Directory -> Integrated Applications -> Users may give applications permission to access their data	NO	Right to Restriction	Art. 18, Sec. 1, Sub. (a)–(d)	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).
		Active Directory -> Integration with local AD -> Directory Sync	Activated	Data Security	Art. 32, Sec. 1, Sub. (a)	Provide mechanism to pseudonymize, encrypt, or otherwise secure personal data.
		ACTIVEDIRECTORY_INTEGRATEDAPPLICATIONS_USERSMAYADDINTEGRATEDAPPLICATIONS	No	Data Subject Rights	Art. 15-17	Provide mechanism for validating identity of the requesting data subject.
		ACTIVEDIRECTORY_USERACCESS_ALLOWINVITATIONS	Yes	Right to access	Art. 15, Secs. 1 – 2	Provide mechanism for data subjects to request access to their personal data and receive information on the processing activities of their personal data.
		ACTIVEDIRECTORY_USERACCESS_ALLOWGUESTSTOINVITE	No	Right to access	Art. 15, Secs. 1 – 2	Provide mechanism for data subjects to request access to their personal data and receive information on the processing activities of their personal data.
		ACTIVEDIRECTORY_USERACCESS_LIMITGUESTACCESS	Yes	Right to access	Art. 15, Secs. 1 – 2	Provide mechanism for data subjects to request access to their personal data and receive information on the processing activities of their personal data.

# Creating a GDPR baseline

Cloud Origin®

Norm Barber  
MasterAdmin

Control Panel Norm Barber

## Category List

Search Services... Go! + Expand All

Compute - Total Service: 6

Active Directory						Cloud Service(Classic)						Virtual Machine						Virtual Machine Scale Sets					
Property			Priority			Property			Priority			Property			Priority			Property			Priority		
System Defined	User Defined	Total	High	Medium	Low	System Defined	User Defined	Total	High	Medium	Low	System Defined	User Defined	Total	High	Medium	Low	System Defined	User Defined	Total	High	Medium	Low
13	3	16	8	3	5	2	5	7	0	3	4	12	16	28	9	12	7	12	18	30	7	14	8

VM Images						AvailabilitySets					
Property			Priority			Property			Priority		
System Defined	User Defined	Total	High	Medium	Low	System Defined	User Defined	Total	High	Medium	Low
2	13	15	3	5	7	4	4	8	4	0	4

Containers - Total Service: 3


Data + Analytics - Total Service: 3


Databases - Total Service: 6

Developer Tools - Total Service: 3










[Show All](#)  
[Compute 6](#)  
[Containers 3](#)  
[Data + Analytics 3](#)  
[Databases 6](#)  
[Developer Tools 3](#)  
[Enterprise Integration 6](#)  
[Internet of Things 4](#)  
[Monitoring + Management 7](#)

# Creating a GDPR baseline

 Cloud Origin®

 Norm Barber  
MasterAdmin
























MICROSOFT AZURE

-  Dashboard
-  Azure Services
-  Manage Services
-  Services Setting
-  Settings Values
-  Baseline
-  Compliance
-  DevOps
-  ARM Templates

## Service Management

[Add New](#) [Export to MS-Excel](#)

Show  entries Search:

Basic Details			Is GDPR?	GDPR Stages				GDPR Compliance type			
Icon	Name	Category	Status	Discover	Manage	Protect	Report	Enabler	Target	Status	Actions
	<a href="#">Active Directory</a>	Compute	Yes	N.A		N.A	N.A	N.A			<a href="#">Edit</a> <a href="#">De-Activate</a>
	<a href="#">Api Apps</a>	Web + Mobile	No	N.A	N.A	N.A	N.A	N.A	N.A		<a href="#">Edit</a> <a href="#">De-Activate</a>
	<a href="#">API Management</a>	Enterprise Integration	No	N.A	N.A	N.A	N.A	N.A	N.A		<a href="#">Edit</a> <a href="#">De-Activate</a>
	<a href="#">Application Gateways</a>	Networking	Yes	N.A	N.A		N.A		N.A		<a href="#">Edit</a> <a href="#">De-Activate</a>
	<a href="#">Application Insights</a>	Developer Tools	Yes	N.A			N.A		N.A		<a href="#">Edit</a> <a href="#">De-Activate</a>
	<a href="#">Audit Logs</a>	Monitoring + Management	Yes	N.A				N.A			<a href="#">Edit</a> <a href="#">De-Activate</a>

# Creating a GDPR baseline

Cloud Origin®

Norm Barber  
MasterAdmin

Tenant Id : d70cb4db-69c4-4a49-aaf3-f1e7ac277686

Domain : unifycloud.com

Norm Barber

Manage Settings/Properties Compliance Values

Active Directory Settings Tree View

Active Directory

GDPR All

Expand Collapse

**Active Directory**

- Integration with local AD**
  - Domains verified for Directory Sync **GDPR**
  - Domains planned for Single Sign-On **GDPR**
  - Directory Sync **GDPR**
- Integrated Applications**
  - Users may give applications permission to access their data **GDPR**
  - Users may add integrated applications **GDPR**
- User Access**
  - Allow Invitations **GDPR**
  - Allow guests to invite **GDPR**
  - Limit Guests access **GDPR**

**Integration with local AD -> Domains verified for Directory Sync**

**GDPR** **HBI** **System Defined**

Types	Values (Compliance)	Actions
Available Values	0	
	1	
Recommended Value	1	<a href="#">Edit</a> <a href="#">Delete</a>
Recommended URL	<a href="https://redmondmag.com/articles/2013/09/01/inside-windows-azure-active-directory.aspx">https://redmondmag.com/articles/2013/09/01/inside-windows-azure-active-directory.aspx</a>	<a href="#">Edit</a> <a href="#">Delete</a>

[Manage GDPR Mapping](#)

**GDPR Subject and Issue Mapping**

<b>Subject</b>	Data Subject Rights
<b>Citation</b>	Art. 15-17
<b>Issue</b>	Provide mechanism for validating identity of the requesting data subject.

MICROSOFT AZURE

- Dashboard
- Azure Services
- Services Setting
- Settings Values
- Baseline
- Compliance
  - Manage Compliance Values
- DevOps
- ARM Templates

# Creating a GDPR baseline

Cloud Origin®

Norm Barber

MasterAdmin

MICROSOFT AZURE

- Dashboard ▼
- Azure Services ▼
- Services Setting ▼
- Settings Values ▼
- Baseline ▼
- Compliance ▼
- DevOps ▼
- Manage DevOps Values
- ARM Templates ▼

## DevOps Values Management

Manage DevOps Recommended Values ^ ↻ ✕

Manage Service Wise AzureStorage ▼

OR

Manage Subscription Wise Show Values

### ⚙️ AzureStorage Control Ids with Values

S.No.	Control ID	RecommendedValue	Actions
1	<b>Azure_Storage_AuthN_Dont_Allow_Anonymous</b> <small>(The Access Type for containers Must NOT allow public access with anonymous authentication)</small>	public	<span style="background-color: #28a745; color: white; padding: 2px 5px; font-size: 0.8em;">✎ Edit Value</span>
2	<b>Azure_Storage_Audit_Issue_Alert_AuthN_Req</b> <small>(Alerts must be issued for authentication request data)</small>	Rules configured	<span style="background-color: #28a745; color: white; padding: 2px 5px; font-size: 0.8em;">✎ Edit Value</span>
3	<b>Azure_Storage_Deploy_Use_Geo_Redundant</b> <small>(A Geo-Redundant Storage Account Type should be used)</small>	Zone-redundant	<span style="background-color: #28a745; color: white; padding: 2px 5px; font-size: 0.8em;">✎ Edit Value</span>
4	<b>Azure_Storage_DP_Encrypt_at_Rest_Blob</b> <small>(HBI Data at Rest in Azure Storage Blob Services must be encrypted)</small>	TRUE	<span style="background-color: #28a745; color: white; padding: 2px 5px; font-size: 0.8em;">✎ Edit Value</span>
5	<b>Azure_Storage_Audit_Config_Log_AuthN_Req</b> <small>(The Storage Account must be configured to log and monitor authentication request data)</small>	365 Retention in days.	<span style="background-color: #28a745; color: white; padding: 2px 5px; font-size: 0.8em;">✎ Edit Value</span>



# Monitoring a GDPR baseline

CloudSupervisor® Contosa 4 demo@unifycloud.com

Month - September

No. of Subscriptions	Total Services	Databases	HD Insights	App Services	SQL	Automation	Monthly Trend
1	90	58	0	32	0	0	

### Databases

Redis Caches			
Resources	Cost /month	Baseline Mismatch	Security Issue
58	0	58	0

### App Services

Website(Classic)			
Resources	Cost /month	Baseline Mismatch	Security Issue
32	0	0	0

Navigation menu:

- Dashboard
- Main Dashboard
- Subscription
- Focus Baseline
- Usage Analytics
- Billing Analytics
- Security Analytics
- Costing Analytics
- Advisor Analytics
- GDPR Dashboard
- BackUp & Recovery
- Cost & Utilization
- Security & Compliance
- Container Security
- Application Migration
- Settings

# Monitoring a GDPR baseline

CloudSupervisor® Contosa 4

demo@unifycloud.com

Resource group With GDPR Mapping

S.no.	Subscription	Resource Group	Service Type (Count)	Total Services	Journey Stage				GDPR Compliance %	GDPR Ready	Recommendation
					Discover	Manage	Protect	Report			
1	87654321-5c41-41e7-9f39-e138c21c7ea1 (Contosa 4)	2015OneWeek	1	10	No	Yes	No	No	25 % 75 %	No	Recommendation
2	87654321-5c41-41e7-9f39-e138c21c7ea1 (Contosa 4)	Api-Default-Central-US	1	2	No	Yes	No	No	25 % 75 %	No	Recommendation
3	87654321-5c41-41e7-9f39-e138c21c7ea1 (Contosa 4)	Api-Default-North-Central-US	1	3	No	Yes	No	No	25 % 75 %	No	Recommendation
4	87654321-5c41-41e7-9f39-e138c21c7ea1 (Contosa 4)	Api-Default-West-US	1	3	No	Yes	No	No	25 % 75 %	No	Recommendation
5	87654321-5c41-41e7-9f39-e138c21c7ea1 (Contosa 4)	azCMDBDevNight	1	4	No	Yes	No	No	25 % 75 %	No	Recommendation
6	87654321-5c41-41e7-9f39-e138c21c7ea1 (Contosa 4)	BCP-PROD-RG	1	1	No	Yes	No	No	25 % 75 %	No	Recommendation

Dashboard

- Main Dashboard
- Subscription
- Focus Baseline
- Usage Analytics
- Billing Analytics
- Security Analytics
- Costing Analytics
- Advisor Analytics
- GDPR Dashboard**
- BackUp & Recovery
- Cost & Utilization
- Security & Compliance
- Container Security
- Application Migration
- Settings

# Monitoring a GDPR baseline

CloudSupervisor® Contosa 4 demo@unifycloud.com

**To make resource group GDPR compliant, add at least any one service from each category**

Protect	Discover	Report
Application Gateways	Azure Information Protection	Audit Logs
Application Insights	Data Catalog	Event Hubs
Audit Logs	Search Services	Log Analytics
Azure Information Protection	SQL Service	
Azure Security Center		

OK

S.no.	Subscription	Resource group	Location	Compliance %	GDPR Ready	Recommendation
1	87654321-5c41e7-9f39-e138c21c7ea1 (Contosa 4)			25 %	No	Recommendation
2	87654321-5c41e7-9f39-e138c21c7ea1 (Contosa 4)			25 %	No	Recommendation
3	87654321-5c41e7-9f39-e138c21c7ea1 (Contosa 4)	Central-US		25 % 75 %	No	Recommendation
4	87654321-5c41e7-9f39-e138c21c7ea1 (Contosa 4)	Api-Default-West-US	1 3	No Yes No No	25 % 75 %	No Recommendation
5	87654321-5c41e7-9f39-e138c21c7ea1 (Contosa 4)	azCMDDBDevNight	1 4	No Yes No No	25 % 75 %	No Recommendation
6	87654321-5c41e7-9f39-e138c21c7ea1 (Contosa 4)	BCP-PROD-RG	1 1	No Yes No No	25 % 75 %	No Recommendation

Navigation: Dashboard, Main Dashboard, Subscription, Focus Baseline, Usage Analytics, Billing Analytics, Security Analytics, Costing Analytics, Advisor Analytics, **GDPR Dashboard**, BackUp & Recovery, Cost & Utilization, Security & Compliance, Container Security, Application Migration, Settings

# Monitoring a GDPR baseline

☰
CloudSupervisor®
Contosa 4
🗨️
🔔
demo@unifycloud.com
👤

🌐 Azure Services With GDPR Mapping

Subscription : 87654321-5c41-41e7-9f39-E138c21c7ea1 > Resource Group : AzCMDDBDevNight

S.no.	Service Type	Total	Journey Stage			
			Discover	Manage	Protect	Report
	<input type="text" value=""/>		<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>
1	Redis Caches	4	No	Yes	No	No

🏠 Dashboard
   
📊 Cost & Utilization
   
🔒 Security & Compliance
   
📦 Container Security
   
🔄 Application Migration
   
⚙️ Settings

# Summary

- 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](http://www.cloudatlasinc.com) for additional information about our solutions.

