

Addressing the Duty to Dispose in a Post-GDPR World

Tara Emory
Director of Consulting, Driven, Inc.

Richard Hogg
Global Privacy Compliance Guru, IBM

Northern Virginia Chapter ARMA NOVA
Building Success Through Relationships

Managing Risky Records: Evolving Privacy Best Practices

Annual Spring Conference | ARMA NOVA & Metro MD
April 10, 2019

Metro MARYLAND Chapter of ARMA International

Tara Emory

Director of Consulting, Driven, Inc.

Tara Emory advises organizations and law firms on information governance programs and e-Discovery. Her IG practice includes privacy and GDPR, data management and compliance, policies, records management technology, defensible deletion and implementation of AI solutions.



Tara is a lawyer, certified PMP, experienced participant in industry advisory groups, and a frequent speaker on IG issues. Tara is also a member of the Board of Directors for Advocates for Justice and Education

Richard Hogg

Global Privacy Compliance Guru, IBM



With 15+ years global experience across Information Governance (#infogov), He spent the last 4 years working with heavily-regulated clients worldwide on their GDPR journey. In parallel he was a workstream leader as part of IBM's own global privacy program. He's a frequent speaker on GDPR & InfoGov across AIIM, ARMA, MER, LegalTech, Insight, World of Watson, InfoGovCon, IPBA, DataWorks, Think & ILTA LegalSEC.

- 2018 Top 50 Social Influencers in Risk, Compliance and Regtech.
- 2017 Finalist Winner InfoCoalition Infogov SME of the Year

Northern Virginia Chapter ARMA NOVA
Building Success Through Relationships

Managing Risky Records: Evolving Privacy Best Practices

Annual Spring Conference | ARMA NOVA & Metro MD
April 10, 2019

Metro MARYLAND
Chapter of ARMA International

Abstract

1. Privacy Drivers for Disposal – Data Minimization
2. Disposition duty overview and legal requirements
3. Legislative Landscape
4. The Privacy & Disposal Transformation opportunity

1.

Privacy Drivers for Disposal – Data Minimization

€50 million

- None
- Of
- Your
- Business

noyb.eu



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 Iannopollo, 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





Most not Ready?



- UK ICO 338%
- IE ICO 378%
- DE DPA 1300%
- Sweden 2
- Belgium 3

Netherlands DPA plan to randomly inspect - “Selected companies are required to produce documentary evidence of compliance with the GDPR.”

+ Germany & Italy

- 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

The more data you have,
The harder it is to quickly and correctly respond.

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.

e20M or 4% of GBP 11.4B = $599M

2.

Disposition duty overview and legal requirements

Disposition:
What to keep? What not to keep?

- In the US, emphasis has been on “Defensible” Disposition
- In the EU, the fear is not deleting something that should have been
- How do multinational companies deal with records retention and disposition in a world of changing regulations, different regulations, and complex data?
- Programs must achieve objectives of data subject rights laws, obligations to delete, and obligations to retain

Disposition as Part of Info Gov

- Accountability
- Transparency
- Integrity
- Protection
- Compliance
- Availability
- Retention
- Disposition

Northern Virginia Chapter ARMA NOVA Building Success Through Relationships

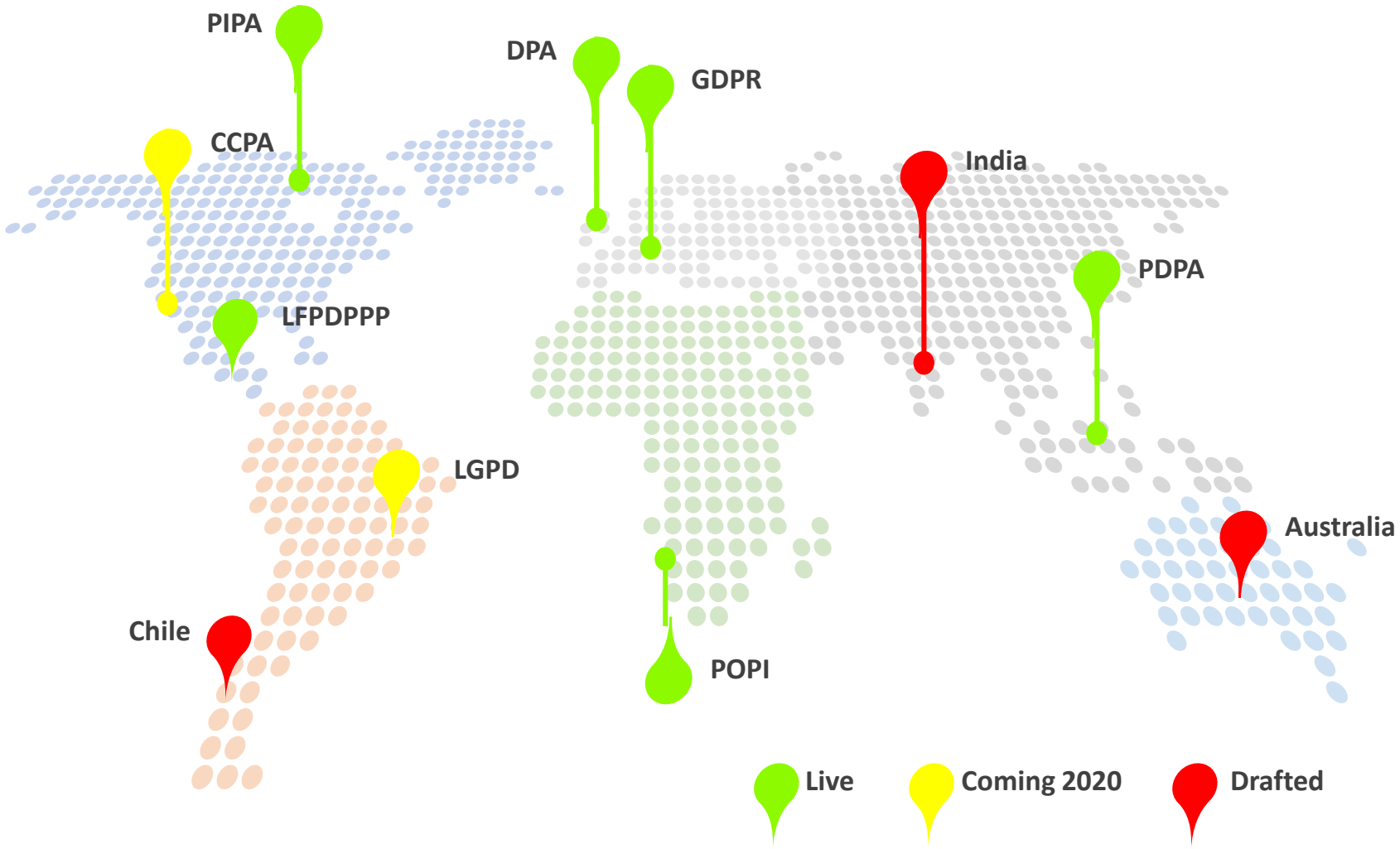
Metro MARYLAND Chapter of ARMA International

3.

Legislative Landscape

Patchwork of Laws

- EU: GDPR
- US: State and
  Federal Laws
- Many, Many More



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.

US Laws on Data Retention and Deletion

- Federal Retention: Employee, Tax, industry-specific (HIPAA, SEC)
  - Legal Holds: reasonably anticipated litigation, government investigation
- Federal Deletion: FTC Disposal Rule (Sort of)
- State Retention: Healthcare, Government entities, industry-specific
- State Deletion:
  - California CCPA
  - New York Department of Financial Services Cybersecurity Regulation
  - Colorado Protections for Consumer Data Privacy Act

Consumer Privacy Act, GDPR Inspired

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/GetCCPAReady

More US States to Come

- Every state has a data breach notification law, as of 2018
- Most states require reasonable security measures for PII
- Many states have laws about how PII can be deleted
- Vermont: Registration of data brokers
- Iowa and Nebraska: New Info Sec Laws
- Chicago: draft ordinance on personal data
- Massachusetts:

Growing global privacy regulations

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

GDPR ↑

88%

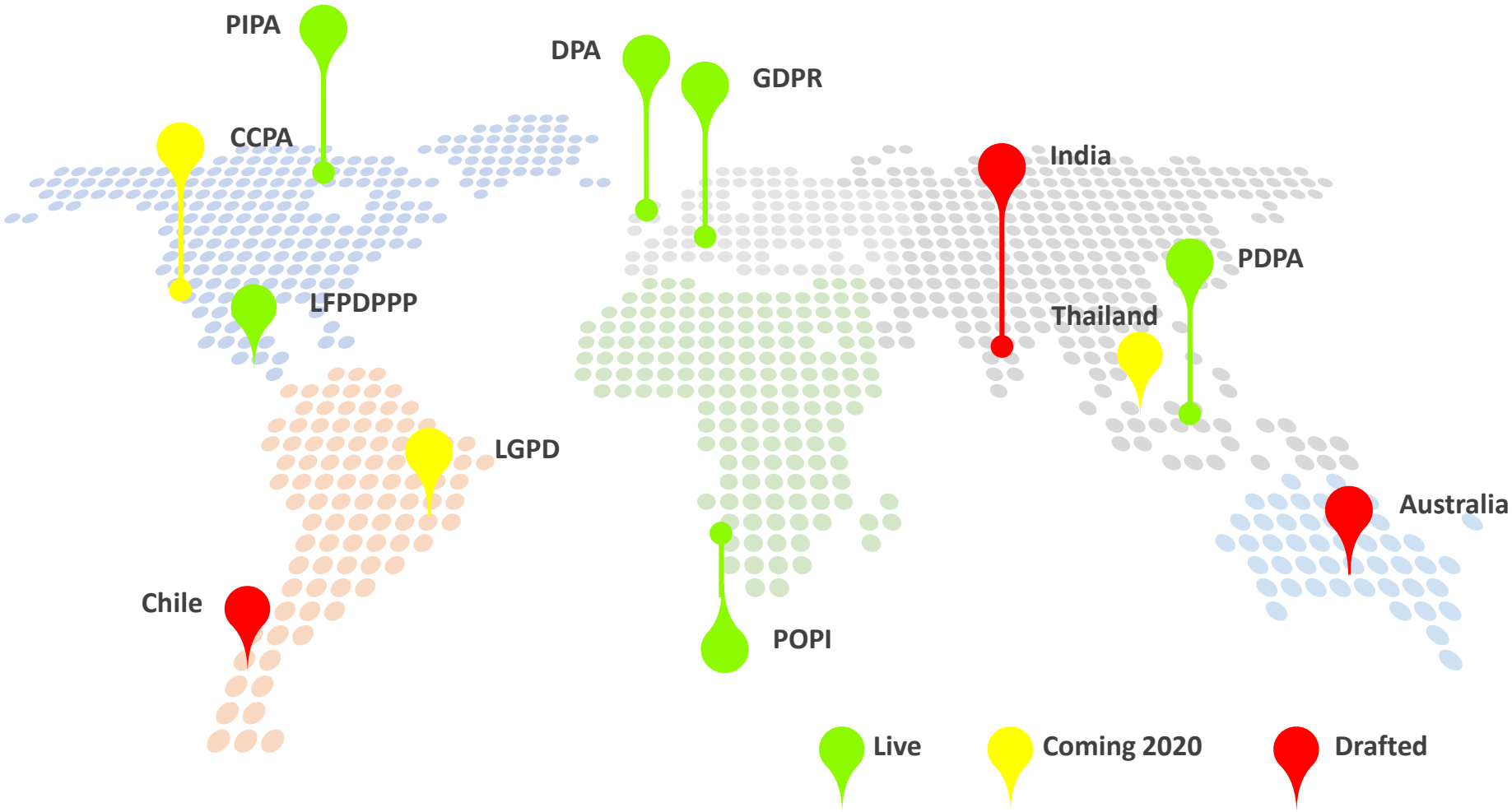
Spent > $1 M

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.

A US Federal Privacy Regulation?



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

'This Is Surveillance.' Apple CEO Tim Cook Slams Tech Rivals Over Data Collection





[Hearings]



NIST

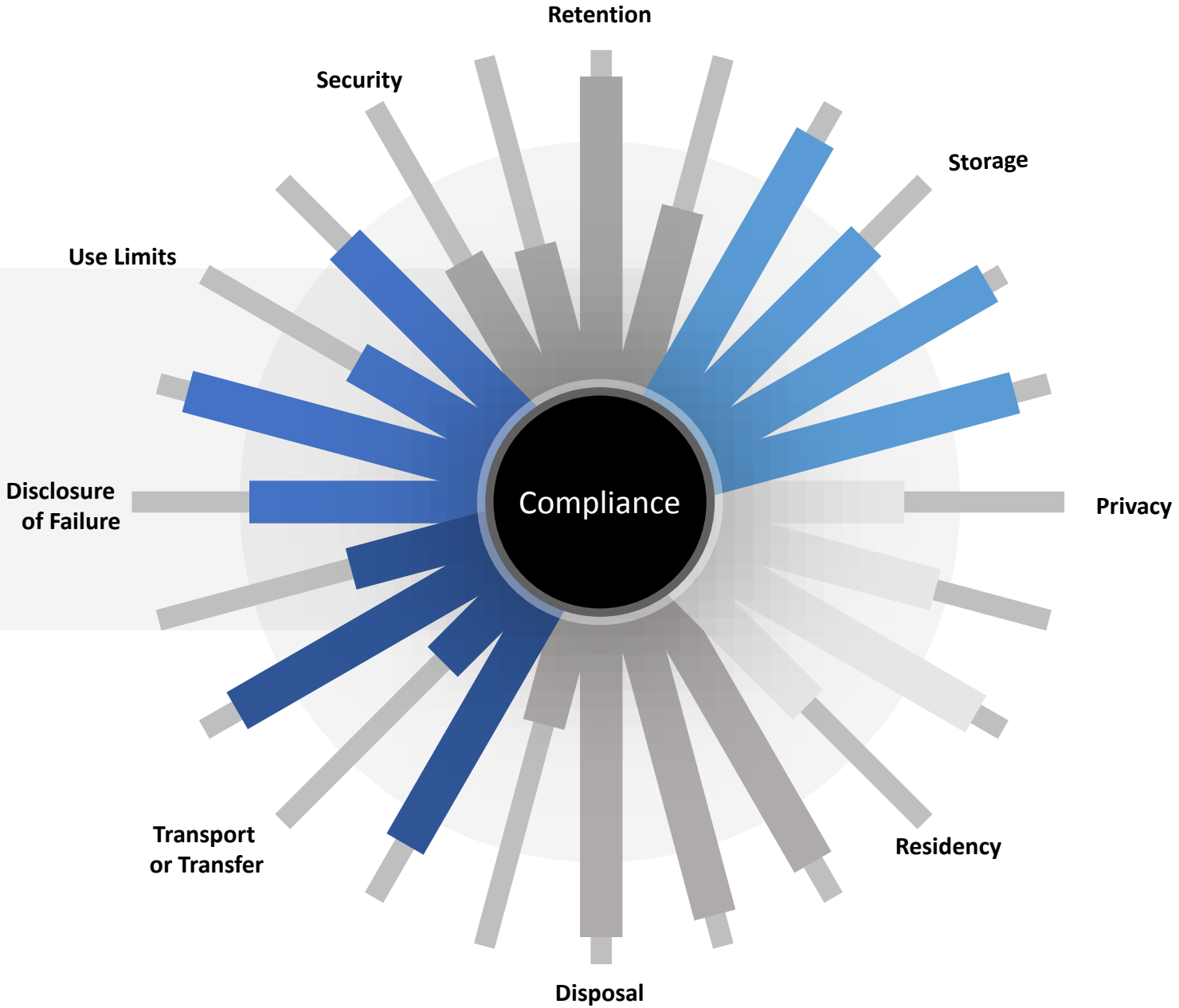
PRIVACY FRAMEWORK




Goodbye

The evolving compliance opportunity

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

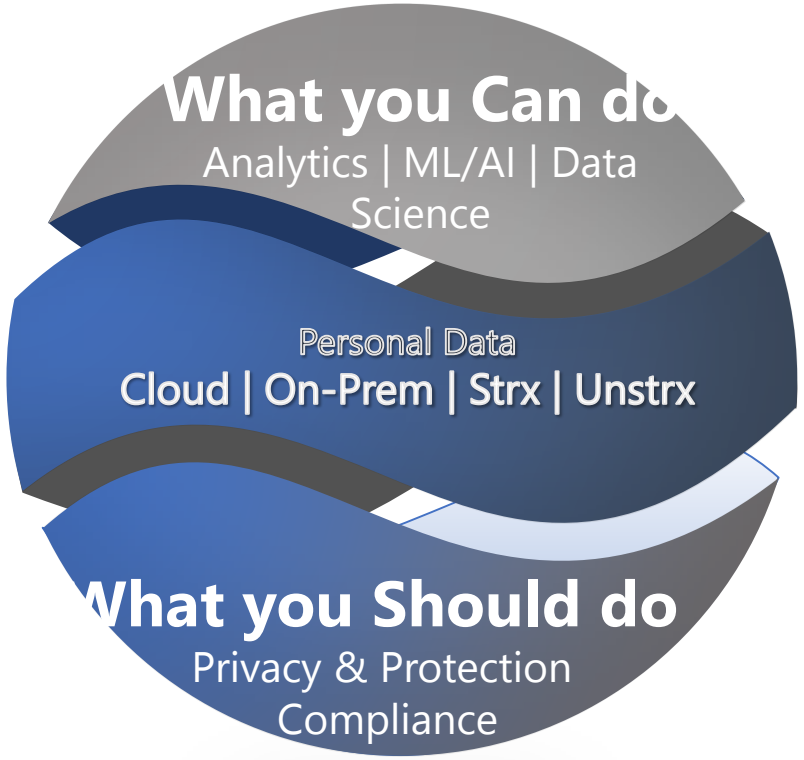
Reporting

Both compliance reporting and data breach obligations continue to grow

Risk

Risk now drives What to do With Data

- 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



Information Governance….

Embracing privacy for transformation

4.

The Privacy & Disposal Transformation opportunity

Data Deletion Policy Strategies

- Work with your DPO
- Avoid ad hoc deletion
- Keep what is required by law
- Identify what might need to be deleted, by law
- Keep what has business value
- Records Retention Policies, and other IG Controls, should reflect what is possible
- Balance geography exceptions with convenience of consistency

Mechanics of Disposition

- Disposition to serve a purpose
  - Legal requirements to destroy
  - Other
- Mechanics
  - Deletion: Deleting, wiping, purging, destroying
  - Encryption
  - Anonymization*
- Reasonability and risk
- Without undue delay
  - Backups
- Third parties, multiple devices, etc.

Implementing Deletion

- Start with a Data Map: You can't delete what you don't know
  - Structured Data
  - Unstructured Data: Organized or Intermingled?
  - Archived and Legacy Data
  - Beware Shadow IT
- What types of data are where?
  - Personal data
    - March 27: Polish Data Authority sanctions from data scraping
  - Sensitive personal data
  - Regulated data
  - Confidential
  - Privileged
- Why do you have the personal data?

Implementing Deletion

- Clean up: Can be done with basic or fancy software
  - Considerations: volume, regulations, data organization, budget, resources
- New Information: Automation is a must
- Requests for Deletion: Have a REAL Process, not just a policy
- Resource: The Sedona Conference Principles and Commentary on Defensible Disposition

Northern Virginia Chapter ARMA NOVA Building Success Through Relationships

Metro MARYLAND Chapter of ARMA International

From May 25th, 2018

Across 28 EU countries

Applies Globally

to any Organization working with Personal Data of a Data Subject residing in the EU
Or Profiling From the EU

4%

of Global Revenue or

€20M

Potential Penalty Per-Incident

5 Key General Data Protection Regulation Obligations



Rights of EU Data Subjects



Security of Personal Data



Compliance & Legal Basis

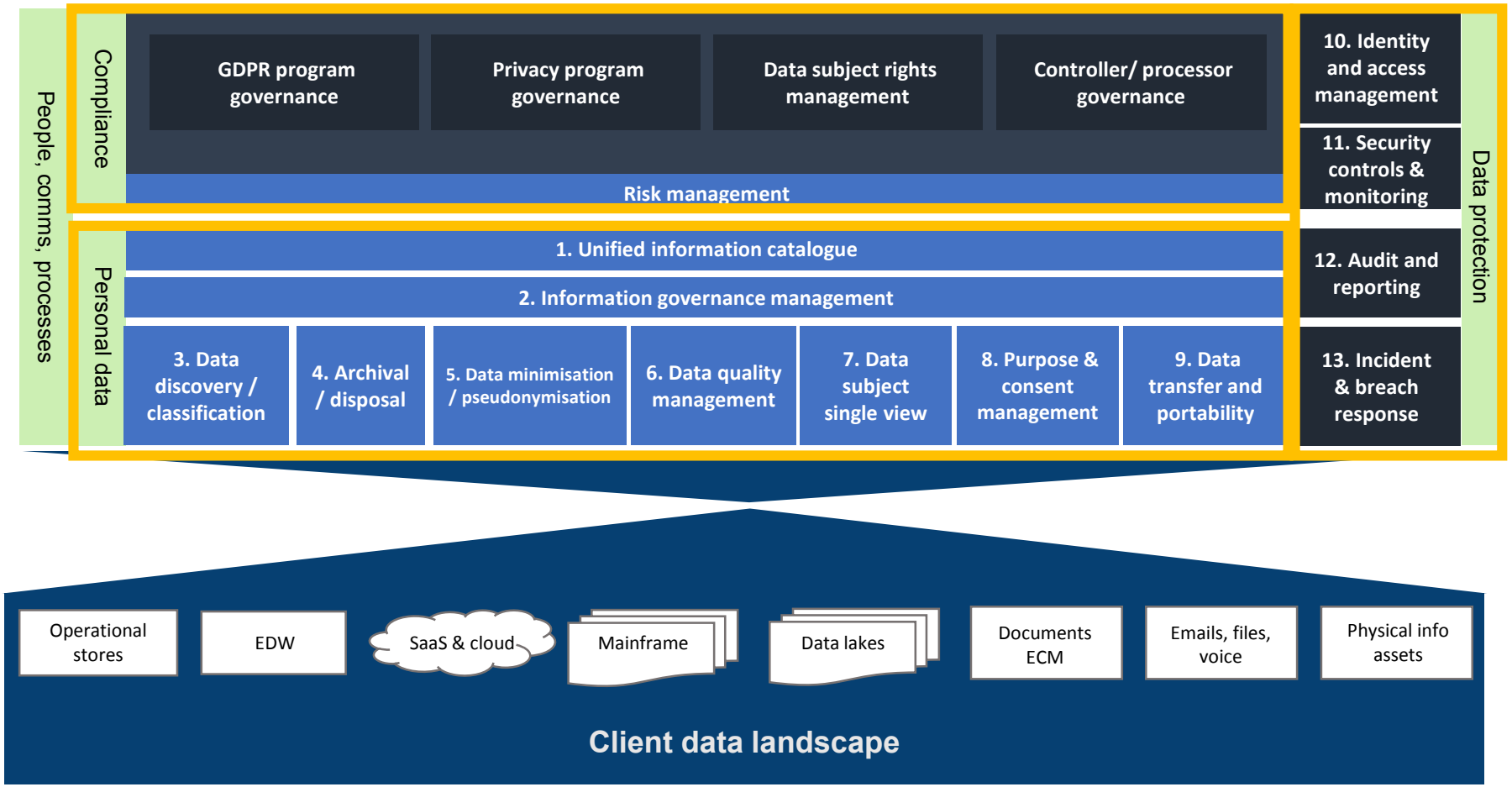


Accountability of Compliance



Data Protection by Design and by Default

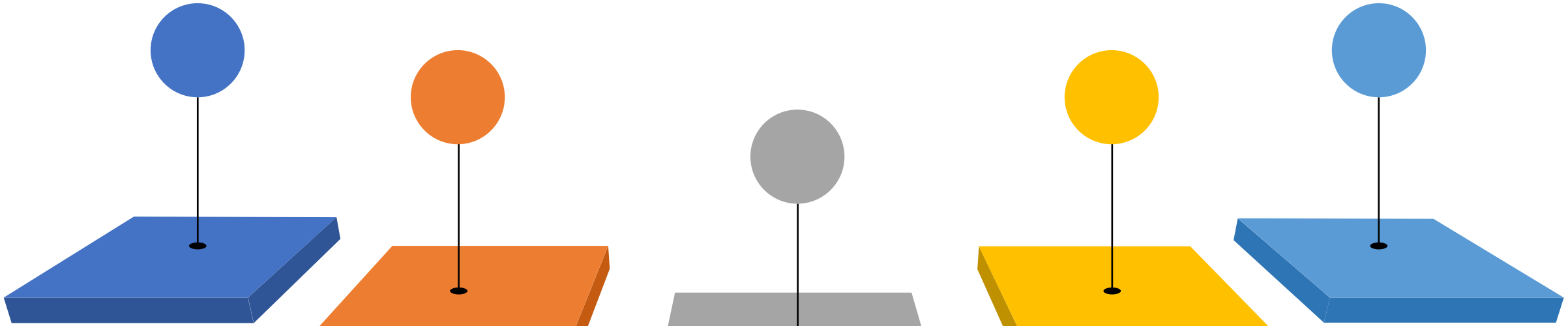
End-to-end Privacy Capabilities Needed



IBM has used the same capabilities internally for its own global readiness program

Privacy compliance building blocks

Prescriptive stepping stones journey with actionable outcomes to compliance



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

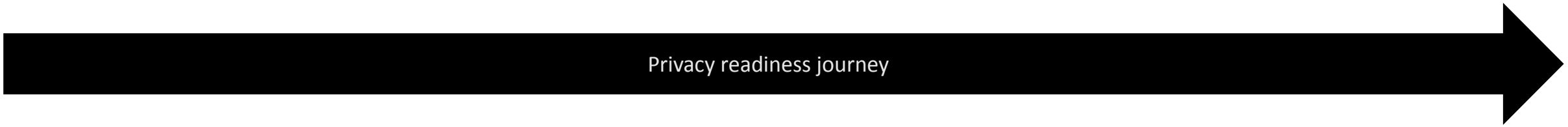
Help you manage the purposes of processing by consumer /data-subject, execute and meet their rights including consent & opt-outs

4. Lifecycle mgmt

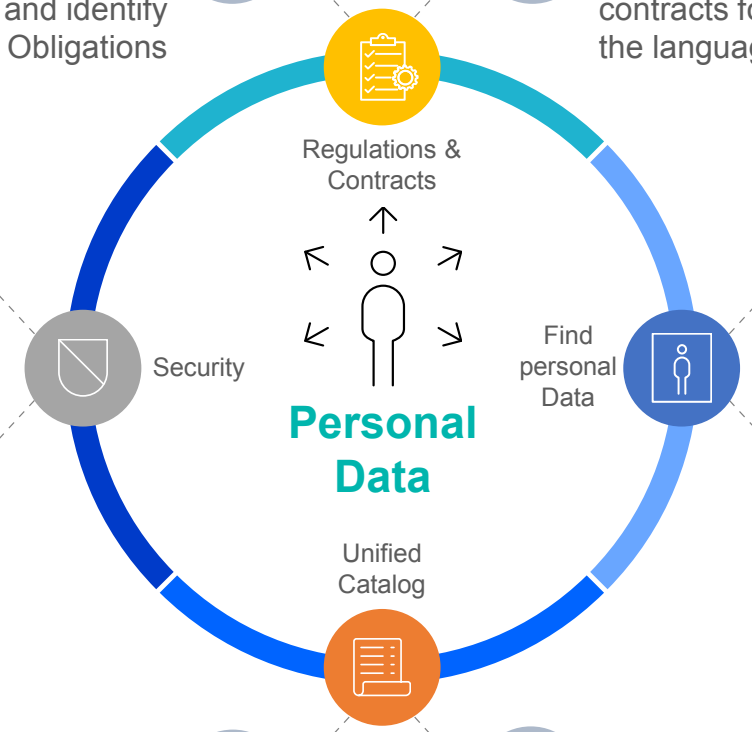
Protect personal data: Safeguard data by applying anonymization and minimization techniques via automatable policy execution for archiving & retention

5. Subject rights

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



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

GDPR focused Cartridges
Plug-in extensive unstructured personal data discovery rules using both RegEx and Machine Learning

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

Purposeful Consent By Design
Consent Service available enterprise wide, linking Data to usage and specific per-citizen consent.

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

IBM

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



IBM's Common Services for Privacy

Regulatory Dashboard

- Single source for audit and regulatory reporting
- Dynamically slice and dice and respond to audit and regulatory requests by Data Type, Processing Activity, Location, Controller and Processor duties

Data Privacy Portal

- Single portal for all Data Subject Rights including preferences for use of their data, privacy policies etc.
- *Currently going thru Design and Development*

Data Privacy Catalog

- Master repository of metadata and contacts for IBM Applications that contain Privacy information
- A central enterprise-wide catalog of what types and categories of Personal Data reside in each data source/application
- Enterprise Personal Data Taxonomy

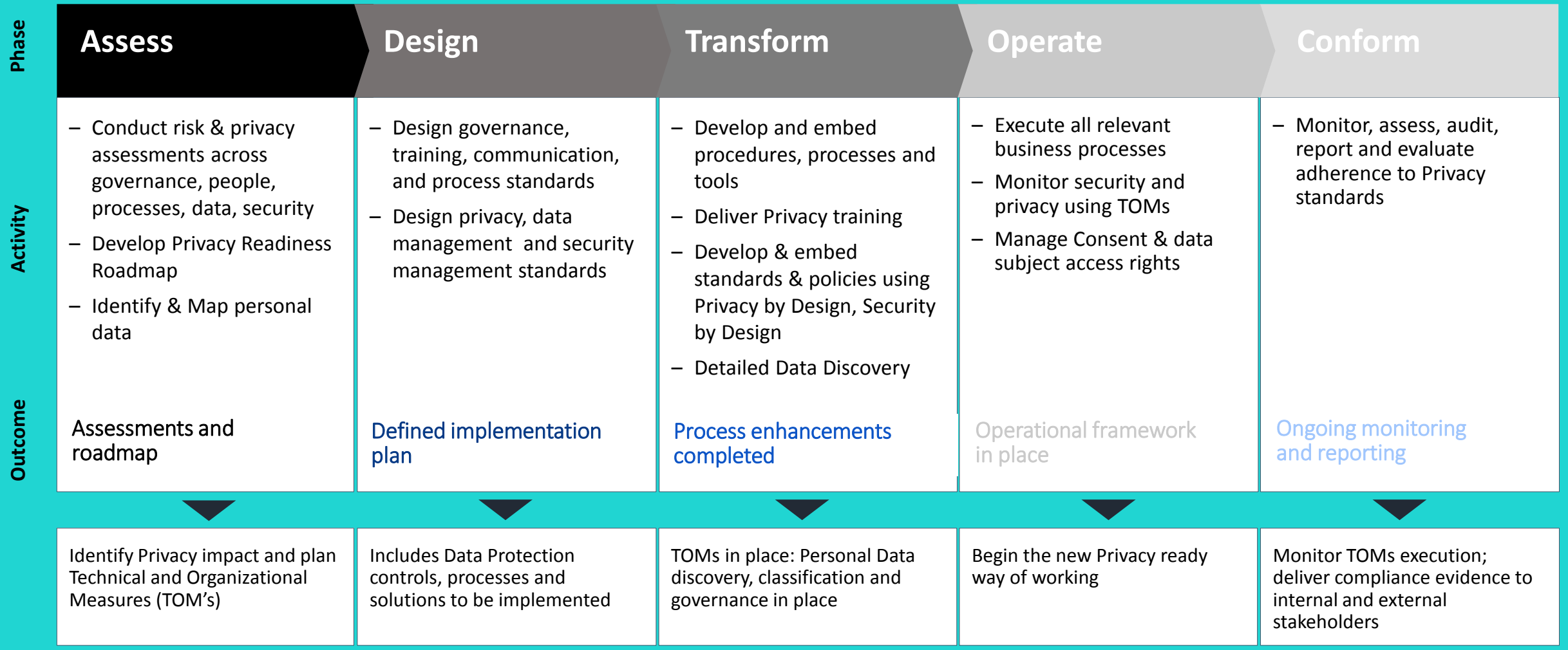
Consent Management

- Central IBM repository with APIs for managing Purposes for which personal data is collected and used; plus auditable records of notifications
- Define, manage and track Consent as one purpose, where required by processing activity

Data Subject Requests

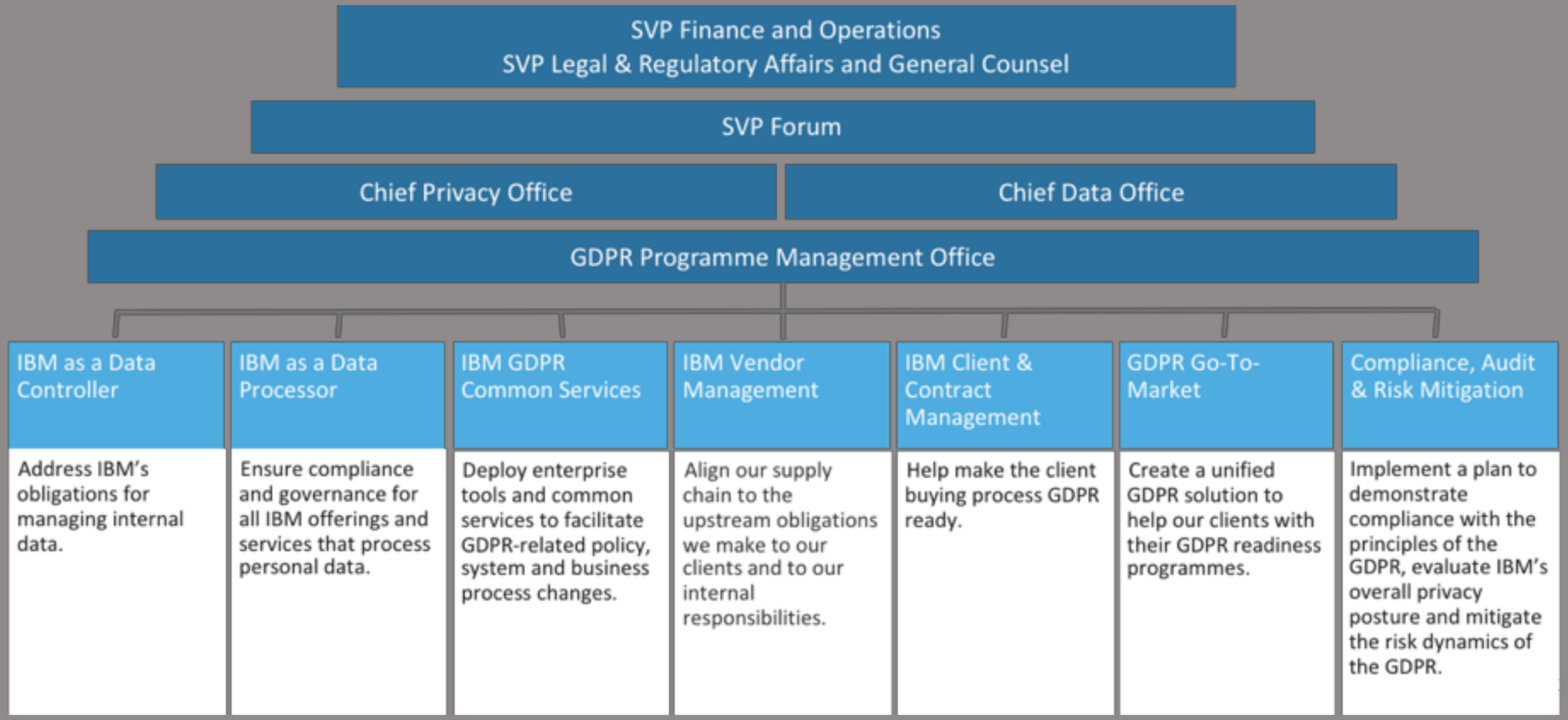
- Corporate Privacy Office workflow & process for data subject requests (Clients or employees)
- Enables tracking, managing activities with application owners to collect data and consolidation of collected data

Data Privacy & Protection Readiness Methodology



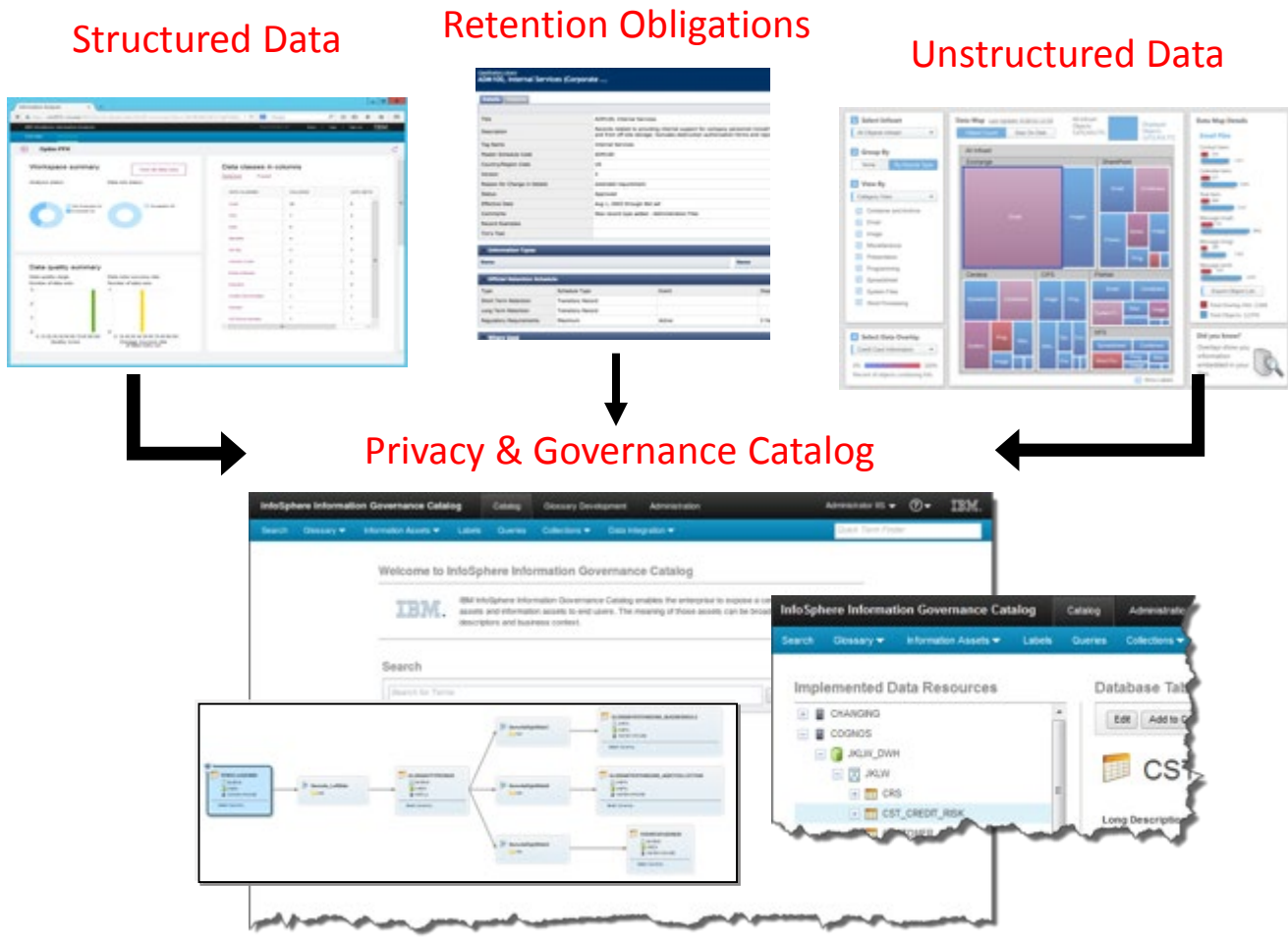
Global Program of Transformation

Launched a global GDPR Program Mgmt Office (PMO)



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

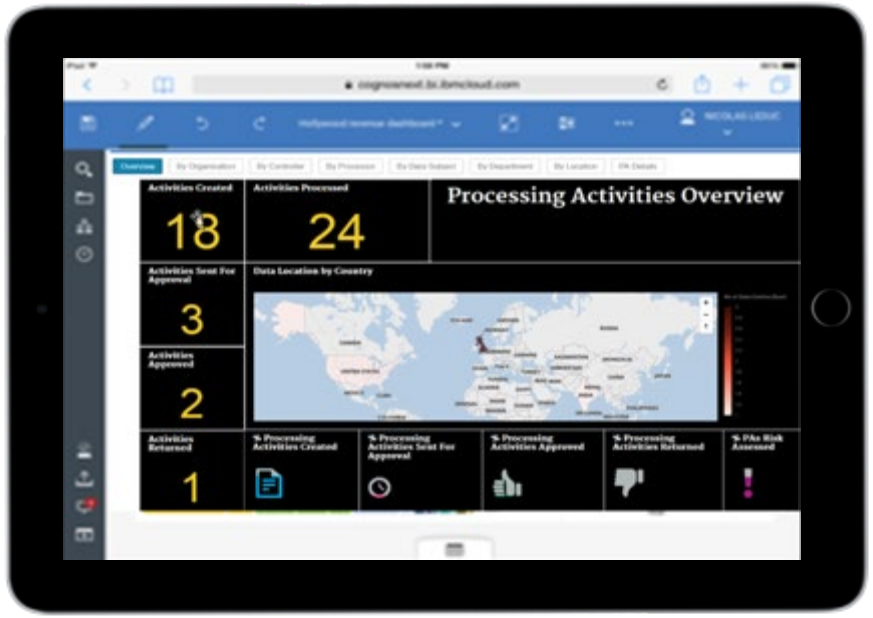


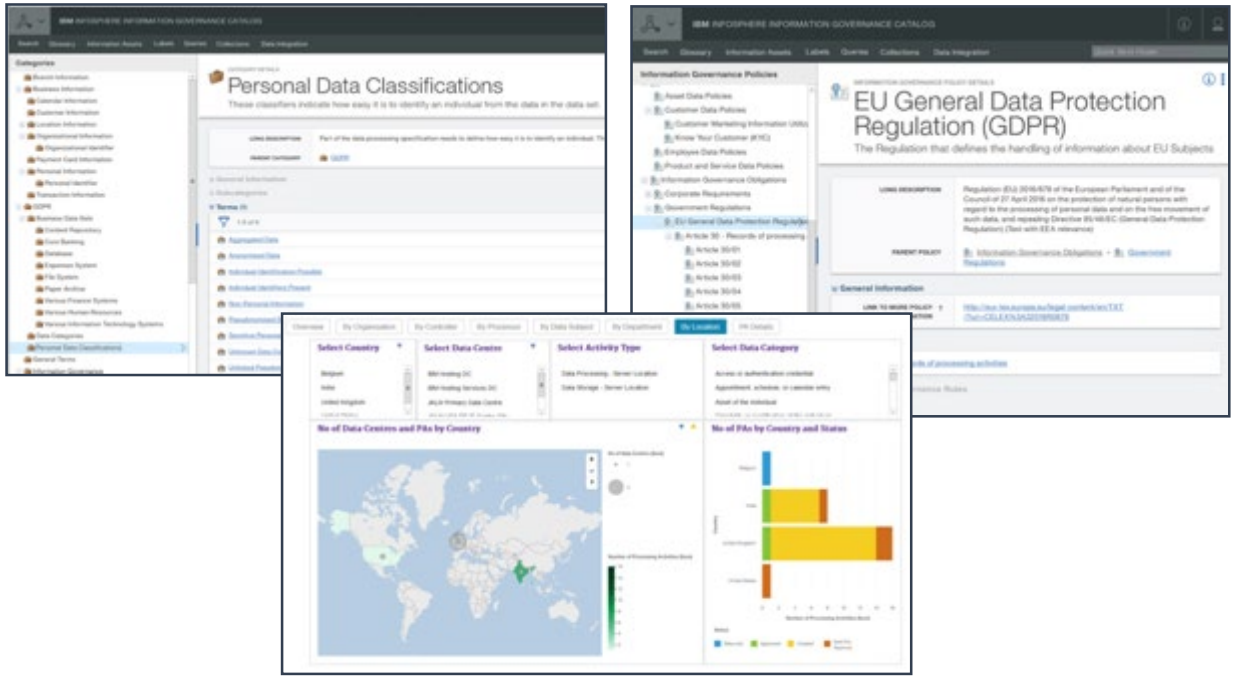
Records of Processing Activities (ROPA)

- 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***

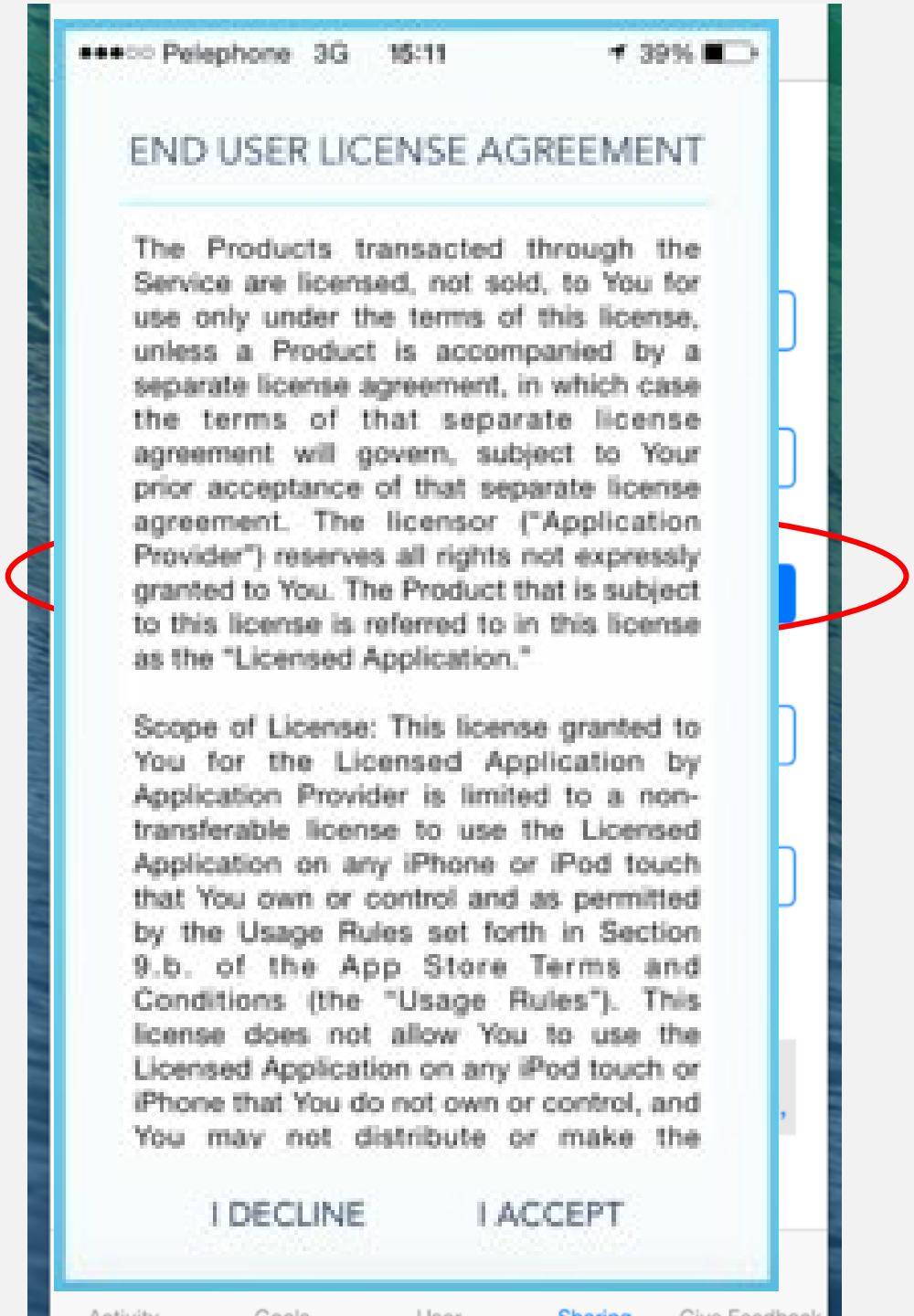
- Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility.





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.



Information Governance

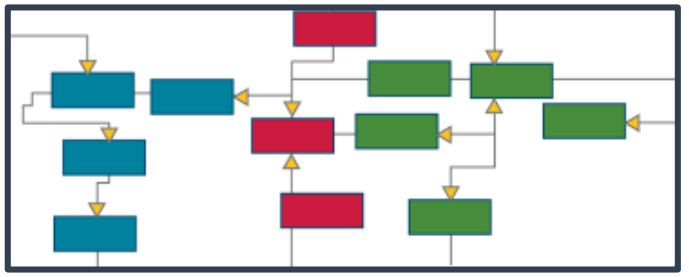
- Govern the lifecycle of data with archival, records management, and disposal
- Provide policy governance across complex regulatory needs for retention
- Automate execution of electronic retention and records mgmt.
- Automate archiving and re-tiering of inactive data
- Drive to Data Minimisation under GDPR



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

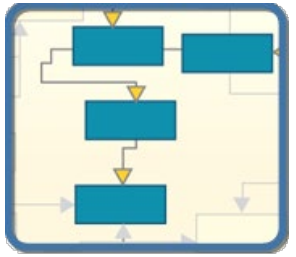






Business View

Overall historical “snapshot” of business activity, representing an application data record – e.g. payment, invoice, customer.



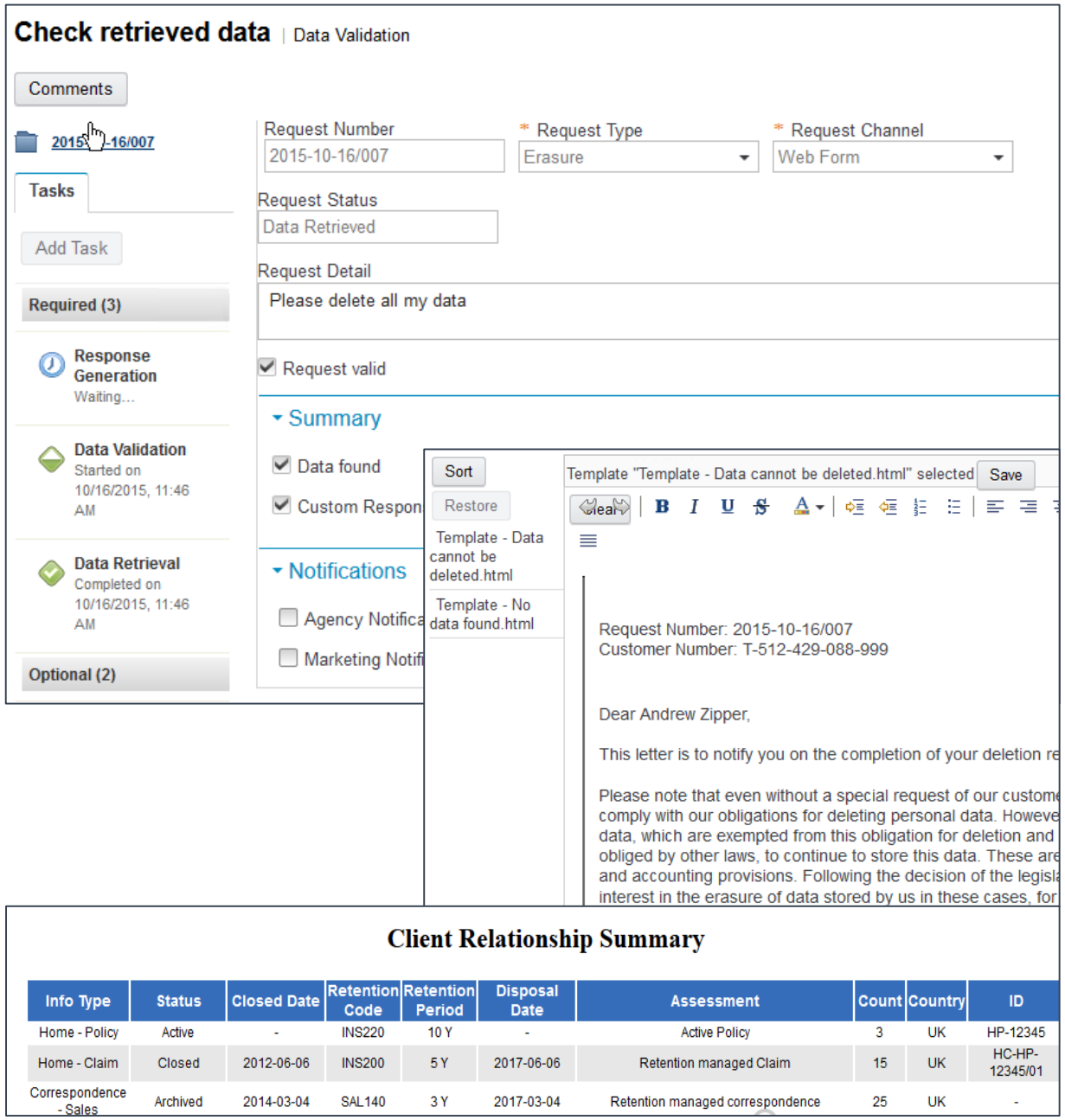


DBA View

Referentially-intact subsets of data across related tables & applications, including metadata.

Data Subject / Consumer Rights

- Enterprise scale consistent auditable processing for all access requests, levering 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



Client Relationship Summary

Info Type	Status	Closed Date	Retention Code	Retention Period	Disposal Date	Assessment	Count	Country	ID
Home - Policy	Active	-	INS220	10 Y	-	Active Policy	3	UK	HP-12345
Home - Claim	Closed	2012-06-06	INS200	5 Y	2017-06-06	Retention managed Claim	15	UK	HC-HP-12345/01
Correspondence - Sales	Archived	2014-03-04	SAL140	3 Y	2017-03-04	Retention managed correspondence	25	UK	-

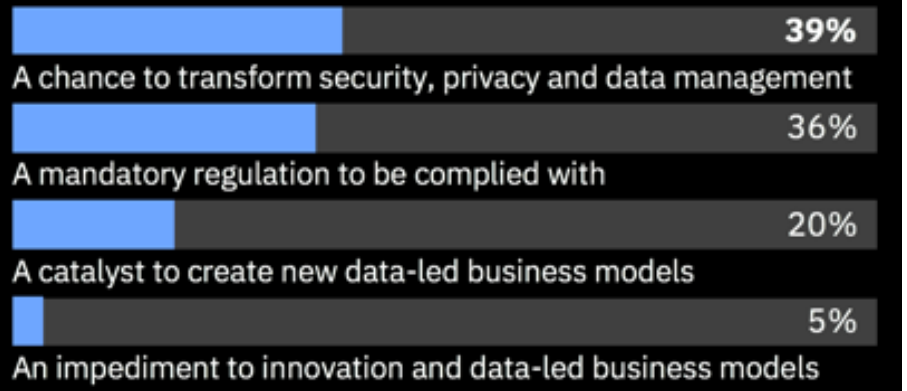
A Global Study

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

ibm.biz/powerofGDPR

The focus areas are also areas of struggle





GDPR component	#1 focus area	#1 struggle	GDPR component
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 (DPO)	4	4	Getting consent from data subjects
Getting consent from data subjects	5	5	Establishing a Data Protection Officer (DPO)

Note: Respondents were asked to rank their top three focus areas and struggles from a list of 11 different GDPR preparation components

Source: IBM IBV Study, May 2018, http://www.ibm.biz/powerofGDPR

Thank You

- Remember to complete the session survey

Tara Emory
Director of Consulting, Driven, Inc.
Tara.Emory@driven-inc.com
@TaraEmoryDriven

Richard Hogg
Global Privacy Compliance Guru, IBM
richardhogg@pm.me
+1-703-963-2900

Data Privacy Academy

bit.ly/ DPD19Academy

IBM Data Privacy Academy
Learn how to embrace data privacy
for organizational transformation



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.
- 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.