OBJECT MANAGEMENT GROUP®

Where's My Data? Managing the Data Residency Challenge

Claude Baudoin & Geoff Rayner

27 February 2018

Speakers

Tracie Berardi Director of Program Management, OMG
Program Manager, Cloud Standards Customer Council
Moderator
tracie@omg.org

Claude Baudoin Principal, cébé IT & Knowledge Management
Steering Committee member, Cloud Standards Customer Council
cbaudoin@cebe-itkm.com

Geoff Rayner CEO, Data Advantage Group
grayner@dag.com

Topics Covered in this Webinar

- Data Residency definition
- History of OMG's work on data residency
- Types of information that pose risks
- Nature of the risks – examples
- Laws and regulations around the world
- Potential applicable standards
- OMG Discussion Paper
- OMG Data Residency Maturity Model (DRMM) 

- How to contribute

Data Residency: Definition

"Data residency is the set of issues and practices related to the location of data and metadata, the movement of (meta)data across geographies and jurisdictions, and the protection of that (meta)data against unintended access and other location-related risks."

- Scope
  - Not just about the protection of personally identifiable information (PII)
  - 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.

OMG's Work on Data Residency

- March 2015: initial request from an OMG member
- June 2015: first OMG Data Residency WG meeting (Berlin)
- Q4 2015: Prepared and issued an RFI
- Q2 2016: Processed RFI results, decided to create a discussion paper as first deliverable
- Q4 2016: Drafted discussion paper, agreed to collaborate with CSCC and issue two separate but almost identical papers
- Q1 2017: Collected contributions, edited paper, agreement to release
- Q2 2017: Create CSCC companion white paper, press releases, webinar
- June-Dec. 2017: Successive tutorials, created and released a maturity model, discussed standards roadmap

Sources of Risk

- Multiple laws and regulations restrict what an organization can do with certain types of data, or potentially *prevent* its protection:
  - Personally identifiable information (PII)
  - Patient health information (PHI)
  - Proprietary corporate information
  - Communications (e-mail, etc.)
  - Government information (incl. military)
  - Information subject to trade controls and embargoes
  - Information on natural resources
  - Banking records
  - Other regulated data, e.g., “sovereign” data

Sources of Risk (cont.)

- Owners of such data may:
  - Relocate this data *intentionally*, for convenience or cost reduction
    - Data center consolidation and managed hosting
    - Centralized employee or customer database
    - Business process outsourcing
    - Helpdesk outsourcing
  - Be *unaware* of its location
    - Cloud service optimization by the provider
    - IoT data collection
- Acquisitions and expansion to new countries change the risk
- The Internet of Things exacerbates the challenge

Nature of the Risks

- Difficulty of providing IT services across borders from few locations
- Higher cost for customers (less competition for local services)
- Inability to consolidate operations
- Inability to provide shared employee services
- Need for multiple local IT operations teams (skills and cost issues)
- Limitations in backup locations
- Restrictions against strong data encryption
- Legal exposure
- Conflict with authorities
- Public mistrust

Data Residency Laws and Regulations

- Multiple, inconsistent, overlapping, and still evolving laws and regulations around the world
- Range from non-existent to severe
- Sometimes (but not always) apply to government data / public records, not to private companies' data
- The European Union's General Data Protection Regulation (GDPR), in effect from 25 May 2018, is among the most comprehensive
- Multiple motivations behind the laws:
  - Protecting the privacy of citizens
  - Enabling police and tax authorities to inspect data
  - Protectionism – force companies to create domestic facilities
  - Monetize the flow of data

A Proliferation of Laws

	Country	Requirements	Stringency
	AUSTRALIA	Australia requires local data centers for the personally controlled e-health record system, impacting insurers.	Limited
	CHINA	China law states t stored on servers China sectoral reg country.	
	CANADA	Several Canadian servers outside of for financial servic	
	DENMARK	Denmark introduc municipalities from located in-country	
	GREECE	"Data generated a within the Greek te territory." The Euro Greece as inconsi remains in effect.	
	INDIA	PROPOSED: Mea their IT infrastructu agencies with reac that data of Indian hosted on the serv the country. Failur offence and comp	

	Country	Requirements	Stringency
	INDONESIA	Regulations mandate all data carriers, including foreign banks operating in Indonesia, to establish local data centers. Banks may have limited exception with approval from the BI/OJK, under certain circumstances.	Serious
	KOREA (SOUTH)	Banking data mu PROPOSED: reg maintain servers restrict transfers employees) outsi	
	MALAYSIA	Enacted the Pers data generated w country, althoug necessary to effe	
	NIGERIA	• Information T 2013 require • Bans the pro technological locally made • Banking Guic transactions prohibit routi • The Cybercri Nigerian legis	
	NORWAY	PROPOSED in 2 services unless t TBD.	

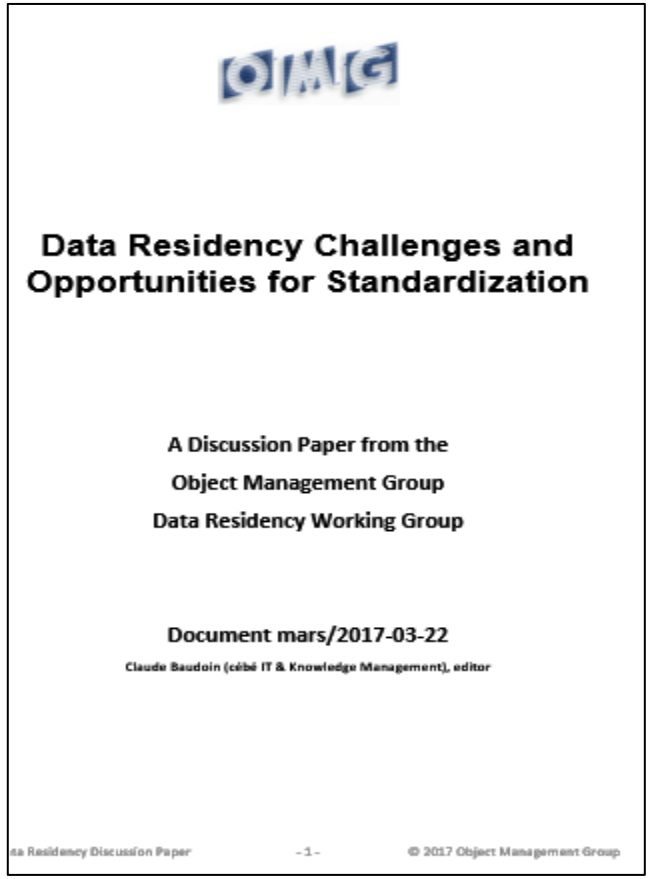
	Country	Requirements	Stringency
	RUSSIA	Enacted new laws effective 9/1/2015 mandating that personal data of Russian citizens be processed via servers located within the territory of Russia. Previously adopted banking legislation requiring infrastructure necessary to core payment processing services be located on the territory of the Federation.	Serious
	TURKEY	Per U.S. Department of State website (May 2015): "Turkey doesn't require local data centers or servers. However, the government is exploring whether or not to require data localization. After the June 2015 elections, localization requirements may be pushed more aggressively."	Proposed
	UKRAINE	PROPOSED: Banking laws/regulations that would establish a domestic monopoly for processing domestic payment transactions and exclude foreign networks from providing processing services.	Proposed
	VIETNAM	Mandatory for every online service provider in country to keep a copy of virtually all Vietnamese data on a local server, so national authorities can access, if needed.	Limited
	VENEZUELA	Banking requirements: local data server requirements due to currency control for debit transactions. Venezuela has adopted a law that effectively requires in-country processing of domestic payment transactions.	Serious

Potential Useful Standards

- There is currently no standard that deals specifically with data residency
- Data residency is related to the security and privacy aspects of
  - Several NIST publications (800-144, 500-299, 1500)
  - Several ISO/IEC standards (27001, 27017, 27018)
  - NIST Big Data Standard, http://fedscoop.com/nist-big-data-framework
  - The work of the CSA's International Standardization Council (ISC)
  - Work being considered in ISO/IEC JTC 1/SC 38
  - The "Voluntary Data Protection Code" of CISPE (Cloud Infrastructure Service Providers in Europe)

OMG's First Discussion Paper

- Two very close versions (OMG and CSCC)

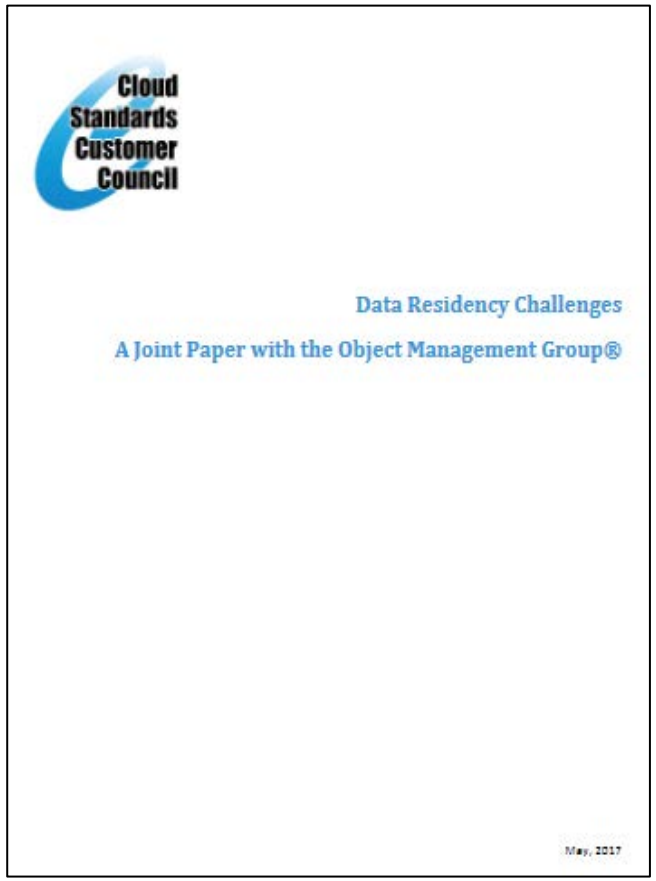


Data Residency Challenges and Opportunities for Standardization

A Discussion Paper from the
Object Management Group
Data Residency Working Group

Document mars/2017-03-22

Claude Baudoin (cébé IT & Knowledge Management), editor



Cloud Standards Customer Council

Data Residency Challenges

A Joint Paper with the Object Management Group®

May, 2017

The Data Residency Maturity Model (DRMM)

- Issued by OMG in December 2017 as a second "discussion paper"
- Structured in a similar manner to the SEI CMM for software engineering (1990)
- 5 levels and 20 "key process areas" that need to be put in place to "climb" to higher levels of maturity

Level	SEI CMM Name	Definition (under construction)	Key Process Areas
5	Optimizing	There is continuous monitoring and improvement of data residency policies, procedures and implementation	● Active monitoring and auditing of data location, transfer, and remote access ● Regular review of changes in business, data content, technology, laws and regulations ● Formal process to evolve policies, procedures, practices and technology ● Formal process to review all incidents and take corrective action
4	Managed	Active management takes place at all levels of the organization	● Executive accountability ● Governance (e.g., steering committee) ● Assign roles and responsibilities for DR policy and implementation ● Formal policies ● Data storage location assignment is part of information modeling ● Logging / audit trail of data creation, movement, access right changes ● Formal program of employee training
3	Defined	Policies, procedures, practices are documented and institutionalized, and data location impact is formally documented	● Active executive involvement ● Formally documented processes ● Taxonomy of sensitive data ● Informal training resources ● People are formally assigned to \data owner/steward/custodian roles
2	Repeatable	The organization performs on the basis of human knowledge, informally shared	● Executive awareness (e.g., evidenced by a letter from each C-level stakeholder stating their belief in the importance of the issue) ● Informal practices and guidelines to identify and locate data ● Employees know who to go to in order to arbitrate a d.r. question ● People act informally in roles of data owners/steward/custodians
1	Initial	None of above practices exist	

How to Contribute

- Participate in OMG's Data Residency Working Group
- Review the existing discussion papers and provide comments
  - http://www.omg.org/cgi-bin/doc?mars/17-03-22.pdf ("Challenges and Opportunities" paper)
  - http://www.omg.org/cgi-bin/doc?mars/17-12-18.pdf (DRMM)
- Consider adopting the DRMM
  - OMG is interested in partnering with organizations that would want to "adopt and adapt" the DRMM and give it broader recognition
- Suggest applicable standards – and if you work in standards group on security and privacy, give them input about data residency issues
- Our current intent
  - Coordinate with other OMG groups working on Data Provenance & Pedigree and on Data Tagging & Labeling – seek a unified "data governance" approach
  - Develop a standard to represent the various data residency laws and regulations in a uniform formal manner

Discussion

- Thanks for your attention
- Please ask questions using the BrightTalk interface
- Ask to be added to our mailing list
  - Send an e-mail to request@omg.org and ask to be added to the "dataresidency" list
- Participate in our next meetings
  - Reston, Va., March 20, 2018
  - Boston, Mass., week of June 18-22
  - Ottawa, Ont., Canada, week of Sept. 24-28 (2-day event on various information governance and security topics for the Canadian government)
- Contact Tracie Berardi, tracie@omg.org, for additional questions or comments