

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



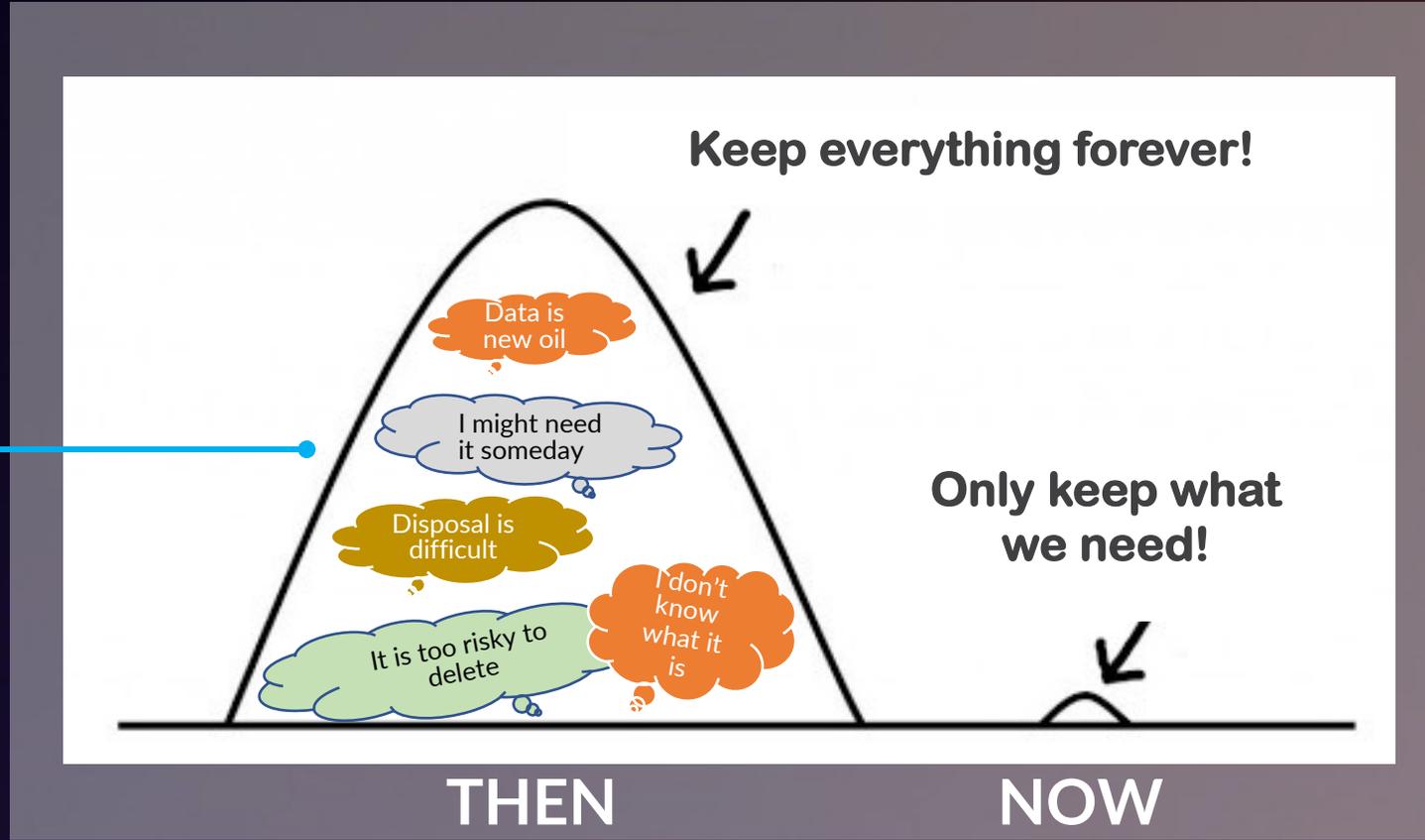
What are the risks of over-retention?



OVER-RETENTION OF PERSONAL DATA IS A LIABILITY

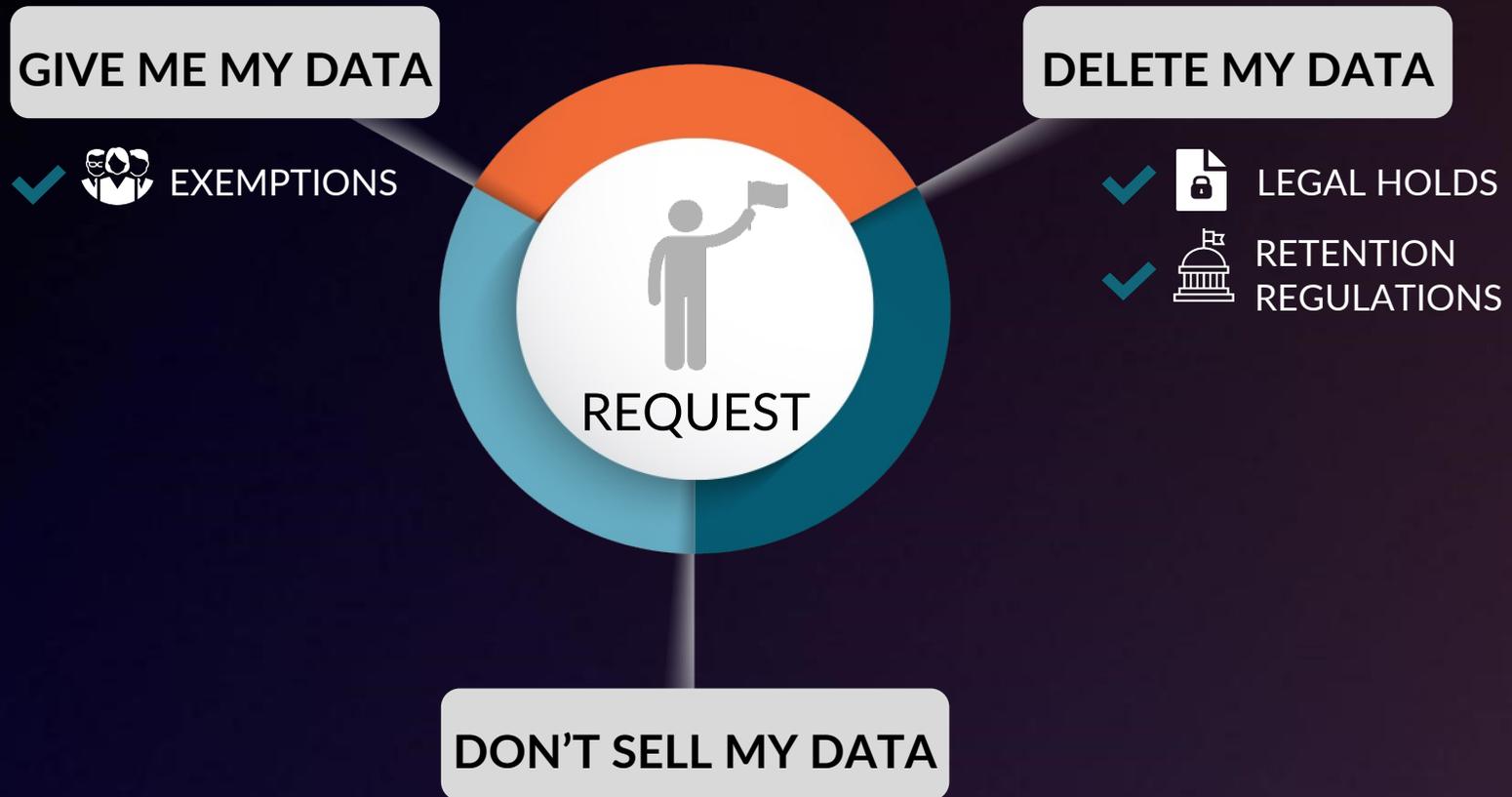
KEY RISKS:

- 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

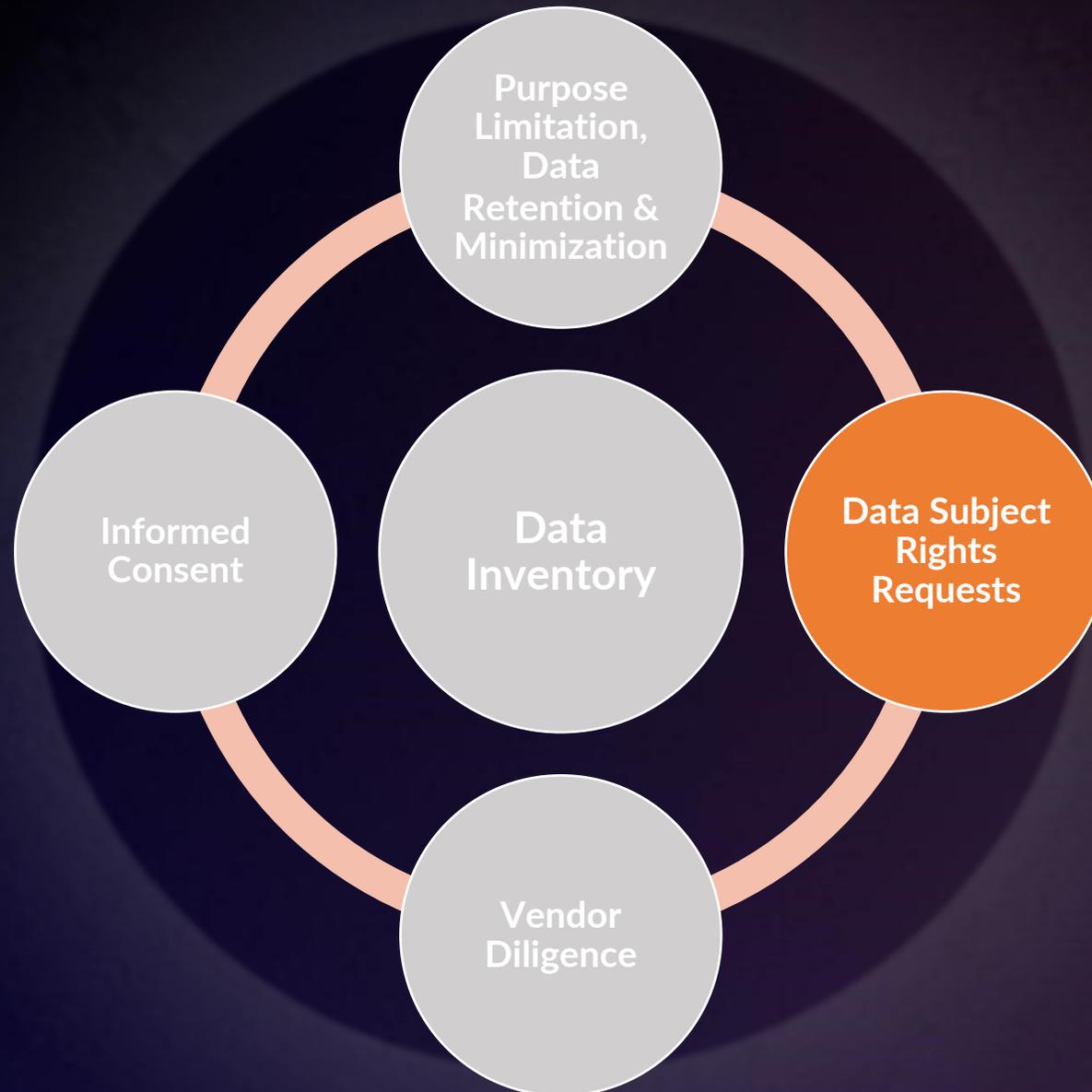


The more data you have, the harder it is to respond to DSARs

Legislative Background



COMMON ELEMENTS OF DATA PRIVACY LAWS



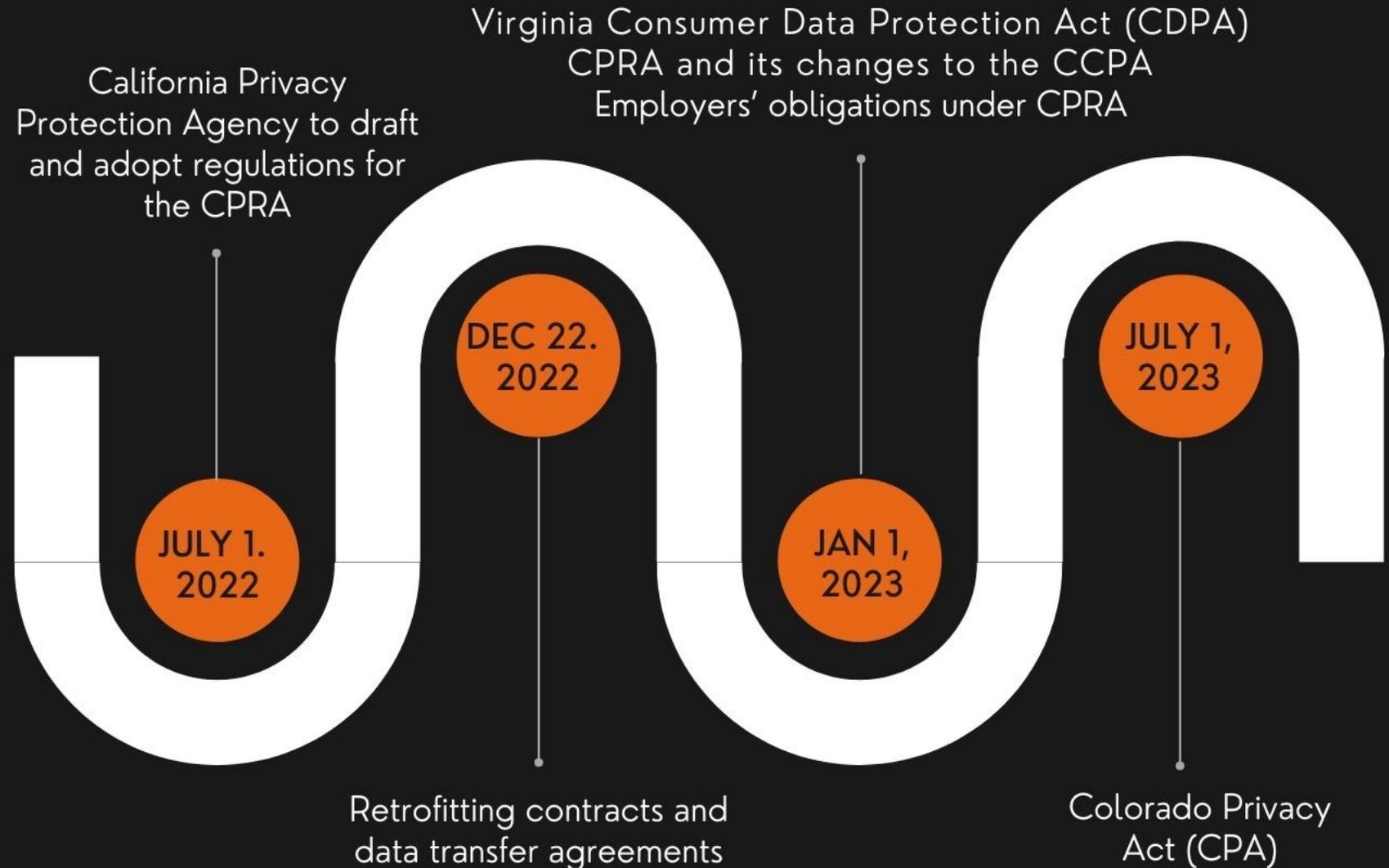
CONSUMER RIGHTS & BUSINESS OBLIGATIONS

Consumer Right	PICICA	CCPA	CPRA	CDPA	GDPR	CPA
Right to access	x	✓	✓	✓	✓	✓
Right to confirm personal data is being processed	x	Implied	Implied	✓	✓	✓
Right to data portability	x	✓	✓	✓	✓	✓
Right to delete ~	x	✓	✓	✓	✓	✓
Right to correct inaccuracies/right of rectification	x	x	✓	✓	✓	✓
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)	x	x****	✓	✓	✓	✓
Right to object to or opt-out of automated decision-making ~ ~	x	x	✓	✓	✓	✓
Opt-in or opt-out for processing of “sensitive” personal data? – “sensitive is defined differently under CPRA, CDPA and CPA	x	x	Opt-out†	Opt-in	Opt-in††	Opt-in†
Right to object to/restrict processing generally	x	x	x	x	✓	x
Right to non-discrimination	x	✓	✓	Limited	Implied	Limited
Purpose / Use / Retention Limitations	x	Implied	✓	✓	✓	✓
Applies to both consumers and in HR and B-to-B contacts	x	+	++	x	✓	x
Privacy and security impact assessments sometimes required	x	x	✓	✓	✓	✓
Obligation to maintain reasonable security	x	✓	✓	✓	✓	✓



KEY DATES

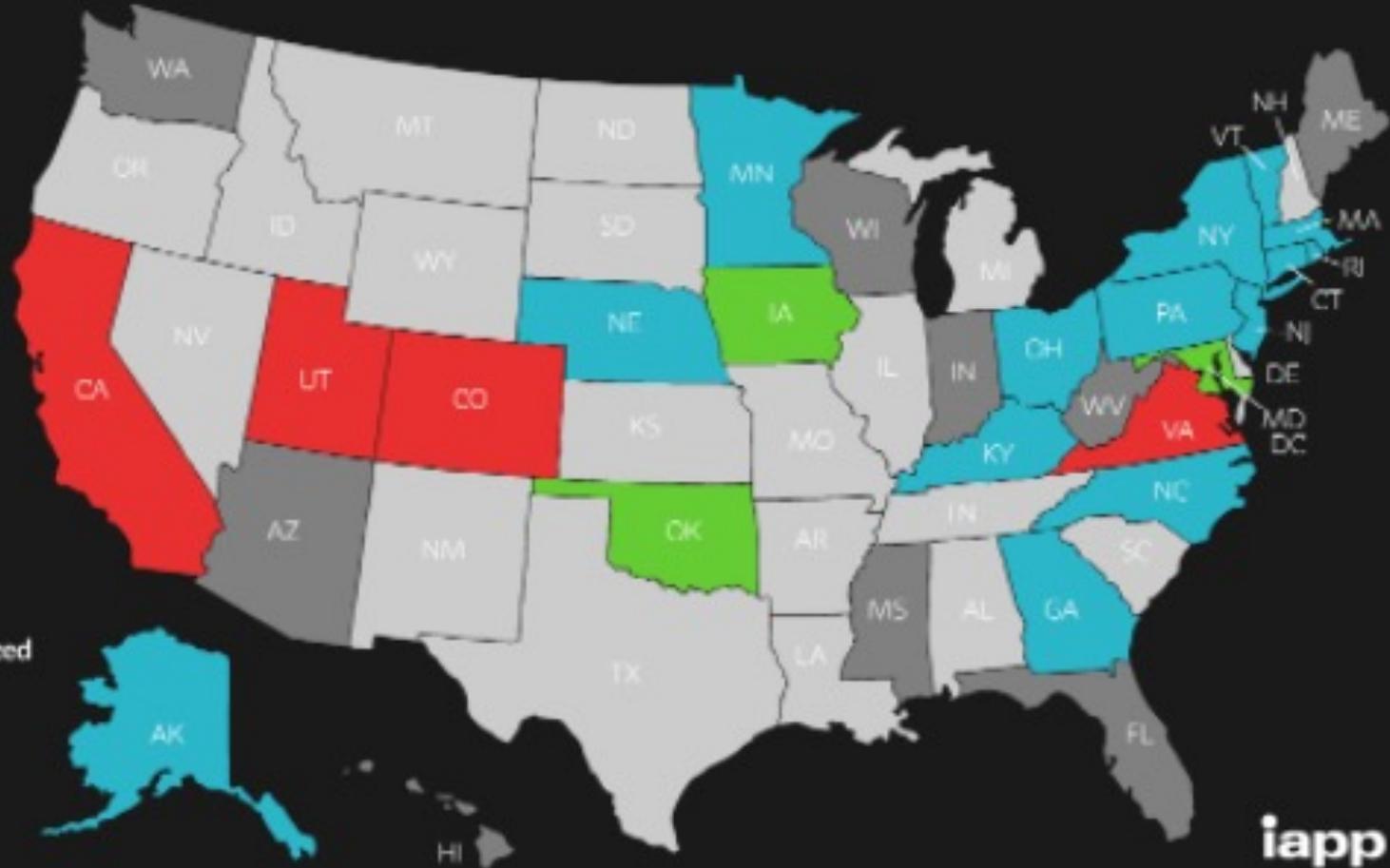
- Deadlines are fast approaching
- Draft regulations will be late



US State Privacy Legislation Tracker 2022

STATUTE/BILL IN LEGISLATIVE PROCESS

- Introduced
- In committee
- In cross chamber
- In cross committee
- Passed
- Signed
- Inactive bills
- No comprehensive bills introduced



Last updated: 3/31/2022

iapp



DATA RETENTION: POSSIBLE CPRA DISCLOSURE FORMAT

Category of PI	Purposes	Retention Period
Identifiers - Name, postal address, Internet Protocol address and email address.	<ol style="list-style-type: none"> 1. Performing Services 2. Short-term Transient Use (e.g., to serve contextual ads) 	<ol style="list-style-type: none"> 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



LINK PERSONAL DATA PROCESSING TO RETENTION

Identify & Profile
Business Processes

Link to Record Types

Understand Retention
Requirements

exterro ABC COMPANY

Data Map | Personal Data Processing Activities

PROCESSING ACTIVITY: HR ONBOARDING
COUNTRY: UNITED STATES

Movement, Access & Sharing

Third-Parties	ADP, Aviva, EEF, ELF, Insurer, Law Firms, Legal & General, MS, NADCAP (PRI), NQA (Iso Accreditor)
Transfer to Other Countries	United Kingdom, Germany, Brazil
Methods of Sharing	Email, Mail, Paper Documents, USB/Flash Drives, Website/Web Application
Corporate Applications	Adobe, ADP, Elf, Epicor, Excel, HSE, MS Office, MS Outlook, PDF

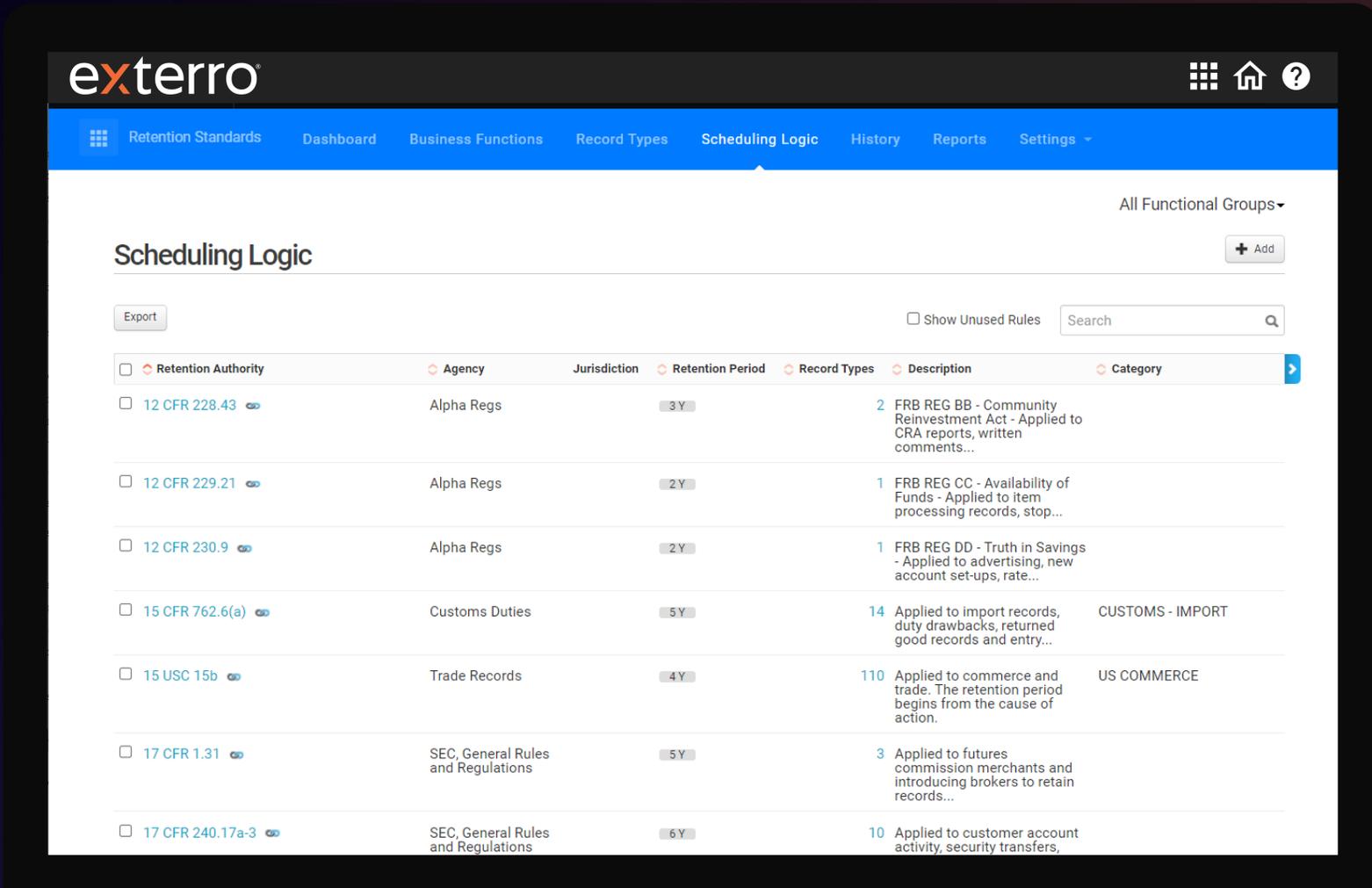
This processing activity is supported by the following record types:

Record Types/Department	Reported Retention	Retention Requirements
Benefit/Pension Plans Human Resources	Permanent	Permanent Corporate Standard
Personnel Files Human Resources	Permanent	7 Years State Payroll Requirements
Recruiting Records Distribution Center	Permanent	1 Year 29 CFR 1627.3(b)(1)
Employment Eligibility Verification Human Resources	Permanent	3 Years 8 USC 1324a

DOCUMENT YOUR RETENTION DECISIONS

Global Retention Considerations

Document Decisions & Retention Logic



The screenshot displays the Exterro Scheduling Logic interface. The header includes the Exterro logo and navigation tabs: Retention Standards, Dashboard, Business Functions, Record Types, Scheduling Logic (active), History, Reports, and Settings. The main content area is titled "Scheduling Logic" and features an "Export" button, a "Show Unused Rules" checkbox, and a search bar. Below this is a table of retention rules with columns for Retention Authority, Agency, Jurisdiction, Retention Period, Record Types, Description, and Category.

<input type="checkbox"/>	Retention Authority	Agency	Jurisdiction	Retention Period	Record Types	Description	Category
<input type="checkbox"/>	12 CFR 228.43	Alpha Regs		3 Y		2 FRB REG BB - Community Reinvestment Act - Applied to CRA reports, written comments...	
<input type="checkbox"/>	12 CFR 229.21	Alpha Regs		2 Y		1 FRB REG CC - Availability of Funds - Applied to item processing records, stop...	
<input type="checkbox"/>	12 CFR 230.9	Alpha Regs		2 Y		1 FRB REG DD - Truth in Savings - Applied to advertising, new account set-ups, rate...	
<input type="checkbox"/>	15 CFR 762.6(a)	Customs Duties		5 Y		14 Applied to import records, duty drawbacks, returned good records and entry...	CUSTOMS - IMPORT
<input type="checkbox"/>	15 USC 15b	Trade Records		4 Y		110 Applied to commerce and trade. The retention period begins from the cause of action.	US COMMERCE
<input type="checkbox"/>	17 CFR 1.31	SEC, General Rules and Regulations		5 Y		3 Applied to futures commission merchants and introducing brokers to retain records...	
<input type="checkbox"/>	17 CFR 240.17a-3	SEC, General Rules and Regulations		6 Y		10 Applied to customer account activity, security transfers,	

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