Compliance and Cloud: a Shared Responsibility

Sandra Miranda Ferreira
Chief Technology Officer – Microsoft Portugal
WHAT DOES GDPR MEAN FOR MY DATA?

- Stricter control on where personal data is stored and how it is used
- Better data governance for better transparency, recordkeeping, and reporting
- Improved data policies to provide control to data subjects and ensure lawful processing

Protecting customer privacy with GDPR
How can I get started?

1. Discover: Identify what personal data you have and where it resides
2. Manage: Govern how personal data is used and accessed
3. Protect: Establish security controls to prevent, detect, and respond to vulnerabilities & data breaches
4. Report: Keep required documentation, manage data requests and breach notifications
The major drivers of IT governance

- Keep risk at acceptable levels
- Maintain availability to systems and services
- Comply with relevant laws and regulation
- Protect customer and company data
Managing compliance is complex.

Managing compliance is increasingly difficult, due to the amount of standards and regulations and international differences.

Compliance is even more of a challenge for regulated industries such as healthcare or financial services.

Standards and regulations are constantly changing making it even more difficult for a business to keep abreast of electronic data handling laws.
WHAT ABOUT “CLOUD”?

A STANDARDIZED SERVICE DELIVERY MODEL WITH...

**On demand self-service**
Users can provision services on their own

**Resource pooling**
Multiple users and dynamic access to pooled resources

**Rapid elasticity**
Resources can expand or contract as quickly as they are used or freed

**Measured service**
Services are charged based on what is used
Hyper-scale Cloud

38
Azure regions

More than AWS and Google combined
LEADERSHIP IN COMPLIANCE

- Global requirements
- Local & regional compliance requirements
- Infrastructure investments
- Highly-regulated industries
- Future requirements
Compliance framework
We look for commonality in compliance controls and implement scalable solutions that either a customer can manage via Azure, or we can manage via internal tooling.

Our role in compliance engineering is to take these standards and actualize them to controls that Microsoft needs to implement.
Azure has the most comprehensive compliance coverage in the industry.
A two-way partnership with our customers

It’s more complex than just meeting a check list of standards and regulations.

Partnership between the customer who owns the data along with the legal obligations for the handling of the data...

...and the cloud vendor who acts as the data processor and must also handle the data in compliance with regulations.

Clearly defined roles and responsibilities are essential.
## Shared Responsibility

### Customer management of risk
Data Classification and data accountability

### Shared management of risk
Identity & access management | End Point Devices

### Provider management of risk
Physical | Networking

<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 &amp; end-point protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity &amp; 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 Infrastructure</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>
Compliance Reports
Audit and GRC assessment reports for Microsoft Cloud Services

aka.ms/stp

Third party independent audit and GRC assessment reports for Microsoft cloud services. Stay up to date on how Microsoft cloud services comply with global standards that matter to your organization.

**SOC Reports**  ISO Reports  FedRAMP  Assessment Reports

<table>
<thead>
<tr>
<th>Service Organization Controls (SOC) Audit assessment reports for Microsoft cloud services.</th>
<th>Description</th>
<th>Report Date</th>
</tr>
</thead>
</table>
Control Implementation and Testing Details

A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.

Control Implementation details

Microsoft develops, documents, and disseminates a security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The Microsoft Security Policy exists in order to provide Microsoft Services Staff and Contractor Staff with a current set of clear and concise Information Security Policies. These policies provide direction for the appropriate protection of the Microsoft Services. The Microsoft Security Policy has been created as a component of an overall Information Security Management System (ISMS) for the Microsoft Services. The Microsoft Security Policy has been reviewed, approved, and is endorsed by Microsoft Online Services management. Each management-level participant is responsible for understanding their role and distributing the policy to their respective team. The Microsoft Security Policy is intended for use by the Microsoft Services Staff for review. All Microsoft Services Staff are responsible for implementing the Microsoft Security Policy documents. All Microsoft Services Staff are required to be familiar with the Microsoft Security Policy. Should one of these parties not be familiar with the Microsoft Security Policy, they are encouraged to contact the assigned team lead to receive a copy of the Policy.

Testing performed to evaluate control effectiveness

Examined the Microsoft Office 365 Information Security Policy, dated October 30, 2014, to confirm that the document addresses purpose (Section 1.0), scope (Section 2.0), roles and responsibilities (Section 3.0), management commitment (Section 4.0 and Section 9.0), coordination among organizational entities (Section 6.0), and compliance (Section 5.0). The O365 Framework is designed to provide a common compliance baseline for all O365 product teams to follow; the SOPs create a mapping between the NIST assessment procedures and the Framework policy identifiers in order to provide an engineering specific starting point for teams to identify exactly what must be done in order to achieve compliance.

Interviewed O365 Foundation Senior Program Manager and O365 Foundation Program Manager. Lead on January 14, 2015 and determined that all information security program documentation, including both policy and procedures, is reviewed and updated no less than annually. Evidence of this was provided in the form of updated policy and procedures documentation and a demonstration of the SOP SharePoint repository used to manage and communicate the procedures.

Browse control set and audit findings directly in product
Microsoft’s commitment to compliance

- Lower costs for achieving compliance
- Assurance of adherence to international privacy and security standards
- Respect for the rules of highly regulated industries
- Decreased overall risk for your data and your business
Compliance is a Shared Responsibility

We are committing to GDPR compliance across our cloud services when enforcement begins on May 25, 2018.
GDPR RESOURCES

- Microsoft.com/GDPR
- Microsoft Online Services and GDPR
  - Microsoft Azure
  - Office and Office 365
  - Microsoft Dynamics 365
  - Enterprise Mobility Suite
  - Windows 10
  - SQL Server
Obrigada