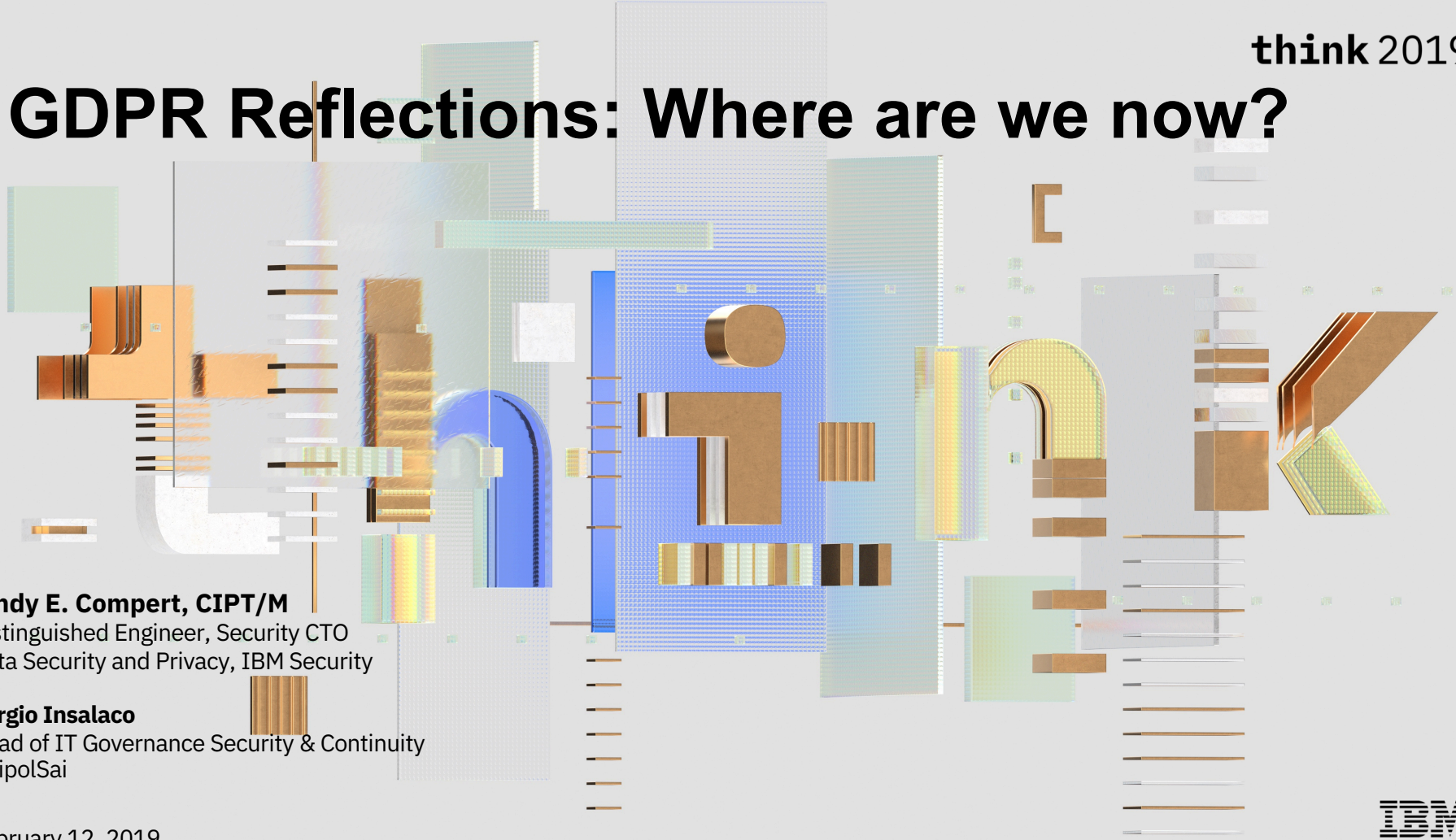
think 2019

GDPR Reflections: Where are we now?



Cindy E. Compert, CIPT/M
Distinguished Engineer, Security CTO
Data Security and Privacy, IBM Security

Sergio Insalaco
Head of IT Governance Security & Continuity
UnipolSai

February 12, 2019

IBM

Disclaimer

Notice: Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.

Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.

The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

None of the statements contained herein constitutes legal advice – it is process advice only.

Learn more about IBM's own GDPR readiness journey and our GDPR capabilities and offerings to support your compliance journey here.

Contents

Privacy Goes Public

A Tale of Three Animals

Hare

Rush to implement

Tortoise

Slow and steady

Ostrich

Wait and see

By the numbers..

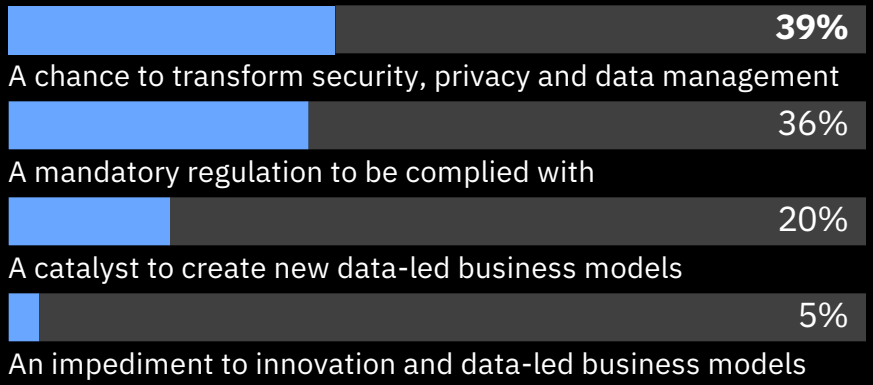
€50

91

59,000

GDPR – Bane or Boon?

Most respondents think GDPR can help them transform their organization – it is not just a mandatory regulation



Source: 2018 IBM Institute for Business Value Study

Where respondents are focused, they are also struggling

Top GDPR priorities / struggles	Priority	Struggle	
Performing data discovery and ensuring data accuracy	1	1	Performing data discovery and ensuring data accuracy
Complying with data processing principles	2	1	Complying with data processing principles
Developing / updating privacy policies and notices	2	3	Developing / updating privacy policies and notices
Establishing a Data Protection Officer	4	4	Getting consent from data subjects
Getting consent from data subjects	5	5	Establishing a Data Protection Officer

Note: Respondents were asked to rank their top three focus areas and struggles from a list of 11 different GDPR preparation components
Source: 2018 IBM Institute for Business Value Study

The GDPR (and Privacy) Thoroughbred

The evolution of modern privacy readiness and controls is based on common privacy principles and practices from GDPR

- Cindy Compert

IBM’s overall GDPR framework: Five phases to readiness

Phase	Assess	Design	Transform	Operate	Conform
Activity	• Conduct GDPR risk and privacy assessments across governance, people, processes, data, security • Develop GDPR readiness roadmap • Identify and map personal data	• Design governance training, communication and processes standards • Design privacy, data management and security management standards	• Develop and embed procedures, processes, and tools • Deliver GDPR training • Develop and embed standards using Privacy by Design, Security by Design • Detailed data discovery	• Execute relevant business processes • Monitor security and privacy using TOMs • Manage consent and data subject access rights	• Monitor, assess, audit, report and evaluate adherence to GDPR standards
Outcome	**Assessments and roadmap**	**Defined implementation plan**	**Process enhancements completed**	**Operational framework in place**	**Ongoing monitoring and reporting**
	Identify GDPR impact and plan Technical and Organisational Measures (TOM**s**)	Includes data protection controls, processes and solutions to be implemented.	TOMs in place: personal data discovery, classification and governance in place	Begin the new GDPR ready way of working	Monitor TOMs execution; deliver compliance evidence to internal and external

IBM PROPRIETARY

Common Practices: What companies can be doing to prepare (1 of 2)

Understand the obligations

Become familiar with the requirements and monitor the development of implementation guidance

Create a cross-functional privacy team

Ensure that all aspects of the business that are impacted are part of the development and implementation of any changes

Appoint a Data Protection Officer or equivalent

Create a structured privacy office & appoint, if required, a data protection officer (DPO) who has expert knowledge on data protection law

Know what data is stored and where it is located

Conduct a data inventory and mapping initiative to assist in understanding and evaluating the operational and technological changes required for compliance

Review privacy policies and statements

Confirm privacy notices are presented in clear and plain language, are transparent, and are easily accessible to data subjects

Review customer consent and choice mechanisms

Ensure that the appropriate consent and choice mechanisms are in place and/or are updated to meet the new consent requirements and to easily facilitate customer choice

Review processes addressing data subjects' access, correction and erasure requests

Confirm that the operational and technical measures are in place to support these requests

Review data retention schedules

Confirm data is only held for as long as there is a legitimate business need or as may otherwise required by law

Limited on time or resources? These are good starting point activities.

Common Practices: What companies can be doing to prepare (2 of 2)

Document privacy compliance activities

Adequately document all processing operations involving personal data through the use of Data Protection Impact Assessments (DPIAs)

Review cross-border transfers of personal data

Confirm there is a legitimate basis for transferring data to other jurisdictions

Implement and document appropriate security measures

Provide technical, physical and administrative security measures 'appropriate' to the processing risks (TOMs)

Train employees

Ensure employees are educated, at least annually, on the requirements and their obligations with respect to data protection

Develop audit capabilities and processes

Establish a robust audit plan and process to monitor ongoing conformance and to mitigate risk, both internally and for processors

Implement a Privacy (and Security) by Design approach to new systems and services

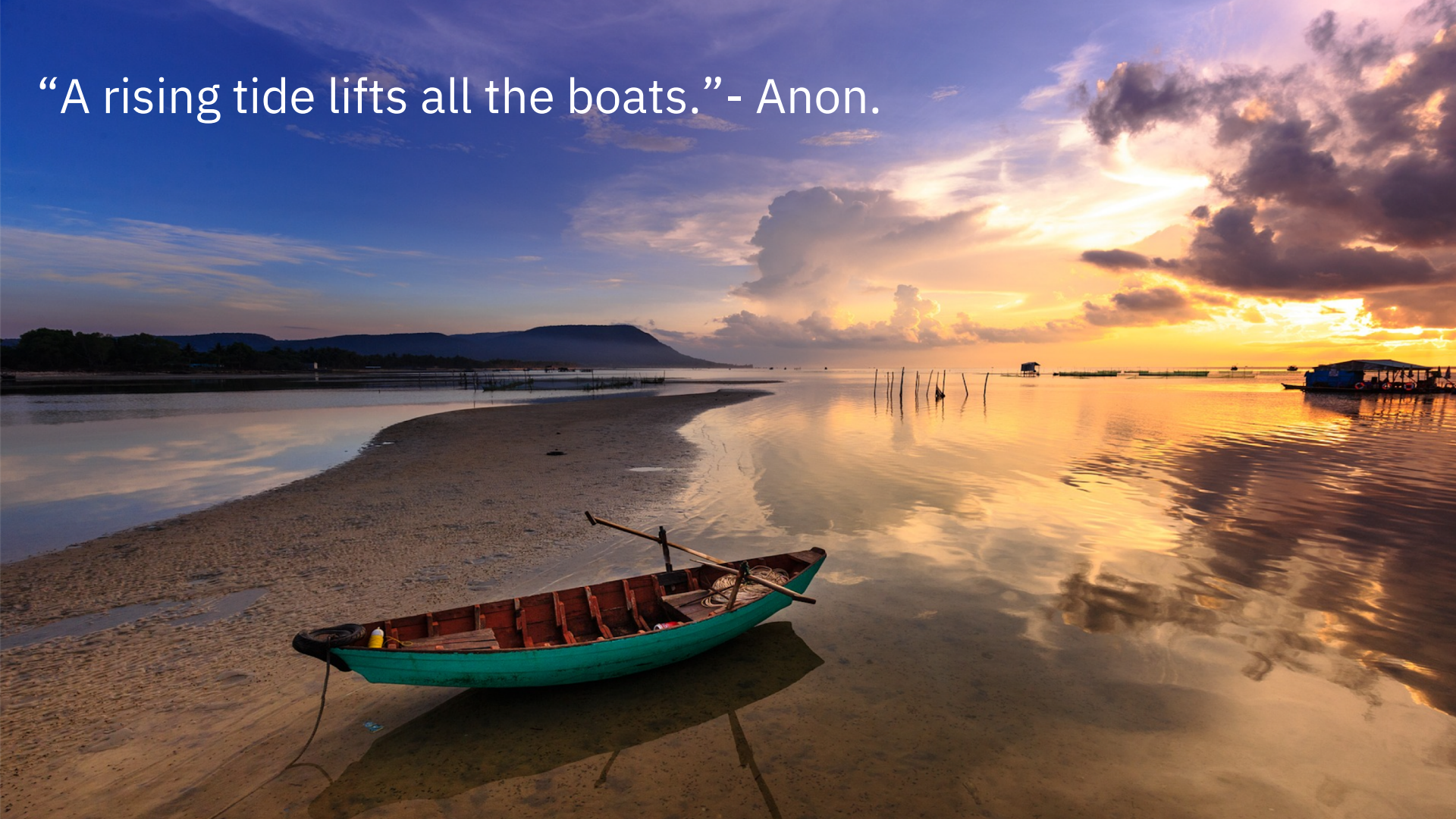
Create a Privacy by Design framework to ensure privacy requirements are embedded, by default and design, from the very outset of the development of new products, systems & services

Create breach response and notification protocols

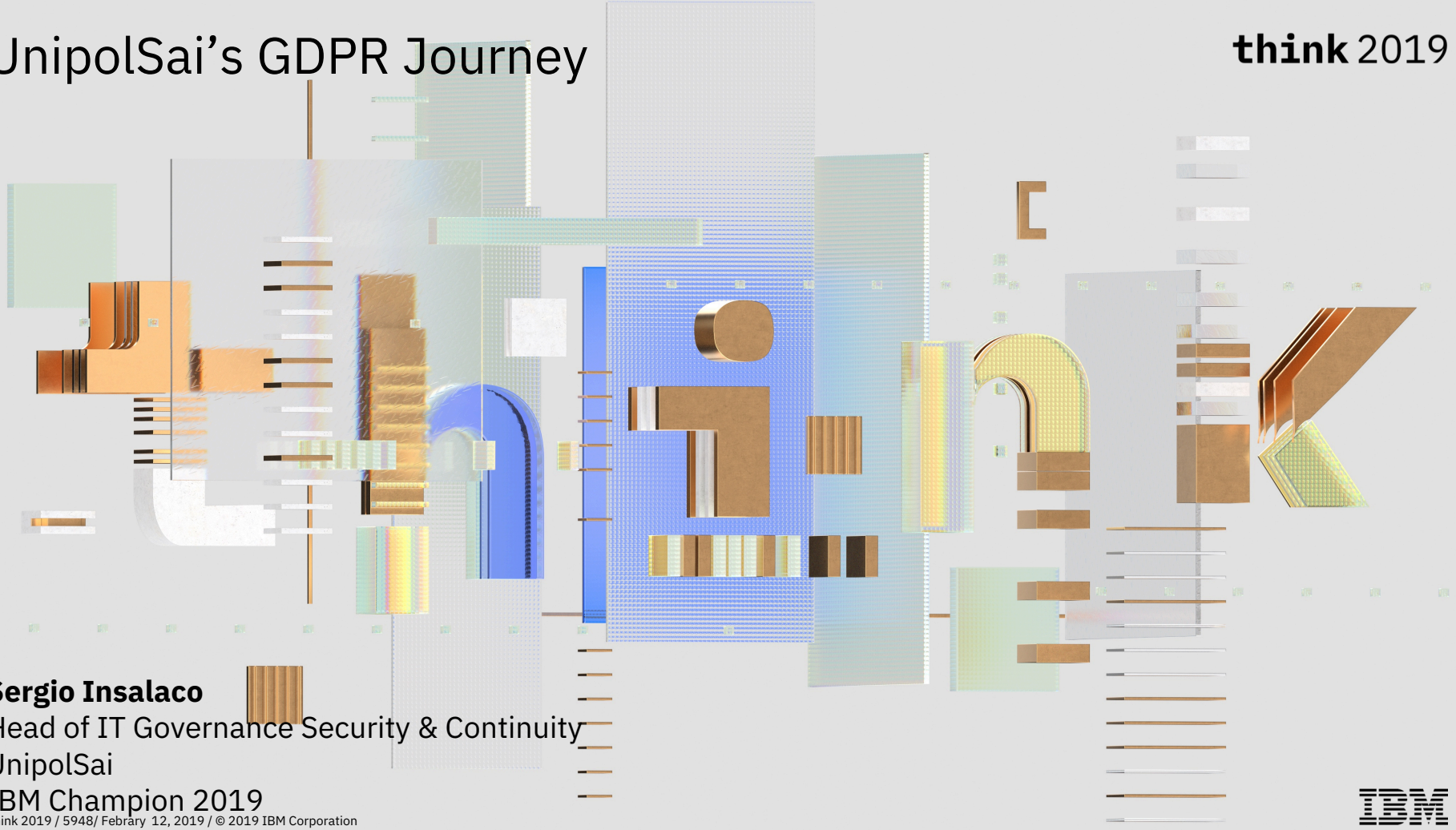
Implement data breach investigation, containment and response processes and procedures, and be sure to be able to test their effectiveness

Obtain executive sponsorship and budgets to support the changes!

Limited on time or resources? These are good starting point activities.


“A rising tide lifts all the boats.”- Anon.

UnipolSai's GDPR Journey



Sergio Insalaco
Head of IT Governance Security & Continuity
UnipolSai
IBM Champion 2019

About UnipolSai

- Italian Insurance Company leader in Life, Non-Life and motor vehicle TPL (third-party liability)
- Direct insurance income of €12.2 billion
- Largest agency network in Italy: over 10+ million customers, 2,700 insurance agencies and 6,000 sub-agencies
- IT divisions organized by business verticals. IT security, technological infrastructures and architectural choices centrally coordinated from Group IT Services Dept.
- IT Infrastructure includes: Z14 IBM mainframes, 6,000 Wintel and Unix / Linux servers, mostly virtual, and a Big Data Hub

http://www.unipolsai.com/

UnipolSai's GDPR Journey: the Enterprise roadmap

PROJECT MANAGEMENT

PHASE 1

- **Understand** the obligations
- Create a **cross-functional enterprise team** (Legal, HR/Organization, Business, IT)
- Obtain executive **sponsorship and budgets** to support the changes
- **Kick off** / start the project tasks

PHASE 2

- **Data inventory** and **mapping**
- GDPR-focused **IT Risk Analysis**
- Review **privacy policies and statements**
- Review **customer consent and choice mechanisms**
- Create **breach response** and **notification protocols**
- Review processes addressing **data subjects' access**, correction and **erasure requests**
- Appoint a **Data Protection Officer**

PHASE 3

- Review **data retention schedules**
- Review **third party contracts** involving personal data
- Implement a **Data Protection by Design / by Default approach**
- **Train** employees
- **Develop audit capabilities** and processes
- Continuous improvement….

- Implement / Enhance appropriate **security measures**
- **Document** privacy compliance activities

UnipolSai ASSICURAZIONI

UnipolSai's GDPR Journey: focus on IBM Guardium project

IBM Security Guardium is a comprehensive data protection platform that enables security teams to automatically analyze what is happening in sensitive-data environments to help minimize risk, protect sensitive data from internal and external threats and seamlessly adapt to IT changes that may impact data security

Solution evaluation and design		*Solution implementation*		*Solution extension*
Q4 2017	Jan 2018	Step 1 (2018Q1)	May 25th 2018	Extension
•Solution evaluation •HW procurement	•Kick-off •Solution design •Scope definition	•Agents deployment •DB Activity Monitoring •Data Discovery •Policies and reports design	•Machine learning •DB Firewall •VA •**GDPR compliance of critical processes**	•Scope extension to less critical systems •Extension to security controls •Continuous improvement

UnipolSai ASSICURAZIONI

Guardium GDPR Project Objectives

- Acquire knowledge and control of where sensitive data are stored and automate continuous update of the “map”
- Continuously monitor data access and track who is accessing sensible data
- Proactively uncover vulnerabilities and risks
- Rapidly respond to potential security threats
- Deploy a solution quickly that could be highly effective and easily manageable

The challenge:
- meet the GDPR requirements
- with a very tight project timeline
- in an heterogenous environment

UnipolSai ASSICURAZIONI

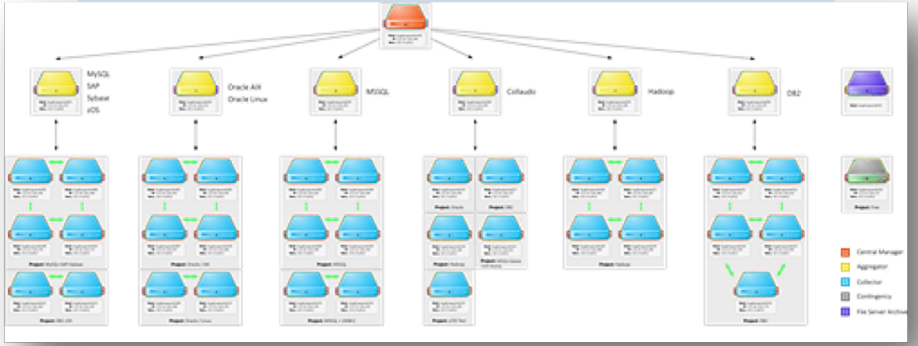
Functional Requirements

- Coverage of a wide range of technologies with one solution: IBM Z, distributed environments, SAP4Hana and Hadoop/Cloudera.
- Wide coverage of GDPR requirements
- Availability of a GDPR-oriented approach, with a proven guideline to compliance path → GDPR Accelerator!
- Data discovery and data classification for GDPR sensitive information
- Implement security measure beyond GDPR → machine learning and behavioral analysis to identify threats and misuse
- Low impact on systems' and DBMS' performance

Implementation Architecture

IBM Guardium®

- Auditing
- Monitor & Alerting
- Discovery
- Hardening
- DB Firewall
- Investigation
- Machine Learning
- SIEM



3-TIER ARCHITECTURE ON **HYPER-CONVERGENCE** INFRASTRUCTURE

TECHNOLOGY **DEDICATED POLICIES AND CLUSTERS**

QA DEDICATED APPLIANCES

41 APPLIANCES

150 DB SERVERS

480 DATABASES

UnipolSai ASSICURAZIONI

How we used the GDPR Accelerator

GDPR Accelerator was a key factor in the decision and proved to be key to success. It provided:

- Immediate confidence to top management that we could achieve goals with a very time constrained project
- Immediate ramp-up to project's short term goal to identify and classify data in scope of GDPR (Data Discovery)
- Quick start using pre-defined policies to immediately track activities needed for GDPR compliance
- Reports and documentation needed to give evidence of project advancement, adherence to compliance process, identification of gaps to trigger remediation
- A great benefit in reducing the impact on both the timeline and the effort (internal and system integrator), thus providing an additional cost saving for the project

UnipolSai ASSICURAZIONI

Compliance and Security Results: GDPR Obligations to Guardium functionalities

General Data Protection Regulation

- Articles 5, 24 "Accountability"
- Article 25 "Data Protection by Design and by Default"
- Articles 12-20 "EU Citizen Rights"
- Articles 5-8 "Lawfulness and Consent"
- Articles 5, 24, 32-34 "Security of Personal Data"

Monitor and audit
- Data Activity Monitoring
- Real-time Alerting
- Threshold Alerting
- Baseline Alerting
- Compliance Reporting
- Compliance Workflow
- User Identification
- Security Integrations

Enforce and protect
- Access Control
- Data and Query Masking
- User Quarantine

Asses and harden
- Vulnerability Assessments
- Configuration Changes
- Entitlement Reporting

Discover and classify
- Discovery of Data Sources
- Classify Sensitive Data
- Enterprise Integration

Guardium

Other results and ROI

Architecture: Using **single console for both mainframe and distributed** environments **reduces admin costs** of the complex UnipolSai infrastructure.

Performance: Optimization of data security architecture **enables speed and flexibility** - **No impact on database performance** as all processing is done on Guardium infrastructure

Reports: Built-in and *ad hoc* reports **monitor and track compliance with GDPR** as well as target security KPIs. Act on remediation for increased risk indicators

Return of Investment - ROI:

- Leveraging Guardium features helped **reduce GDPR Compliance Project cost and implementation time**.
- Using Hyper-Convergence architecture enabled UnipolSai to **reduce implementation and maintenance costs** further and increase capacity with limited expenditures.
- **Additional savings** are expected in ongoing compliance and improved security integration.

Best Practices

- Have a clear understanding of GDPR and the data processing in your company to define how to address the challenge.
- Define a roadmap and the goals to reach. Accelerator helps in identifying what can be achieved in the short term.
- Use the Accelerator to prove to Management what can be ‘easily’ accomplished, to reach quick wins and to speed up early deployment.
- Start by assessing where your data is, and start a continuous cycle to monitor activities and posture.
- Act on security alerts and threats detected; identify gaps and remediate to stay compliant
- Make Guardium part of your GDPR and Security processes and extend its usage beyond GDPR

Best Practices


Thank you

How Will You Build Trust?

https://www.ibm.com/legal/us/en/copytrade.shtml

IBM’s statements regarding its plans, directions, and intent are subject to change or withdrawal without notice and at IBM’s sole discretion.

Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.

The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user’s job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

Notices and disclaimers

© 2018 International Business Machines Corporation. No part of this document may be reproduced or transmitted in any form without written permission from IBM.

U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed "as is" without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.

IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply."

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

Notices and disclaimers continued

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.**

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

IBM, the IBM logo, ibm.com and [names of other referenced IBM products and services used in the presentation] are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: .