Privacy?
What Now and What's Next?

Richard Hogg
Global Privacy Compliance Guru, IBM

rghogg@us.ibm.com
Abstract

• We're nearly a year into GDPR - What happened? Were you ready? What's next?
• Next up includes California's CCPA and Brazil's LGPD coming in 2020 - are you ready?
• Where else is there a rising tide around data privacy and protection and how does that sync with information governance?
• What can and should you do to raise your readiness and accelerate your journey to compliance? What have large organizations done?
Notices and disclaimers

- 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: [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

- **GDPR 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.
€50 million
The executive European Commission reported on the number of complaints filed with EU countries since GDPR went live.

95,000
It’s Mostly Quiet On The GDPR Front — But This Is Not The Time For Complacency

Enza Iannopolo, Senior Analyst

4-5 minutes

So where are all the GDPR enforcement actions? The General Data Protection Regulation (GDPR) entered into force at the end of May 2018, giving unprecedented powers to regulators. From ongoing regulatory audits to hefty fines and a range of new privacy requirements, the GDPR is the most dramatic change in data protection and governance in the last 20 years. Some firms are still completing their readiness plans, others are just waiting to see what happens next. and many are wondering why regulators have been so
Growing global privacy regulations

With many similarities at the core but different duties across regulations, whatever the regulation, our capabilities can help in readiness.

88%
Spent > $1 M

40%
Spent > $10 M

$78B
U.S. costs so far
Brazil LGPD vs GDPR

**LGPD**
- **Scope**: will have transversal, multi-sectoral application to all sectors of the economy, both public and private, online and offline. With few exceptions;
- **Penalties**: Up to 2% Brazilian revenue up to fifty million Reais plus daily fines
- **Who**: Any data subjects in Brazil, branches in Brazil offering goods/services in country
- **What**: Personal including Sensitive Personal Data w differing Legal Bases (10)
- **Processing**: Requires entities to have a lawful basis for processing information if not seeking subjects’ consent
- **Data Requests**: Complete in 15 days
- **Execution**: International data transfers w consent, Breach Notif.

**GDPR**
- **Scope**: Any Business processing EU data-subjects personal data anywhere in the world; & **Opt-In without charge**
- **Penalties**: Up to 4% Global Revenue or EU 20M
- **Who**: Data Subject, a Natural Living Person in Europe
- **What**: Personal Data and Sensitive across 6 Legal Bases
- **Processing**: Requires entities to have a lawful basis for processing information if not seeking subjects’ consent
- **Data Requests**: Complete in 30 days
- **Execution**: International data transfers, Breach Notif.
California CCPA

- **Goes live** Jan 2020, **enforcement** expected from July 2020
  - Expect further regulatory amendments through 2019 that could affect those dates and scope
- **Scope** - Businesses with more than $25M revenue, who trade in data of more than 50K persons or derive more than 50% revenue from selling personal data; & **opt-out with charges**
- **Penalties**: $7,500 per violation via CA attorney general
- **Who**: California resident consumers, their households & devices; or any CA company or organization entity, requests to complete in 45 days
  - With current **12 month lookback requirement** from Jan 2019
- **Disclosures**: Provide clear link on your homepage & app titled “Do not sell my personal information,” to consumer options to opt-out

[https://ibm.co/GetCCPAPre](https://ibm.co/GetCCPAPre)
Getting ever more Complicated, N.A. Privacy Regulations continue to evolve weekly

Do you also do business in?

- **New York** went live Sept 1, 2018 with 5 new requirements included in the New York State Department of Financial Services’ (DFS) Cybersecurity Regulation effecting – (1) audit trails, (2) application security, (3) data disposal requirements, (4) monitoring authorized users’ activity, and (5) encryption of nonpublic information

- **Colorado** signed a new bill in June around personal data of Colorado residents, one of the strictest state-based privacy and data breach laws in the US, effective Sept 1 2018

- **Vermont** new state regs on registering all those holding info on state residents

- **Iowa** and **Nebraska** have new info security laws that went live July 2018

- **Chicago** has even drafted their own city ordinance to clamp down on personal data misuse
A US Federal Privacy Regulation?

FTC fines app TikTok/Musical.ly $5.7 million for child data privacy violations

For a US federal privacy bill, senators want to dig deeper than just pre-emption
Goodbye
Many different stakeholders will be impacted by the requirements but need to act in sync to lower organization risk and costs.

- **Privacy**
  - Existing and pending global privacy compliance laws

- **Retention**
  - Heritage retention and records-keeping requirements

- **Residency**
  - Growing volume of regulations that include keep-in-country mandates

- **Reporting**
  - Both compliance reporting and data breach obligations continue to grow
Risk

- With privacy now a boardroom and C-level risk management issue, driven by regulations such as GDPR and CCPA, the regulatory compliance landscape is accelerating complexity, cost and risks across the business.

Value creation
Agile businesses want to distill, derive and act across their data using the latest accelerators.

Global scale
It’s about All your data, whatever and wherever it is - knowing, managing and using it appropriately.

Regulatory complexity
Before acting on any data, you should ensure you’re first on top of compliance.
How to embrace privacy compliance

1. Compliance
Organizational and technical measures across people, policy, process and education change management, demonstrating transparent accountability

2. Personal Data
Knowing what you have, where and why, know the lineage, lifecycle and purpose and be able to timely respond to data subject and consumer rights

3. Data protection
Protecting the data you have, across cybersecurity, encryption, access controls & monitoring through to incident breach readiness and reporting

Embracing privacy for transformation
Most respondents think GDPR can help them transform their organization - it is not just a mandatory regulation.

<table>
<thead>
<tr>
<th>From May 25th, 2018</th>
<th>Applies Globally</th>
<th>4% of Global Revenue or €20M Potential Penalty Per-incident</th>
</tr>
</thead>
<tbody>
<tr>
<td>Across 28 EU countries</td>
<td>to any Organization working with Personal Data of a Data Subject residing in the EU Or Profiling From the EU</td>
<td></td>
</tr>
</tbody>
</table>

5 Key General Data Protection Regulation Obligations

- Rights of EU Data Subjects
- Security of Personal Data
- Compliance & Legal Basis
- Accountability of Compliance
- Data Protection by Design and by Default
The more data you have, the harder it is to quickly and correctly respond.

- Facebook saw a fourfold increase in SAR Requests
- Marriott, the hotel operator, has asked for extensions to the one-month response period
- Technology companies, media groups, retailers and banks targeted

Netherlands DPA plan to randomly inspect - “Selected companies are required to produce documentary evidence of compliance with the GDPR.”
+ Germany & Italy
10 Months Later...

1st - ICANN Loses First GDPR Court Ruling in Germany

- ICANN being the internet corporation for assigned names and numbers.
- The WHOIS system allows for us to see, sometimes not all the time, the person that was responsible for purchasing the domain
- Data Minimization

Detailed discussion [here](#)

“British Airways breaches GDPR with Social Media Errors”

- British Airways was reported to be breaching GDPR in July after a security researcher discovered that the airline’s social media team was requesting that customers post their personal details publicly on Twitter if they wished to have their complaints addressed.
- found that British Airways has been employing the use of tracking cookies in a web browser to gather personal information which it then shares with third-party websites and that online check-in was only being permitted when Ad-blocker software was disabled on a passenger’s internet browser.

$20M or 4% of GBP 11.4B = $599M
Address these Privacy Pains

**Discovery**
- No catalog of the categories or types of personal data, where it is by system or by location

**Records of processing**
- Lack ROPA inventory to respond to initial regulator requests
- No privacy catalogue matched to processing activities

**Purpose & Choice**
- Lack lawful-basis of processing defined against data
- No central consent definition and client tracking by purpose

**Lifecycle mgmt**
- De-facto permanent over-retention
- Lack records-keeping & disposal
- Escalating risk of duplicating production data into Test without masking or anonymization

**Subject rights**
- Lack customer-360 and master data entity resolution
- Manual risk-prone and cost-escalating processes to try to find and respond to requests

**Accelerate:**
- ML accelerated tools to find and classify
- Across all Strx and Unstrx data
- Supporting hybrid and multi-cloud
- Populating a central privacy catalogue
- Models to start when they have no definition of personal data

**Scale:**
- GDPR template for ROPA
- Integrated discovery tools against a privacy catalogue
- Accountable reporting ready to respond live to audit & regulator requests
- Enterprise scale across all clouds & on-prem silos

**Accountability:**
- Extensible purpose & consent definition, management and tracking
- Integrated into central privacy catalogue
- Master-data integrated to accelerate entity resolution

**Comply:**
- Enterprise retention & records-keeping across all data
- ML powered auto-classification for automation with archiving
- Masking and anonymization plus test data fabrication reducing risk in test/dev/QA

**Transparency:**
- Case Management workflows for enterprise-scale management of requests
- Robotic Process Automation to automate against privacy catalogue and discovery tools
IBM has used the same capabilities internally for its own global readiness program.
1. Discovery
Know your relevant data: Understand where personal data & metadata resides around a central catalogue

2. Records of Processing
Capture your processing activities on personal data and demonstrate progression towards privacy specific requirements

3. Purpose & Choice
Help you manage the purposes of processing by consumer /data-subject, execute and meet their rights including consent & opt-outs

4. Lifecycle mgmt
Protect personal data: Safeguard data by applying anonymization and minimization techniques via automatable policy execution for archiving & retention

5. Subject rights
Enable your organization to comply to consumer /data-subject rights requests within the timescales defined

Privacy compliance building blocks
Prescriptive stepping stones journey with actionable outcomes to compliance
IBM Accelerators for Privacy Regulations

**Cognitive Insights**
IBM Regulatory Compliance Analytics, with IBM Watson, digest GDPR and identify Controls & Obligations

**Contract Review**
Increased insight with the ability to load contracts for Watson to analyze and consider the language, clauses or paragraphs

**Data Protection**
Structured personal data discovery & classification. Personal data access & data subject rights audit trails; reports and readiness-risk dashboard

**Incident Response**
GDPR program preparatory guide, GDPR incident simulation & GDPR-enhanced Privacy module

**Industry Models**
GDPR supportive content taxonomy with predefined terms, data model elements, against each article

**Subject 360 Access**
Discover and register data source and the personal data they contain. Golden record identification with Workflows for DSAR requests

**Purposeful Consent By Design**
Consent Service available enterprise wide, linking Data to usage and specific per-citizen consent.
IBM is using the same method & solutions as it provides to clients

• “At IBM, we have a deep rooted understanding that privacy is foundational to trust. We are approaching the GDPR in the same spirit, both internally and with respect to our client offerings. IBM’s data privacy teams have been reviewing and assessing the new EU General Data Protection Regulation since its early draft stages, and as IBM’s Chief Privacy Officer, I recently published a statement that outlines IBM’s commitment to GDPR readiness. Teams across IBM are adapting our internal processes and commercial offerings to prepare for when the GDPR comes into effect on May 25, 2018. These same experienced professionals are available to support you at each stage of your own GDPR readiness journey. And what better customer reference for IBM’s capabilities on GDPR, than IBM itself?”

Cristina Cabella
IBM Chief Privacy Officer
ibm.com/privacy
ibm.com/gdpr
Data Privacy & Protection
Readiness Methodology

<table>
<thead>
<tr>
<th>Phase</th>
<th>Activity</th>
<th>Outcome</th>
</tr>
</thead>
</table>
| Assess     | – Conduct risk & privacy assessments across governance, people, processes, data, security  
– Develop Privacy Readiness Roadmap  
– Identify & Map personal data | Assessments and roadmap                                                   |
| Design     | – Design governance, training, communication, and process standards  
– Design privacy, data management and security management standards | Defined implementation plan                                              |
| Transform  | – Develop and embed procedures, processes and tools  
– Deliver Privacy training  
– Develop & embed standards & policies using Privacy by Design, Security by Design  
– Detailed Data Discovery | Process enhancements completed                                             |
| Operate    | – Execute all relevant business processes  
– Monitor security and privacy using TOMs  
– Manage Consent & data subject access rights | Operational framework in place                                             |
| Conform    | – Monitor, assess, audit, report and evaluate adherence to Privacy standards | Ongoing monitoring and reporting                                          |

**Operational Framework**

- Includes Data Protection controls, processes and solutions to be implemented
- TOMs in place: Personal Data discovery, classification and governance in place
- Begin the new Privacy ready way of working
- Monitor TOMs execution; deliver compliance evidence to internal and external stakeholders
Global Program of Transformation

Launched a global GDPR Program Mgmt Office (PMO)

SVP Finance and Operations
SVP Legal & Regulatory Affairs and General Counsel

SVP Forum

Chief Privacy Office
Chief Data Office

GDPR Programme Management Office

IBM as a Data Controller
- Address IBM’s obligations for managing internal data.

IBM as a Data Processor
- Ensure compliance and governance for all IBM offerings and services that process personal data.

IBM GDPR Common Services
- Deploy enterprise tools and common services to facilitate GDPR-related policy, system and business process changes.

IBM Vendor Management
- Align our supply chain to the upstream obligations we make to our clients and to our internal responsibilities.

IBM Client & Contract Management
- Help make the client buying process GDPR ready.

GDPR Go-To-Market
- Create a unified GDPR solution to help our clients with their GDPR readiness programmes.

Compliance, Audit & Risk Mitigation
- Implement a plan to demonstrate compliance with the principles of the GDPR, evaluate IBM’s overall privacy posture and mitigate the risk dynamics of the GDPR.
Personal Data Discovery

- Know your relevant data: Understand where personal data resides
- Define your inventory of Personal Data
- Discover where Personal Data is stored
- Reveal ‘shadow’ data stores
- Process structured and unstructured data and store results in a common privacy catalog
- Leverage GDPR specific content in Industry Models and GDPR Accelerator Cartridges for (RegEx & ML) to accelerate discovery
They were looking for a robust platform that would serve as a compliance and audit solution to help drive GDPR compliance, litigation support and records management processes. They sought a solution that could be implemented quickly, would help accelerate their GDPR remediation, and offer an integrated enterprise-grade platform that could scale to index and categorize over 1 PB of unstructured content across file shares, email, Box and a myriad of other repositories. The key challenge for them was to be able to rapidly find GDPR related content across a global network.
Records of Processing Activities (ROPA)

• helps enable companies to address the requirements to report on processing activities as defined in Privacy Regulations through appropriate tooling and a set of artifacts provided through a ROPA Template.

• **Example: Art. 30 in the GDPR:**
  
  *Records of processing activities*

• Each controller and, where applicable, the controller’s representative, shall maintain a record of processing activities under its responsibility.
Purpose & Consent Mgmt

- Consent Service providing framework for obtaining, maintaining and applying where specific consent is required for data processing by the regulation, away from the current blanket single consent commonly imposed

- Supports any categories of Consent or Sharing preferences for data subjects, flexible and changeable by them at any time.

- Each is more granular, specific for each purpose and clearly conveys what data is related to that consented purpose

- Where required, explicit transparent Purposeful Consent of any personal data categories is available for data subject and processors to know and understand how it is defined and used.
Govern the lifecycle of data with archival, records management, and disposal

Provide policy governance across complex regulatory needs for retention

Automate execution of electronic retention and records mgmt.

Automate archiving and re-tiering of inactive data

Drive to Data Minimisation under GDPR
Little Substantial Progress

IG maturity remains anemic on the Process Maturity Model*

- 7% Tools in place to categorize data and automate retention schedules, processes are integrated
- 29% Some automated processes and tools in place, data may still exist in departmental silos
- 49% People manually link discovery and regulatory obligations to IG practices
- 16% No structural linkage of duties and value to IG

CGOC IG Process Maturity Model
Masking & Test Data Fabrication

- Mask personal data with realistic but fictional data, de-identify sensitive information; mask complete business objects across heterogeneous databases & applications; when needed, generate synthetic test data
- Govern the lifecycle of data with archival, records management, and disposal
- Drive to Data Minimisation as requested in regulations like the GDPR
- Understand Data Lineage and adhere to accountability requirements for data repositories defined in the regulations
Did You Know?

Rabobank accelerated test data delivery from weeks to days, reducing risk employing pseudonymization to keep data private.

Speeding software development and protecting data privacy

Masking & Test Data Fabrication

- **Cuts time** taken to prepare test data from weeks to days
- **Higher-quality** data enables more efficient testing and development
- **Enhances** regulatory compliance and meets strict data privacy law

ibm.com/case-studies/Rabobank-Test-Data-Factory-InfoSphere-Optim-HADES
Data Subject / Consumer Rights

- Enterprise scale consistent auditable processing for all access requests, leveraging a single catalog, policy and processing criteria for each data subject
- Streamline the access decision and template repeatable but personalized responses back to the data subject
- Provide auditable tracking, management and execution of access requests e.g. Article 15 in GDPR
“There are analytical processes we have stopped doing due to GDPR. We need to find a way to resume doing them.”
Businesses are looking for a way to protect their customers’ privacy, maximize the value of their data assets, and minimize their risk of violating GDPR.
Thank You

• Remember to complete the session survey In the App!

Richard Hogg
Global Privacy Compliance Guru, IBM
rghogg@us.ibm.com
+1-703-963-2900
Who we are:

- We are a cloud-hosted, data anonymization, and analytics solution
- We are all about protecting privacy and powering results
- Our solution is ground-breaking, unique, and timely
- We are already winning awards for innovation
- Our investors are Mastercard, IBM, and C3
- Mastercard, our first customer, is in production on the IBM cloud
- IBM is a key selling partner for Trūata