Experts in navigating risk

Microsoft Security Summit

28 March 2017
KPMG is moving cyber to the heart of its business.

Johan Björk
Head of Information Protection and Business Resilience at KPMG Sweden

17 years in IT and dedicated to security for the last 11 year, changing perceived security into real security.

https://www.linkedin.com/in/johanbjork/
Agenda

1. Why GDPR matters for the cloud journey
2. Due diligence and review
3. Accurate technical and organisational measures
4. KPMG and Microsoft CTC
Why GDPR matters for the cloud journey

01 Accountability
Processing of personal data requires controller to be able to demonstrate compliance

02

03

04
Why GDPR matters for the cloud journey

01 Accountability
Processing of personal data requires controller to be able to demonstrate compliance

02 Security of the personal data
Limited transparency into provider practices

03

04
Why GDPR matters for the cloud journey

01 Accountability
Processing of personal data requires controller to be able to demonstrate compliance

02 Security of the personal data
Limited transparency into provider practices

03 Service add-ons
Controllers responsibility to select the applicable security add-on services

04
Why GDPR matters for the cloud journey

01
Accountability
Processing of personal data requires controller to be able to demonstrate compliance

02
Security of the personal data
Limited transparency into provider practices

03
Service add-ons
Controllers responsibility to select the applicable security add-on services

04
Enterprise risk management
GDPR needs to be embedded in current ERM or ISMS framework
Due diligence and assessment

Assess privacy impact and personal data type
Due diligence and assessment

Assess privacy impact and personal data type

Understand the services in scope
Due diligence and assessment

- Assess privacy impact and personal data type
- Understand the services in scope
- Review certification, location and agreement
Architecture and Data Segregation

The Covered Services are operated in a multitenant architecture that is designed to segregate and restrict Customer Data access to business needs. The architecture provides an effective logical data separation for different customers via customer-specific "Organization IDs" and allows the use of customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production. The specific infrastructure used to host Customer Data is described in the “Infrastructure and Sub-processors” documentation available here.

Certain customers may have the option to subscribe to Covered Services hosted on the infrastructure of a public cloud provider (“Public Cloud Option”). This infrastructure is described in the “Infrastructure and Sub-processors” documentation. For customers who elect the Public Cloud Option, this will mean the underlying physical infrastructure on which your Customer Data is stored will be with a public cloud provider for what is commonly referred to as Infrastructure as a Service, and the Covered Services will run on top of the public cloud provider. Unless otherwise noted in this documentation, customers who choose the Public Cloud Option will receive the same services, software functionality and operational processes as described here.
annual certification to the EU-U.S. Privacy Shield framework as administered by the U.S. Department of Commerce, as further described in our Privacy Shield Notice. The current certification is available at [https://www.privacyshield.gov/list](https://www.privacyshield.gov/list) by searching under “Salesforce.”

- **ISO 27001/27018 certification**: Salesforce operates an information security management system (ISMS) for the Covered Services in accordance with the ISO 27001 international standard and aligned to ISO 27018. Salesforce has achieved ISO 27001/27018 certification for its ISMS from an independent third party. The Salesforce ISO 27001/27018 Certificate and Statement of Applicability are available upon request from your organization’s Salesforce account executive. The current Statement of Applicability does not include the Quote-to-Cash Services as an in-scope product.

- **Service Organization Control (SOC) reports**: Salesforce’s information security control environment applicable to the Covered Services (except Quote-to-Cash Services) undergoes an independent evaluation in the form of SOC 1 (SSAE 16 / ISAE 3402), SOC 2 and SOC 3 audits. Salesforce’s most recent SOC 1 (SSAE 16 / ISAE 3402) and SOC 2 reports are available upon request from your organization’s Salesforce account executive.

- **TRUSTe Privacy Seal**: Salesforce has been awarded the TRUSTe Privacy Seal signifying that Salesforce’s Web Site Privacy Statement and associated practices related to certain of the Covered Services have been reviewed by TRUSTe for compliance with TRUSTe’s program requirements, including transparency, accountability, and choice regarding the collection and use of personal data.

- **Payment Card Industry (PCI)**: For the Covered Services (except Quote-to-Cash Services), Salesforce has obtained a signed Attestation of Compliance (“AoC”) demonstrating Level 1 compliance with the applicable Payment Card Industry Data Security Standard, as formulated by The Payment Card Industry Security Standards Council (“PCI DSS”) as a data storage entity or third party agent from an Qualified Security Assessor that is certified as such by The Payment Card Industry Security Standards Council. A copy of Salesforce’s AoC is available upon request from your organization’s Salesforce account executive. Customers must use either “Platform Encryption” for supported field types and file attachments or the “Classic Encryption” custom fields feature when storing personal account numbers (“PAN” or “credit card numbers”) to benefit from Salesforce’s PCI DSS AoC. Information about “Platform Encryption” and “Classic Encryption” is available in the Security Implementation Guide.

Additionally, the Covered Services undergo security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments, on at least an annual basis.
annual certification to the EU-U.S. Privacy Shield framework as administered by the U.S. Department of Commerce, as further described in our Privacy Shield Notice. The current certification is available at [https://www.privacyshield.gov/list](https://www.privacyshield.gov/list) by searching under “Salesforce.”

- **ISO 27001/27018 certification**: Salesforce operates an information security management system (ISMS) for the Covered Services in accordance with the ISO 27001 international standard and aligned to ISO 27018. Salesforce has achieved ISO 27001/27018 certification for its ISMS from an independent third party. The Salesforce ISO 27001/27018 Certificate and Statement of Applicability are available upon request from your organization’s Salesforce account executive. The current Statement of Applicability does not include the Quote-to-Cash Services as an in-scope product.

- **Service Organization Control (SOC) reports**: Salesforce’s information security control environment applicable to the Covered Services (except Quote-to-Cash Services) undergoes an independent evaluation in the form of SOC 1 (SSAE 16 / ISAE 3402), SOC 2 and [SOC 3](https://www.privacyshield.gov/list) audits. Salesforce’s most recent SOC 1 (SSAE 16 / ISAE 3402) and SOC 2 reports are available upon request from your organization’s Salesforce account executive.

- **TRUSTe Privacy Seal**: Salesforce has been awarded the [TRUSTe Privacy Seal](https://www.truste.org) signifying that Salesforce’s [Web Site Privacy Statement](https://www.salesforce.com) and associated practices related to certain of the Covered Services have been reviewed by TRUSTe for compliance with [TRUSTe’s program requirements](https://www.truste.org), including transparency, accountability, and choice regarding the collection and use of personal data.

- **Payment Card Industry (PCI)**: For the Covered Services (except Quote-to-Cash Services), Salesforce has obtained a signed Attestation of Compliance (“AoC”) demonstrating Level 1 compliance with the applicable Payment Card Industry Data Security Standard, as formulated by The Payment Card Industry Security Standards Council (“PCI DSS”) as a data storage entity or third party agent from an Qualified Security Assessor that is certified as such by The Payment Card Industry Security Standards Council. A copy of Salesforce’s AoC is available upon request from your organization’s Salesforce account executive. Customers must use either “Platform Encryption” for supported field types and file attachments or the “Classic Encryption” custom fields feature when storing personal account numbers (“PAN” or “credit card numbers”) to benefit from Salesforce’s PCI DSS AoC. Information about “Platform Encryption” and “Classic Encryption” is available in the [Security Implementation Guide](https://www.salesforce.com).

Additionally, the Covered Services undergo security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments, on at least an annual basis.
Disaster Recovery

Salesforce has disaster recovery plans in place and tests them at least once per year. The Covered Services utilize secondary facilities that are geographically diverse from their primary data centers, along with required hardware, software, and Internet connectivity, in the event Salesforce production facilities at the primary data centers were to be rendered unavailable.

The Covered Services’ disaster recovery plans currently have the following target recovery objectives: (a) restoration of the Covered Service within 12 hours after Salesforce’s declaration of a disaster; and (b) maximum Customer Data loss of 4 hours; excluding, however, a disaster or multiple disasters causing the compromise of both data centers at the same time, and excluding development and test bed environments, such as the Sandbox service.

Viruses

The Covered Services do not scan for viruses that could be included in attachments or other Customer Data uploaded into the Covered Services by a customer. Uploaded attachments, however, are not executed in the Covered Services and therefore will not damage or compromise the Covered Services by virtue of containing a virus.

Data Encryption

The Covered Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer’s network and the Covered Services, including 128-bit TLS Certificates and 2048-bit RSA public keys at a minimum. Additionally, Customer Data is encrypted during transmission between data centers for replication purposes.

Return of Customer Data

Within 30 days post contract termination, customers may request return of their respective Customer Data submitted to the Covered Services (to the extent such data has not been previously deleted by Customer). Salesforce shall provide such Customer Data via a downloadable file in comma separated value (.csv) format and attachments in their native format. Note that Customer Data your organization submits to the Analytics Cloud Services’ instance groups for analysis is derived from data contained in Salesforce and is only used for the purposes for which it was collected.
Disaster Recovery

Salesforce has disaster recovery plans in place and tests them at least once per year. The Covered Services utilize secondary facilities that are geographically diverse from their primary data centers, along with required hardware, software, and Internet connectivity, in the event Salesforce production facilities at the primary data centers were to be rendered unavailable.

The Covered Services’ disaster recovery plans currently have the following target recovery objectives: (a) restoration of the Covered Service within 12 hours after Salesforce’s declaration of a disaster; and (b) maximum Customer Data loss of 4 hours; excluding, however, a disaster or multiple disasters causing the compromise of both data centers at the same time, and excluding development and test bed environments, such as the Sandbox service.

Viruses

The Covered Services do not scan for viruses that could be included in attachments or other Customer Data uploaded into the Covered Services by a customer. Uploaded attachments, however, are not executed in the Covered Services and therefore will not damage or compromise the Covered Services by virtue of containing a virus.

Data Encryption

The Covered Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer’s network and the Covered Services, including 128-bit TLS Certificates and 2048-bit RSA public keys at a minimum. Additionally, Customer Data is encrypted during transmission between data centers for replication purposes.

Return of Customer Data

Within 30 days post contract termination, customers may request return of their respective Customer Data submitted to the Covered Services (to the extent such data has not been previously deleted by Customer). Salesforce shall provide such Customer Data via a downloadable file in comma separated value (.csv) format and attachments in their native format. Note that Customer Data your organization submits to the Analytics Cloud Services’ instance groups for analysis is derived from
Accurate technical and organisational measures

1

Threat modelling
Accurate technical and organisational measures

1
Threat modelling

2
Add applicable controls
Accurate technical and organisational measures

1. Threat modelling
2. Add applicable controls
3. Review and assess risk
Cloud Transformation & Compliance (CTC)

Enterprise Cloud Products Suite

Value Management, Risk & Transformation

Software

Platform

Infrastructure

© 2017 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.
# Cloud Transformation & Compliance (CTC)

<table>
<thead>
<tr>
<th>Focus</th>
<th>Offerings</th>
</tr>
</thead>
</table>
| Value          | 1. Vision and Cloud Business Case  
2. Suitability Assessment and Conceptual Architecture  
3. TOM Design  
4. Impact Assessment and Transformation Road Map |
| Risk           | 1. Cloud Governance, Risk, and Compliance Assessment  
2. Cloud Governance, Controls, and Compliance Design |
| Transformation | 1. Architecture  
2. Application Integration  
4. Information Management |

<table>
<thead>
<tr>
<th>Offerings</th>
</tr>
</thead>
</table>
| 1. Technology Business Management  
2. Workload Migration Factory and Tech Refresh  
3. IT Management Enablement and Automation  
4. Service Catalog and Provisioning  
5. Service Configuration, Integration and Monitoring  
6. Security and Resiliency Management |

<table>
<thead>
<tr>
<th>KPMG transformation journey</th>
</tr>
</thead>
</table>
| Strategy  
High-level design  
Detailed design  
Build  
Implement  
Improve |

**PORTFOLIO, PROGRAM, AND PROJECT MANAGEMENT**

**LEADERSHIP AND CHANGE**

**VALUE DELIVERY**

© 2017 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.
Tack!