





OBJECT MANAGEMENT GROUP

Addressing Data Residency Challenges

Webinar

April 14, 2016

Speakers

	Tracie Berardi	Sr. Marketing Manager, OMG Moderator
	Andrew Watson	Technical Director, OMG
	Claude Baudoin	Principal, cébé IT & Knowledge Management Energy Domain Consultant, OMG
	Denise Tessier J.D., CPCU, ARe, ARM-E	Regulatory Compliance Project Executive – Insurance IBM Global Technology Services Financial Services Center of Excellence

Introducing OMG



- **One of the most successful forums for creating open integration standards in the computer industry**
 - Middleware platforms (DDS, CORBA and related specs)
 - Modeling platforms (UML, BPMN, SysML and related work)
 - System Assurance (SACM, DAF for SSCD ...)
 - Vertical domain specifications (Finance, Healthcare, C4I, ...)
- **Member-controlled industrial consortium**
 - Both vendors and users
 - Not-for-profit
- **Adopted specifications are freely available to all**
 - Visit <http://www.omg.org>
- **Path to adoption by ISO and other standards bodies**

Worldwide Membership



ACORD	EDM Council	Microsoft	OSD	Sparx
Adaptive	EMC	Micro Focus	Penn Nat'l	State St
Adelard LLP	FICO	MID GmbH	PrismTech	Thales
Airbus Grp	FSTC/BITS	MITRE	PROSTEP AG	Thematix
Appian	Fujitsu	Mitsubishi	PTC	TIBCO
AT&T	Gen. Electric	Mphasis	PwC	Toshiba
BAE Systems	HPE	NASA	Remedy IT	Toyota
Bizagi	Honda	NARA	Rolls-Royce	Twin Oaks
Bloomberg	Huawei	NEC	RTI	Unisys
Boeing	IBM	No Magic	SAP	VDMbee
CA	KDM Analytic	Northrop	Selex ES	Visumpoint
Camunda	Lockheed	Oracle	Softeam	WebRatio
Eclipse Fndn.	MEGA	Orbus	Software AG	(200+ more)

Data Residency: Definition and Scope

- **In the OMG Data Residency Request for Information, we use the following definition of “data residency”**
 - *Issues and practices related to the location of data, movement of data across geographies and jurisdictions, and protection of that data against unintended access*
- **... and we clarify the scope:**
 - *This topic has a broader reach than just the protection of personally identifiable information (PII). It also concerns the right to move “sovereign” data, such as oil reserves data; international licensing of genomics data; distribution of biometrics data for security purposes; etc.*

Challenges: Example 1

■ Migration to the cloud

- Am I allowed to put my data in the cloud if it is going to be stored in another country, or if there is a *possibility* that the cloud provider might move it to another country later without my knowledge or consent?
- Regulations may be unclear
- Regulations may be used as a rationale to reject the cloud... even when they do not really exist (Mexico government example)
- Authorization may require high-level approval (Danish bank example)



Challenges: Example 2

■ Genomic data sets

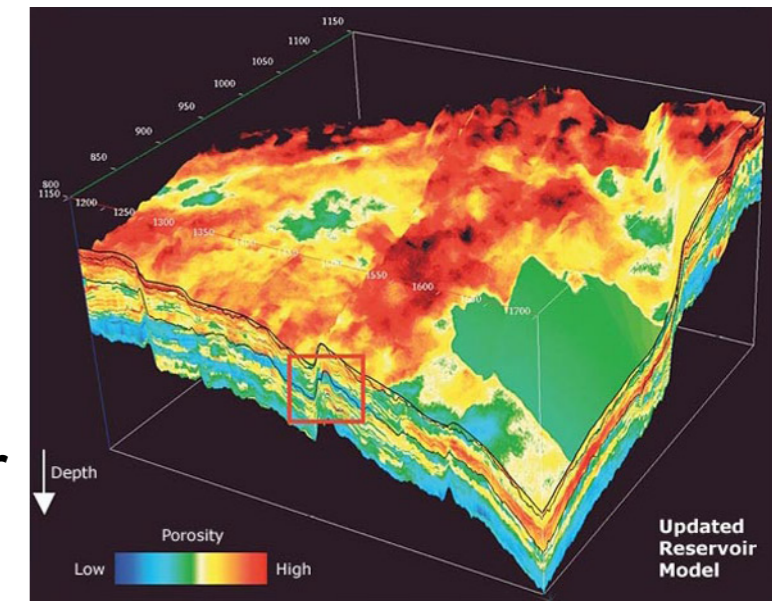
- Can I license a data set from another country to perform research on a larger sample?
- How do I prove to regulators that the data no longer contains personally identifiable information (PII)?



Challenges: Example 3

■ Processing data on petroleum reserves

- In countries with national companies, subsurface data is often considered a national asset
- Exploration is subcontracted to foreign companies
 - Can it remotely control an automated drilling operation from a monitoring center in another country?
 - Can it move data to a foreign location in order to do better analytics?
 - If it returns data interpreted in a center in another country, does it have to pay duties on the added value of those results?



Challenges: Example 4

■ Law enforcement vs. personal communication

- A US citizen is suspected of criminal activity
- Some evidence may reside in their e-mail stored in the cloud by a US provider
- However, the data is stored outside of the US, in a country with strong data protection laws
- Which law prevails? Is the provider “damned if they do, damned if they don’t” give the US government access to the data?



Reasons for Data Residency Regulation








- Residency laws are a kind of trade barrier that seek to impose location-specific conditions on global production, procurement, investment, and data flows.
- Designed to protect, favor, or stimulate domestic manufacturing industries, service providers, and/or intellectual property (IP) providers at the expense of foreign competitors, particularly those operating in innovative industries. IT services are a popular target.
- In some cases, data residency laws may also be driven by a governmental desire to increase access to its own citizen's records/information and / or exclude other countries from accessing such information.

Types of Residency Regulations

- Local IT infrastructure requirements
 - Designed to force companies to establish data centers and other infrastructure within the country
- Local data storage or local data residency laws
 - Compel companies to keep the data they collect within the territory of that country
- Either requirement may be applied at various levels of government
 - country, state, municipality
- Legal or compliance analysis may overlap into related areas such as Privacy and Data Protection Laws



Sample Country Localization Rules

	Country	Requirements	Stringency
	AUSTRALIA	Australia requires local data centers for the personally controlled e-health record system, also impacting insurers.	Limited
	CHINA	China law states that data generated within the country must be stored on servers within the country. Also there is a Bank of China sectoral regulation requiring banking data to be kept in country.	Serious
	CANADA	Several Canadian provinces prohibit data processors from using servers outside of the territory, particularly for municipalities and for financial services transactions	Limited
	INDIA	PROPOSED: Measures requiring companies to locate part of their IT infrastructure within the country to provide investigative agencies with ready access to encrypted data on their servers; that data of Indian citizens, government organizations and firms hosted on the servers of these companies not be moved out of the country. Failure to comply with this rule will be a criminal offence and company officials will face prosecution.	Proposed, not adopted
	RUSSIA	Enacted new laws effective 9/1/2015 mandating that personal data of Russian citizens be processed via servers located within the territory of Russia. Previously adopted banking legislation requiring infrastructure necessary to core payment processing services be located on the territory of the Federation.	Serious

Regional regulations, trade pacts, and national laws

- **European Union**
 - Data can flow within union members
 - EU-US “privacy shield” issue pending resolution
- **APEC** (Asia-Pacific Economic Cooperation)
- **OECD** (Organization for Economic Co-operation and Development)
- **TTIP** (Transatlantic Trade and Investment Partnership)
- **NAFTA** (North American Free Trade Agreement)
 - Future Information Technology, Privacy and Data Protection Amendment
 - Canada, U.S. and Mexico



OMG's Data Residency Roadmap

Data Residency Working Group
(started June 2015)

Request for Information
(issued January 2016, deadline 9 May 2016)

Analysis of Responses → Discussion paper
(end of 2016)

Determine Potential Useful Standards
(end of 2016)

Request(s) for Proposal
(2017+)

RFI Content – Demographic Questions

1. Nature of the responding organization
2. Industry sector
3. Cloud user, provider, both, neither?
4. Storing/moving data across boundaries?
5. Countries of presence and activity
6. Nature of the data handled
7. Role in charge of data residency policies
8. Other people involved in data location
9. *Requirement for anonymization of response?*

RFI Content – Substantial Questions

10. Respondent's definition of data residency
11. Official or individual definition?
12. Assessment of risk level related to data residency
13. Examples of types of data at risk now
14. Evolution of these risks in the future
15. Regulations the respondent is aware of
16. Known incidents
17. What can OMG do to help?
18. Non-OMG standards to consider
19. Provide any additional relevant documents
20. References and web links

Summary

- **Data residency is a serious challenge for suppliers as well as users**
 - Can (and already does) hurt the ability to do business
- **It may well get worse before it gets better**
- **Organizations need to learn about it and develop business and technical approaches**
- **OMG is looking into what standards may help**
 - Metadata describing data location constraints?
 - Formal description of data residency laws and regulations?
- **Call to action**
 - Answer the RFI at <http://www.omg.org/cgi-bin/doc?mars/15-12-07>
 - Participate in OMG Data Residency Working Group