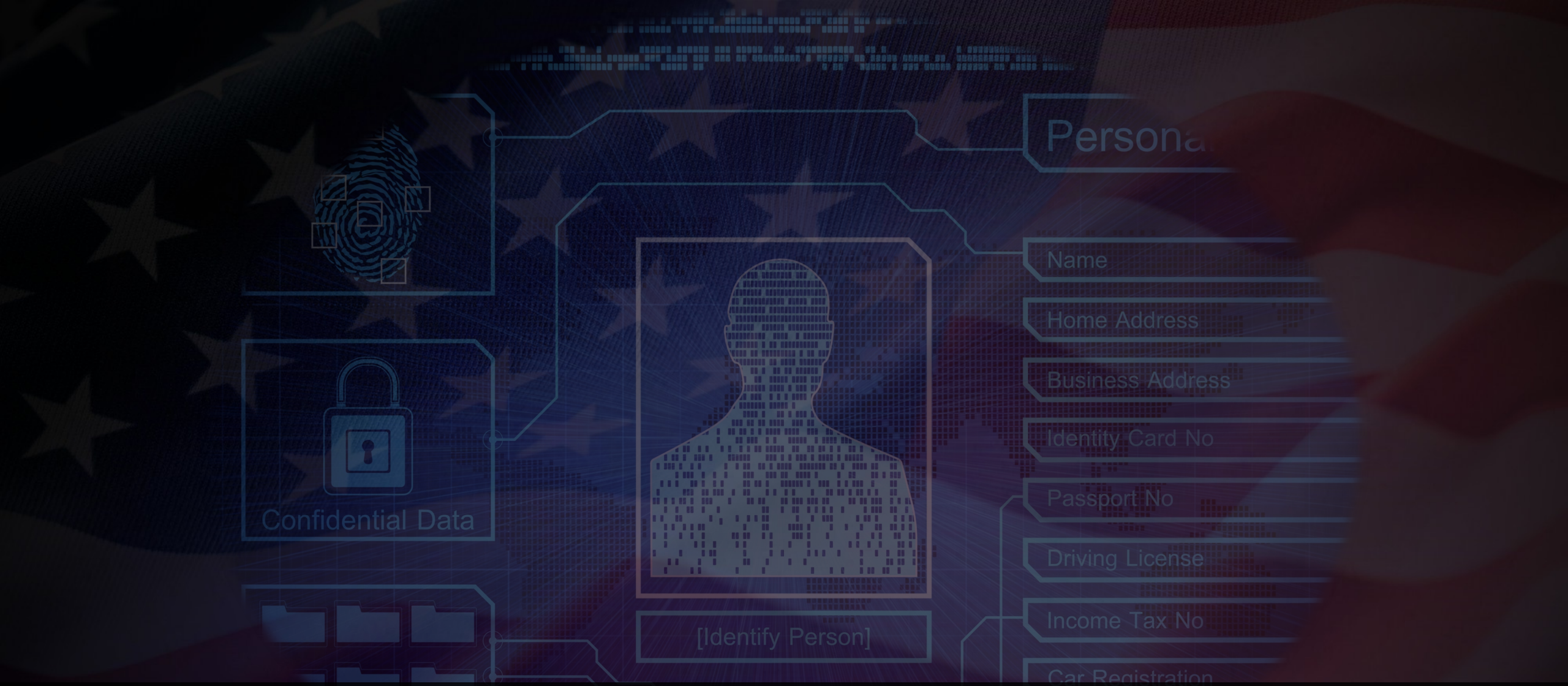


Overly Retentive: Data Retention and DSARs

WELCOME AND INTRODUCTIONS

Constantine Karbaliotis
Senior Privacy Advisor,
Exterro

Theresa Sippert
Manager - Information Management,
Hydro Ottawa

Description

- It’s trite to say that one of the best de-risking exercises in privacy is to get rid of data. Yet it is also trite to say that retention is one of the areas that most companies set themselves up for failure – first by adopting a retention schedule and policy that they then do not comply with.
- Historically the over-retention of data has compounded data breaches, by exposing far more information than should have been retained. DSARs, both from consumers, and now in California (given the employee exemption from CCPA is set to expire at the end of 2022), will likely expose organizational over-retention even further, with complaints and litigation increasingly likely. As importantly, it is essential to be able to articulate the retention of data is being done pursuant to legal and business requirements, so as to avoid unneeded challenges and complaints. Experience under GDPR has seen that failure to abide by retention schedules, even in the absence of a breach, has resulted in significant fines, as retention needs to be linked to valid legal and business purposes.
- This session will focus on the relationship between privacy and data retention requirements and programs, and how this relates to responding to DSARs efficiently and defensibly.

AGENDA

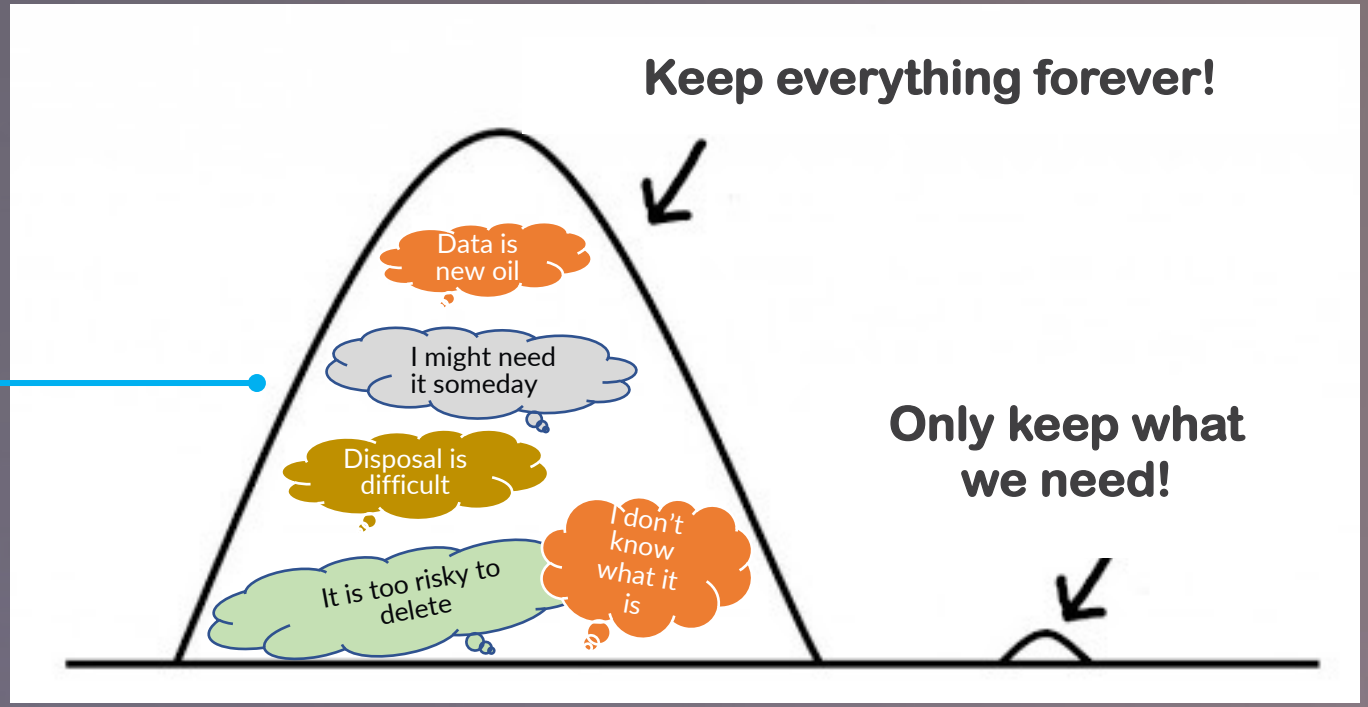
- What are the risks of over-retention
- Legislative background
- The lifecycle of a DSAR: what does retention mean from a DSAR standpoint
- Strategies to address over-retention

What are the risks of over-retention?

OVER-RETENTON OF PERSONAL DATA IS A LIABILITY

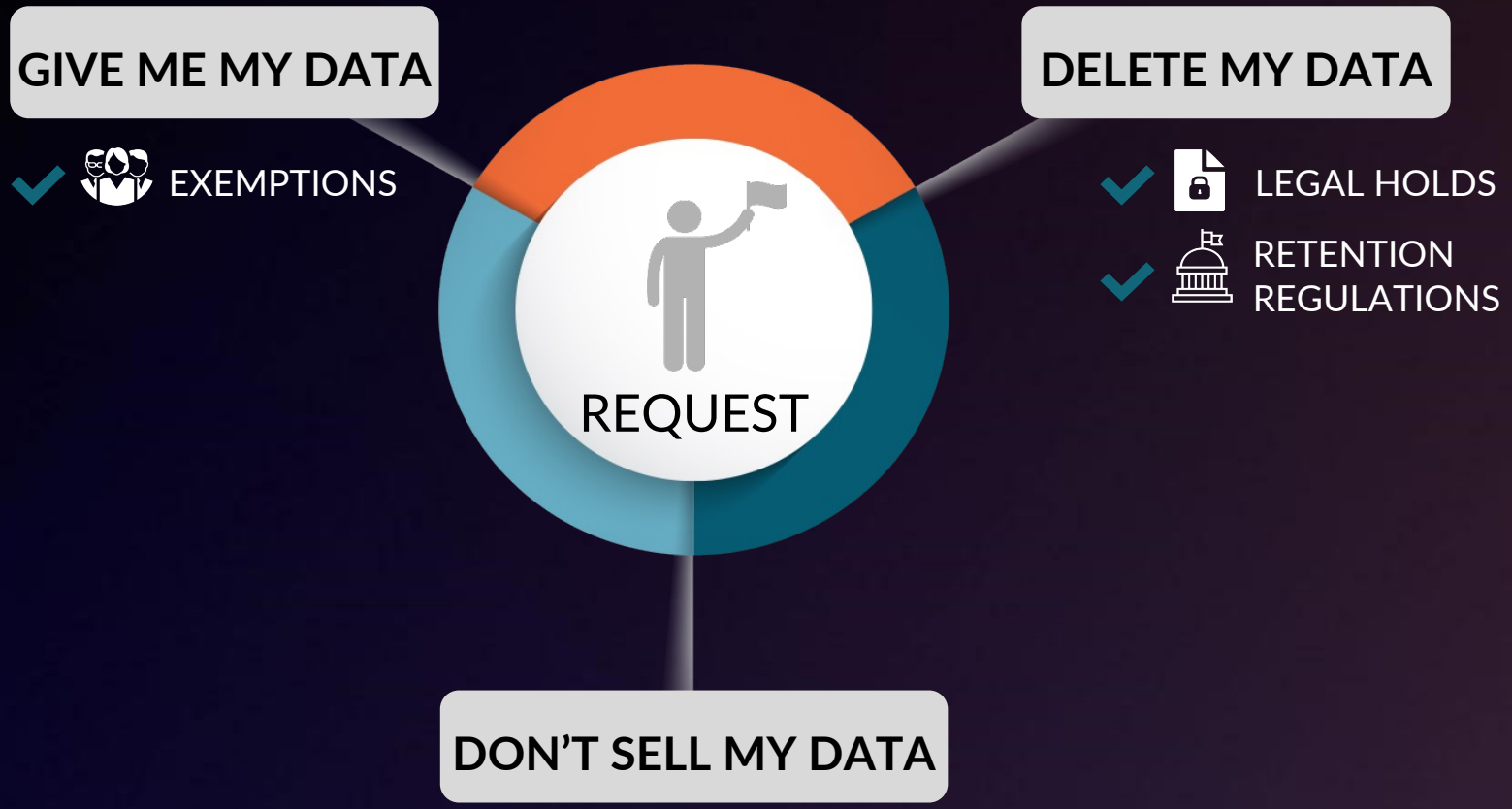
KEY RISKS:

- Data Breach
- Ransomware Attack
- Enforcement Action
- Litigation
- Consumer Requests



In addition to these areas, organizations must now consider the impact of DSARs both (a) increasing the risk over-retention comes to light, and (b) that existing retention policies that are unenforced, create a risk of regulatory action and liability

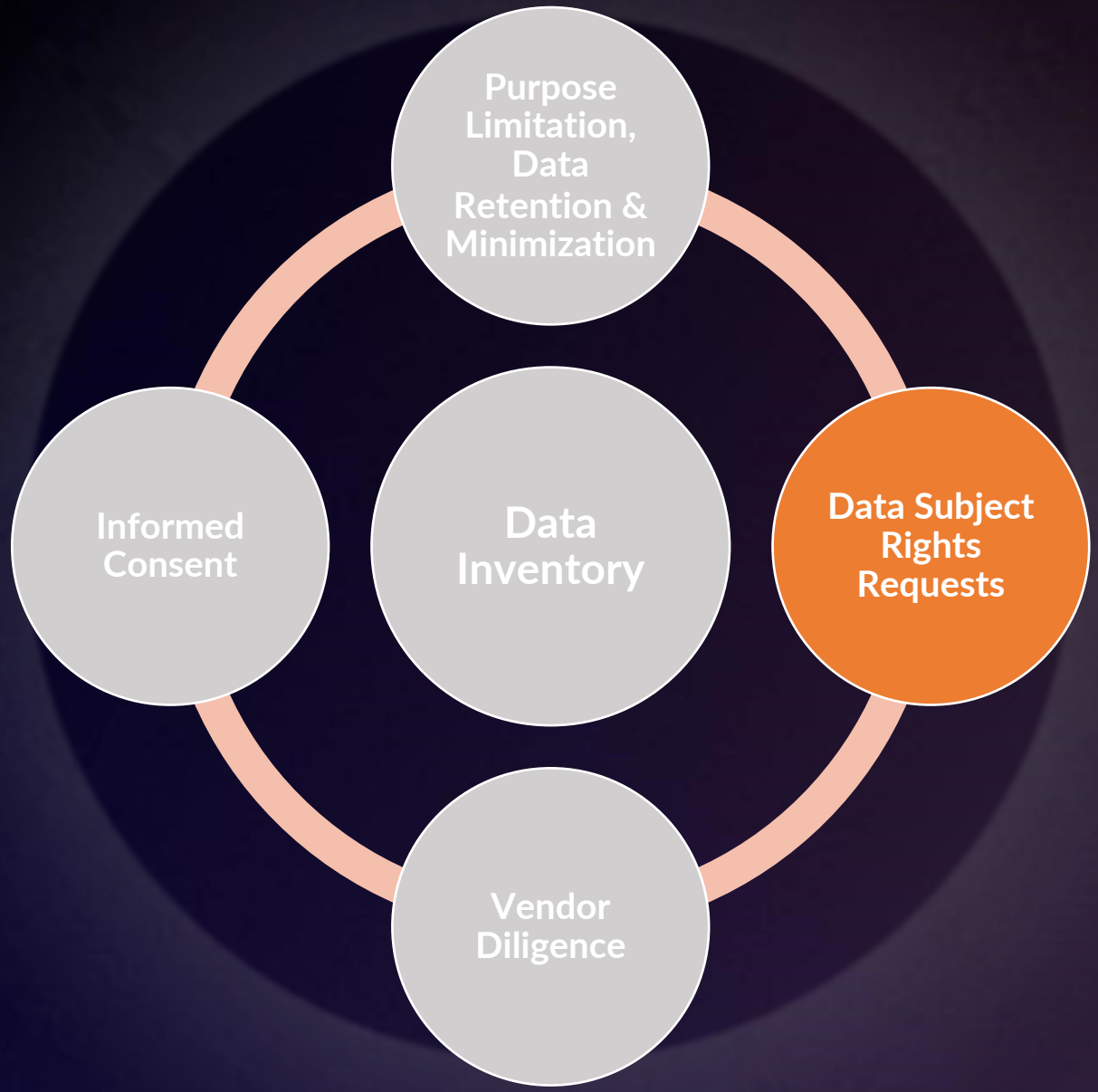
CONSUMER RIGHTS REQUESTS



The more data you have, the harder it is to respond to DSARs

Legislative Background

COMMON ELEMENTS OF DATA PRIVACY LAWS

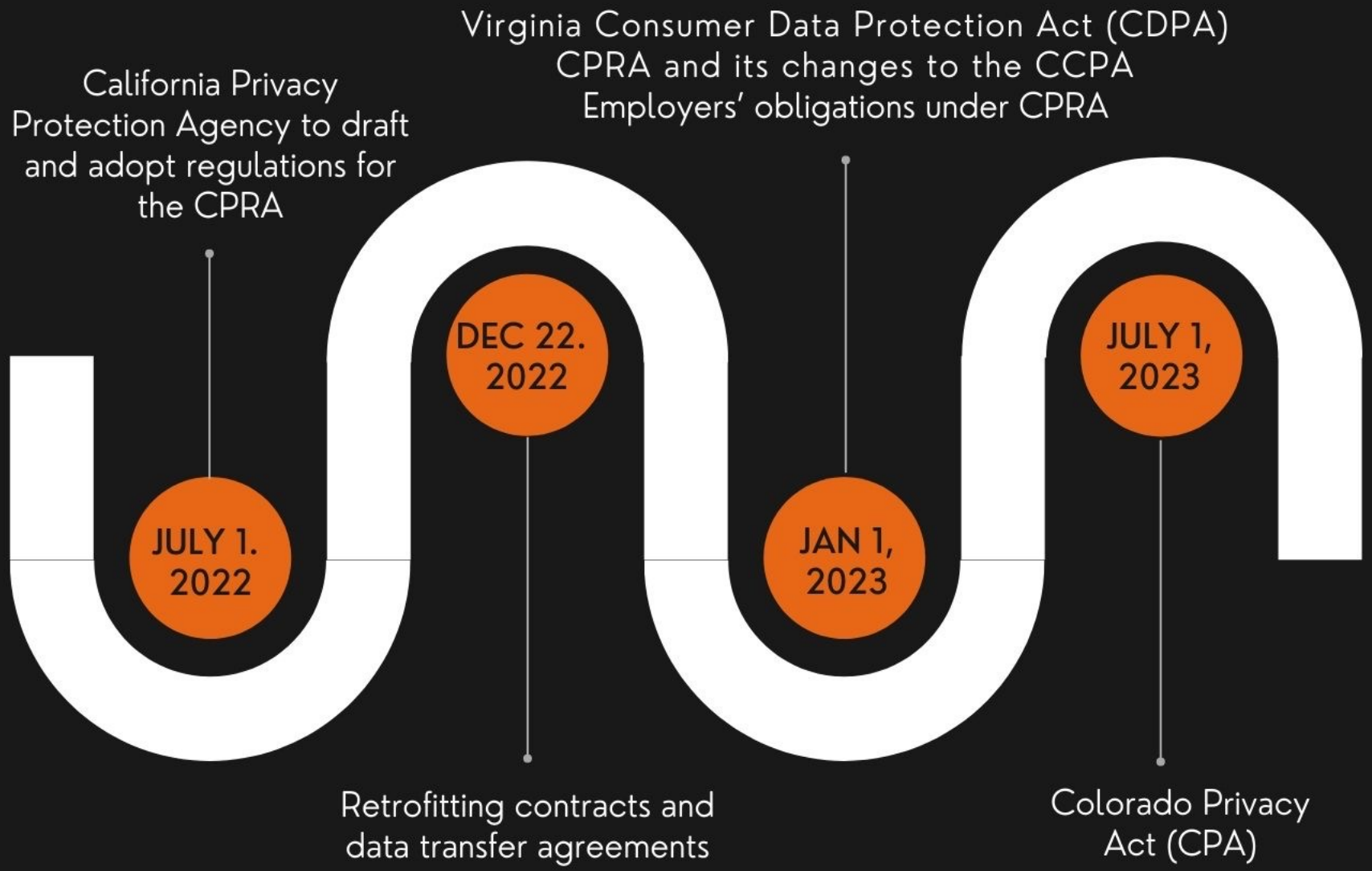


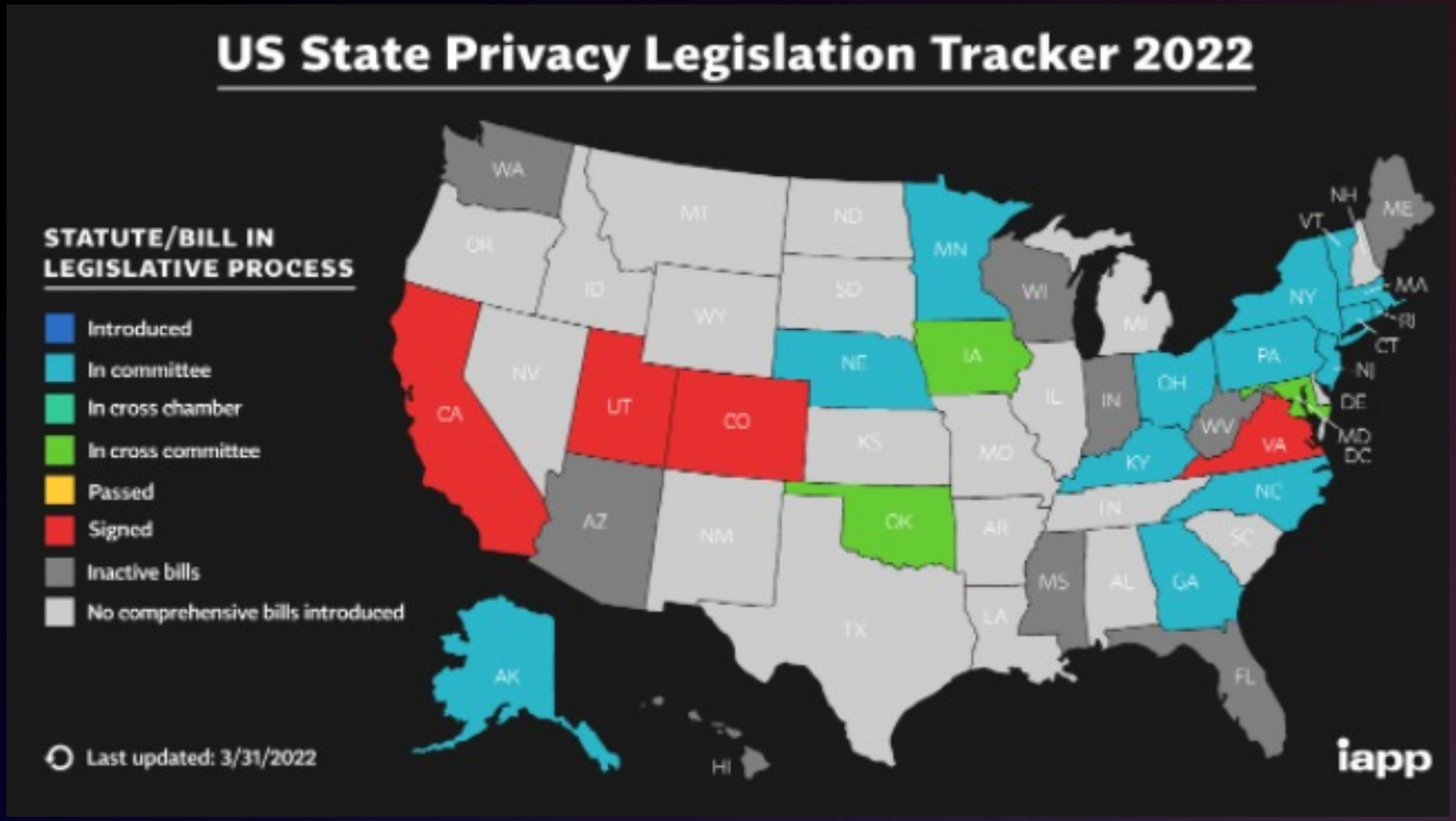
CONSUMER RIGHTS & BUSINESS OBLIGATIONS

Consumer Right	PICICA	CCPA	CPRA	CDPA	GDPR	CPA
Right to access	×	✓	✓	✓	✓	✓
Right to confirm personal data is being processed	×	Implied	Implied	✓	✓	✓
Right to data portability	×	✓	✓	✓	✓	✓
Right to delete ~	×	✓	✓	✓	✓	✓
Right to correct inaccuracies/right of rectification	×	×	✓	✓	✓	✓
Notice and transparency requirements	✓	✓	✓	✓	✓	✓
Right to opt-out of sales	✓*	✓*****	✓*****	✓****	✓**	✓*****
Right to opt-out of targeted advertising (CO and VA) / cross-context behavioral advertising sharing (CA)	×	×***	✓	✓	✓	✓
Right to object to or opt-out of automated decision-making ~ ~	×	×	✓	✓	✓	✓
Opt-in or opt-out for processing of "sensitive" personal data? – "sensitive is defined differently under CPRA, CDPA and CPA	×	×	Opt-out†	Opt-in	Opt-in††	Opt-in†
Right to object to/restrict processing generally	×	×	×	×	✓	×
Right to non-discrimination	×	✓	✓	Limited	Implied	Limited
Purpose / Use / Retention Limitations	×	Implied	✓	✓	✓	✓
Applies to both consumers and in HR and B-to-B contacts	×	+	++	×	✓	×
Privacy and security impact assessments sometimes required	×	×	✓	✓	✓	✓
Obligation to maintain reasonable security	×	✓	✓	✓	✓	✓

KEY DATES

- Deadlines are fast approaching
- Draft regulations will be late





DATA RETENTION: POSSIBLE CPRA DISCLOSURE FORMAT

Category of PI	Purposes	Retention Period
Identifiers - Name, postal address, Internet Protocol address and email address.	1. Performing Services 2. Short-term Transient Use (e.g., to serve contextual ads)	1. For as long as services are performed, thereafter 4 years for records keeping or as otherwise required by law or legal process 2. Only as needed to complete the transient use, typically less than a day
Sensory Data - Audio recordings of customer support calls.	Customer Service Quality & Training Purposes	Retained for 3 years from date of recording unless on Legal Hold.
Geolocation Data - Approximate physical location	(fill in purpose)	(fill in retention period)

The Lifecycle of the DSAR

The Lifecycle of a DSAR

RECEIPT

- Receipt of a Request Is it a DSAR?
- Authentication
- Routing the DSAR: 80/20 Rule

ACTIONING

- Structured v/s unstructured
- Transparency and self-service
- Too much data, too long?
- Search and collection; third-party issues

COMMON PAIN POINTS

ANALYSIS

- Is it something we can provide? Does motive matter?
- Exclusions: Privilege? Other people's data?
- Consumer versus employee
- Transparency and self-service

RESPONSE

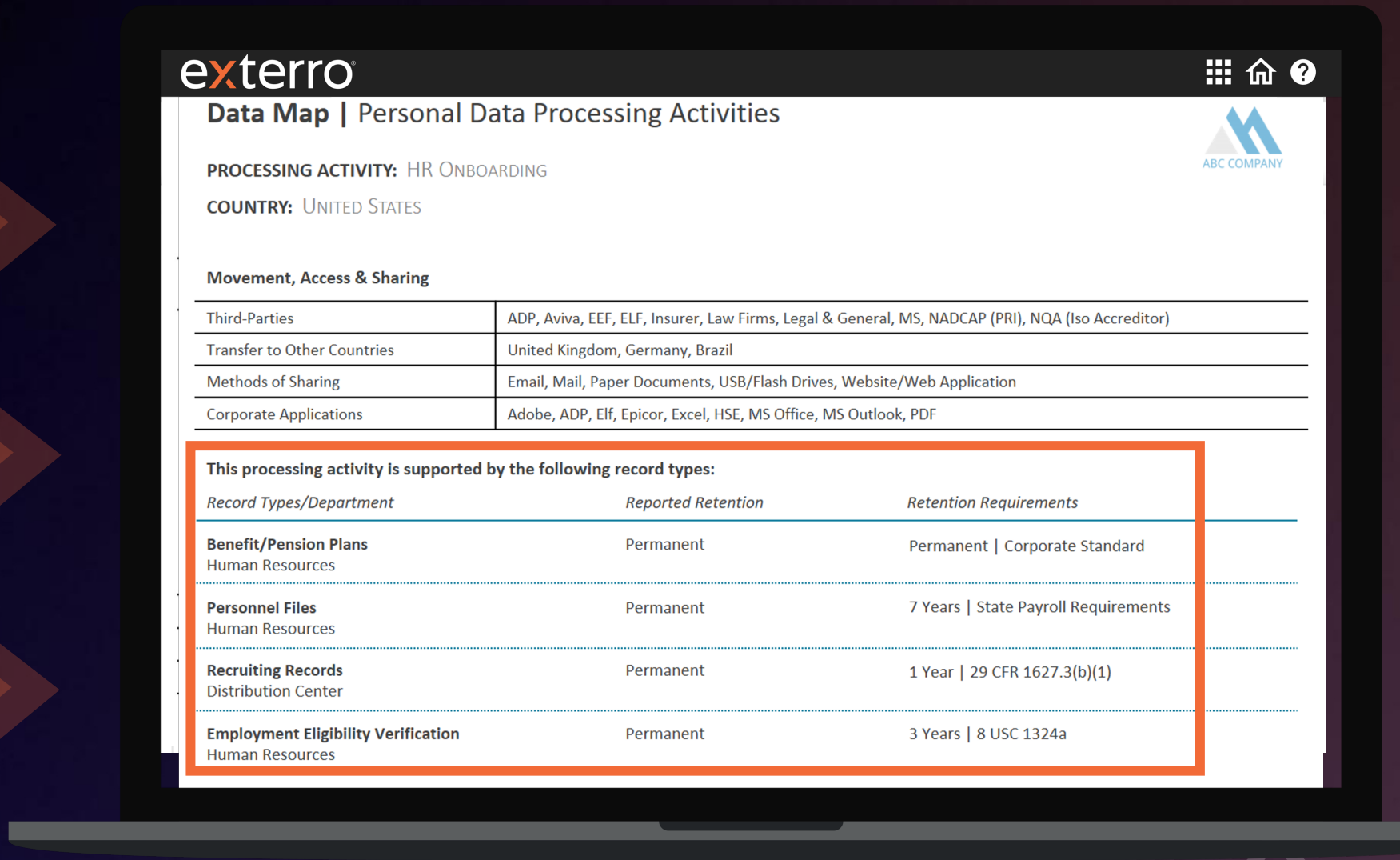
- Deletion and correction
- Do not Sell
- Responding and delivery
- Objections and other issues

LINK PERSONAL DATA PROCESSING TO RETENTION

Identify & Profile Business Processes

Link to Record Types

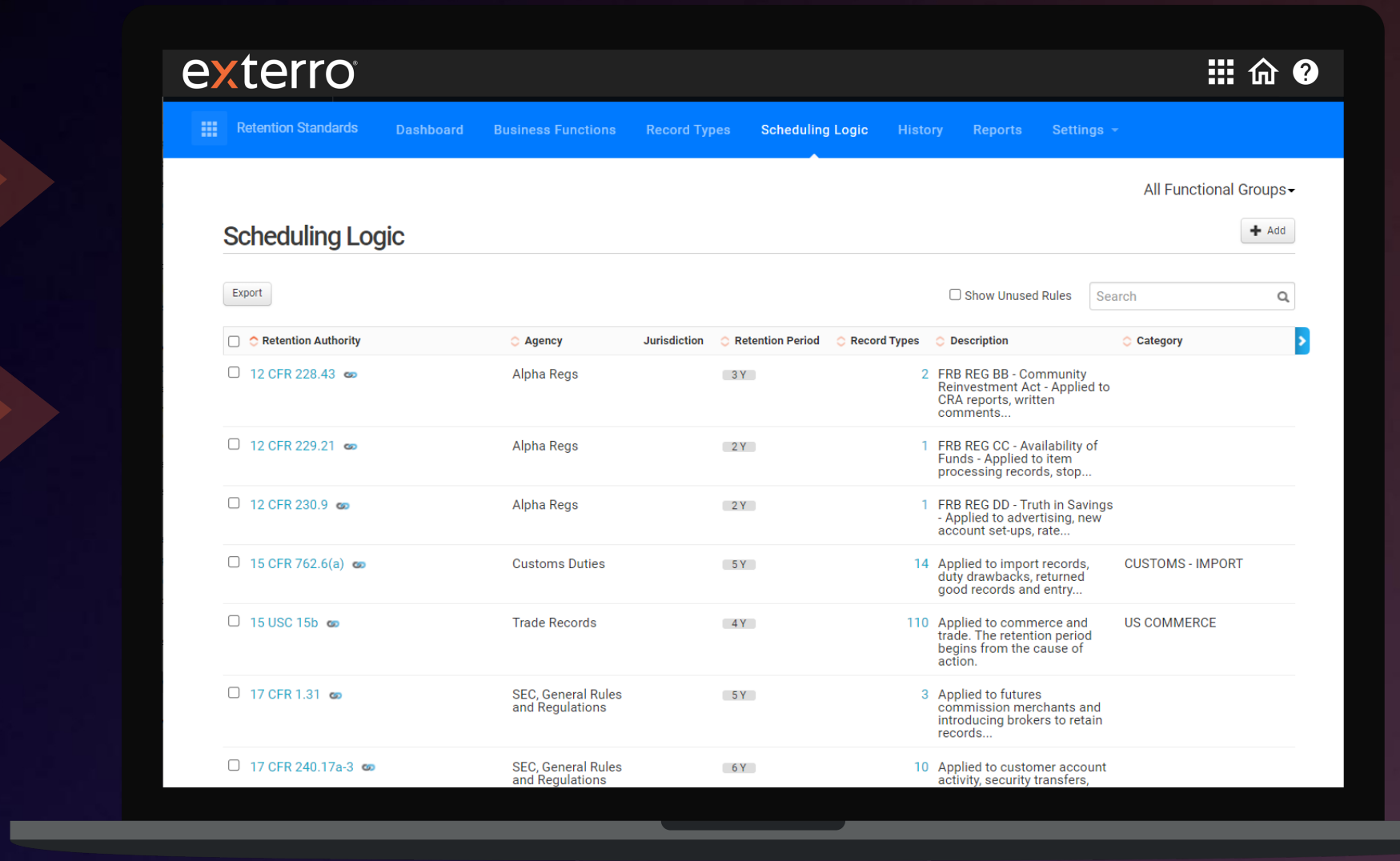
Understand Retention Requirements



DOCUMENT YOUR RETENTION DECISIONS

Global Retention Considerations

Document Decisions & Retention Logic



Strategies to address over-retention

How can we engage the organization to address over-retention?

Questions to ask in order to operationalize data retention requirements:

- What types of personal information does the business unit collect and store?
- How long does the business store the various types of personal information?
  - For what purposes (e.g., internal primary/secondary, legal, regulatory, etc.)?
- Does the business have a written retention policy and schedule? Does it follow the schedule?
- Can the business demonstrate it deletes/destroys personal information?
- Can we carve out any buckets of personal information under legal (e.g. CPRA) exemptions?
- Does the business unit disclose, publicly (e.g., in a privacy policy), the purposes for which it collects and stores personal information?
- There may be a legitimate legal or business reason for keeping data – can you articulate it?

Breaking down the silos in retention

Developing a community of interest:

- Records management (obviously)
- Information Security (risk reduction, ransomware planning)
- Information Technology (storage challenges)
- Legal (liability management)
- ESG (environmental impact)
- Finance (reducing costs)
- Cyberinsurance (reducing premiums)
- Privacy (reducing privacy risk, simplifying DSAR response)

When? (Hint: now)

On Monday

- Assess your retention schedule and records management program
- Identify leverageable technology for DSAR response
- Begin dialog with IT/HR/IG about responding to DSARs

Next Month

- Retention policy/schedule update project
- Process for including legal review in DSAR manually with consumer automation
- Link back to notice and consent relating to data retention

6 Months

- Retention notifications and implementation for consumer or employee data
- Preference management designed into all channels for non-mandatory retention
- Automated review for DSAR responses

How Exterro Helps

THE ONLY PLATFORM TO BRING IT ALL TOGETHER

Panelists

A Streamlined Process to Minimize Risks & Costs

Questions?

Constantine Karbaliotis
Senior Privacy Advisor,
Exterro

Theresa Sippert
Manager - Information Management,
Hydro Ottawa

Peter Stockburger
San Diego Managing Partner,
Dentons

Matt Dumiak
Director of Privacy Services
Compliance Point