ROADMAP

60 Days To CPRA Compliance

exterro®

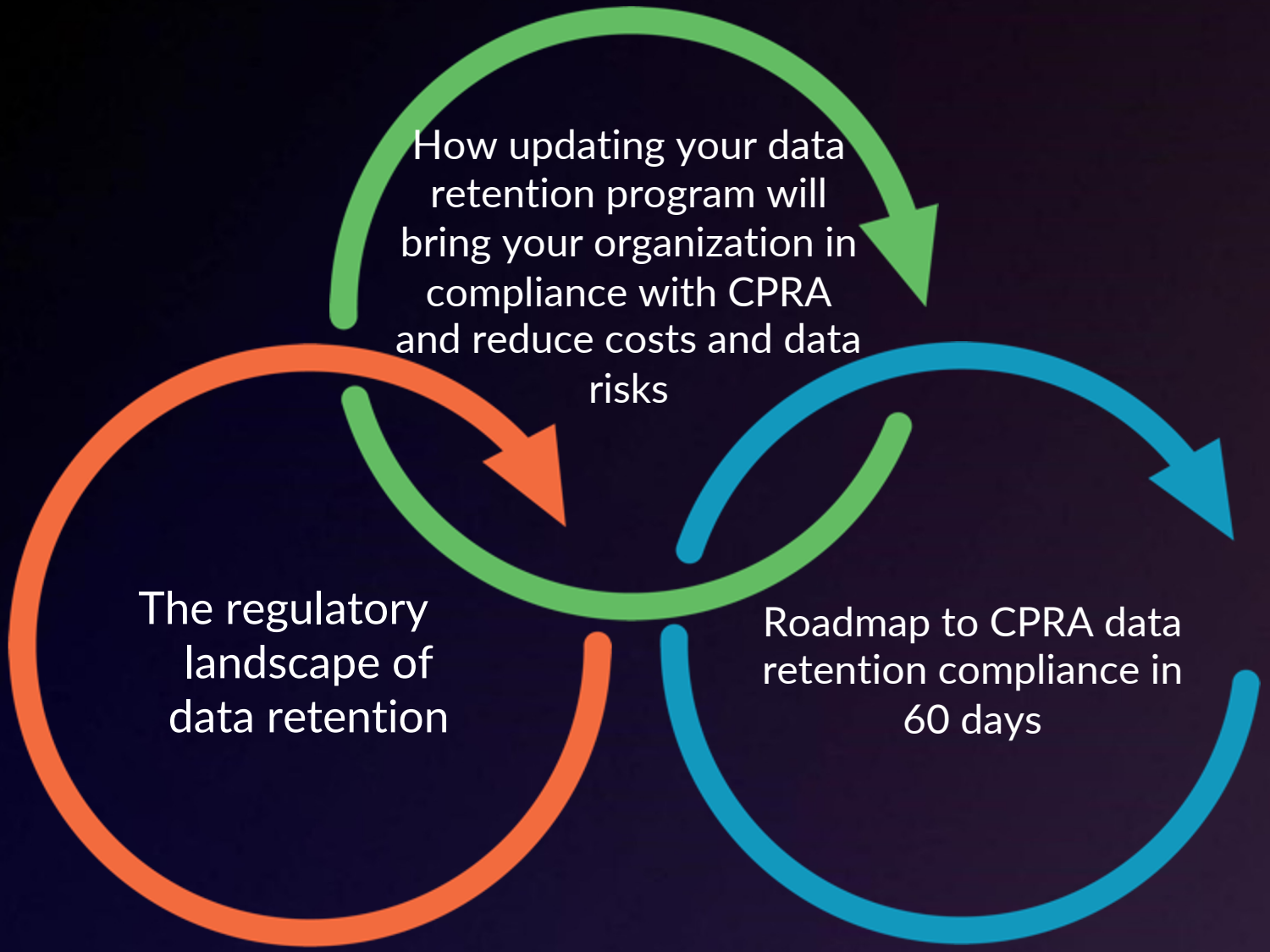
Today's Panelists

Robert Fowler
Director of Strategic Partnerships, Exterro
Robert.Fowler@exterro.com

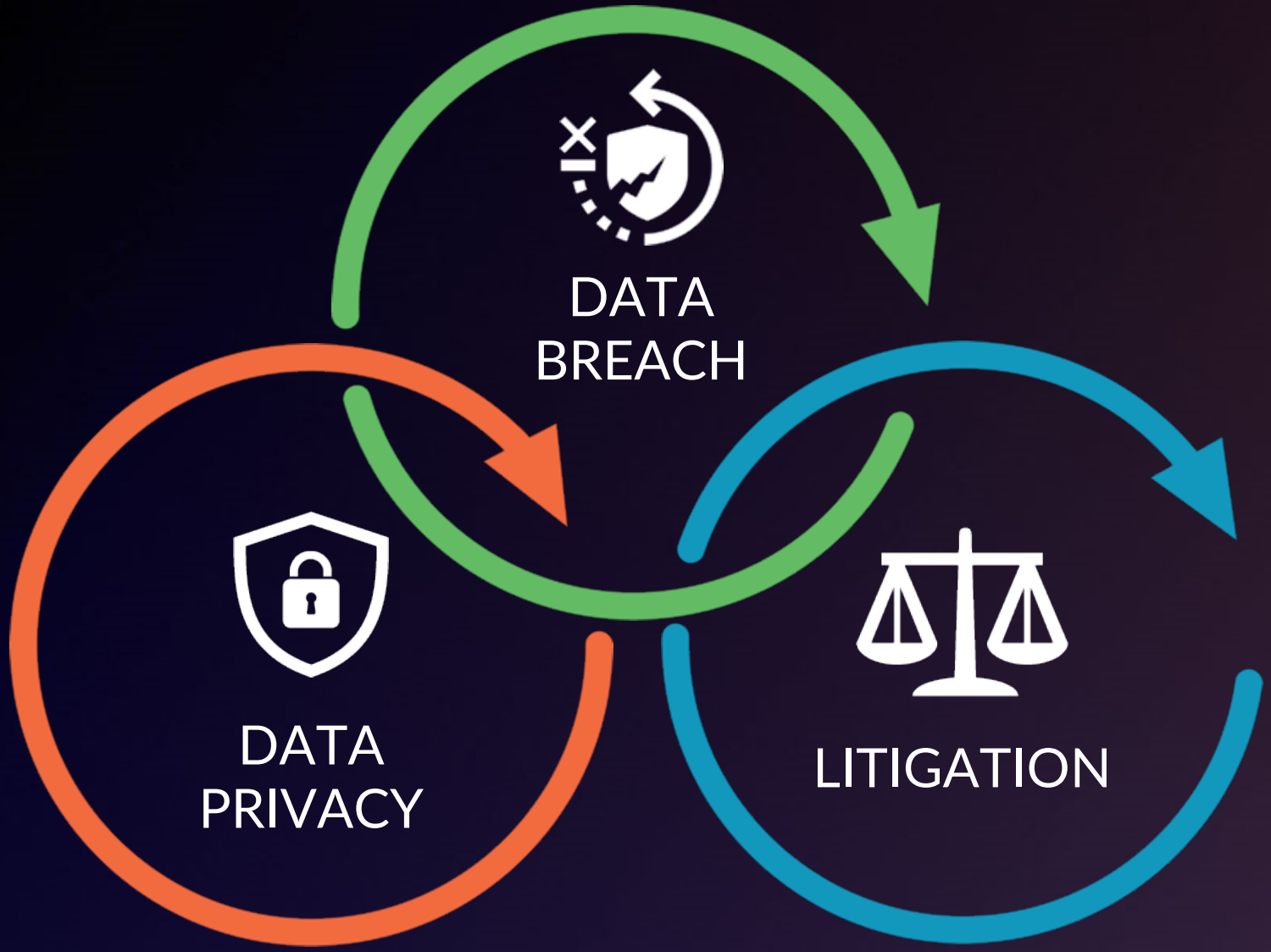
Mary Blatch
Regulatory Counsel and Data Privacy Officer
CFA Institute
Mary.Blatch@cfainstitute.org

Iliana Peters
Shareholder
Polsinelli
ipeters@polsinelli.com

In this webcast our panel will review…



THE CASE FOR DATA RETENTION



Expanding Data Privacy Regulations

Evolving Regulatory Landscape

CONTROLLER OBLIGATIONS	GDPR	CDPA VIRGINIA	CCPA CALIFORNIA	CPRA CALIFORNIA	CPA COLORADO	PIPEDA CANADA (Bill C-11)
Data Minimization	Yes	Yes	No	Yes	Yes	Yes
Purpose Limitation	Yes	Yes	Yes	Yes	Yes	Yes
Security Requirements	Yes	Yes	No, but the private right of action applies to security breaches	Yes	Yes	Yes
Consent for sensitive data	While consent is required for special category processing, no express right to withdraw consent	Yes	No	No, consumers can limit use to what is reasonably necessary	Yes	Yes - OPC Guidance Yes
Special requirements for children's data	Yes (children under 16 must have their parents' or guardians' consent on their behalf, with Member States being allowed to lower that age to 13)	Yes (sensitive data of children under 13 years of age)	Yes (sale of personal information of children under 16 years of age and under 13 years of age	Yes (sale of Personal information of children under 16 years of age and under 13 years of age	Yes (personal data for a known child under 13 years of age)	Yes – OPC Guidance Yes
Privacy Notice	Yes	Yes	Yes	Yes	Yes	Yes
Disclose sale	Yes, (as part of larger right to object to legitimate interest or withdraw consent)	Yes	Yes	Yes	Yes	No? Yes?
Data protection assessment	Yes	Yes	No	Yes, Risk assessments submitted to CA Privacy Protection Agency	Yes, available upon request by CO AG	Yes
Requirement for de-identified data	Yes (Strict definition of terms)	Yes (Qualifying attributes)	Yes (strict definition, limitation on "publicly available)	Yes (CCPA + public commitment)	Yes	No Yes

California Privacy Rights Act

- Key Dates
  - 1/1/2022 – Lookback period begins
  - 7/1/2022 – Final Regulations
  - 7/1/2023 – Enforcement begins
- California Privacy Protection Agency
- End of employee exemption
- Notification of retention periods at the point of collection
- Disposal of out of policy data

1798.100. General Duties of Businesses that Collect Personal Information

(a) A business that controls the collection of a consumer's personal information shall, at or before the point of collection, inform consumers of the following:

(3) The length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine such period, provided that a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose.

Data Retention Principles

- Transparency / Notice
- Data Minimization
- Purpose Limitation
- Storage Limitation

Over Retaining Personal Data is a Liability

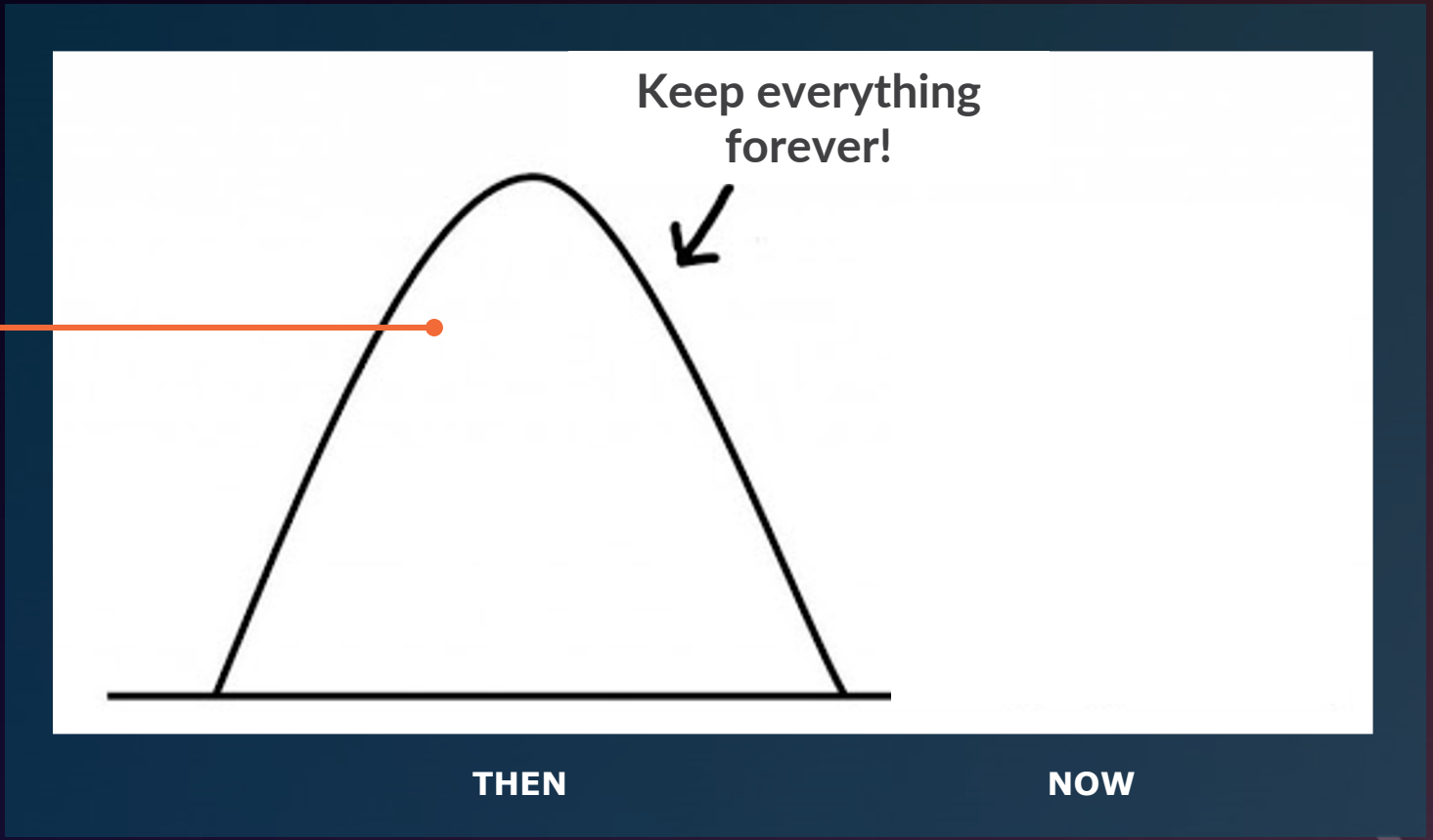
75%

OF RECORD TYPES WITH PERSONAL DATA ARE **OVER RETAINED**

Over-Retaining Personal Data is a Liability!

KEY RISKS:

- Data Breach
- Ransomware Attack
- Enforcement Action
- Class Action
- Business Email Compromise



COMMON PAIN POINTS

THE PLAN

- No retention policy
- Out of date retention policy
- Not executed or put into effect

THE PROCESS

- Ad-hoc processes for managing retention plans
- Ad-hoc processes for inventorying records types
- Manual workflow processes to delete information

THE PEOPLE

- Don't have correct stakeholders at the table (Legal, Privacy, IT, HR)
- Data management teams lacking authority
- Employee roles and response

DEFENSIBILITY

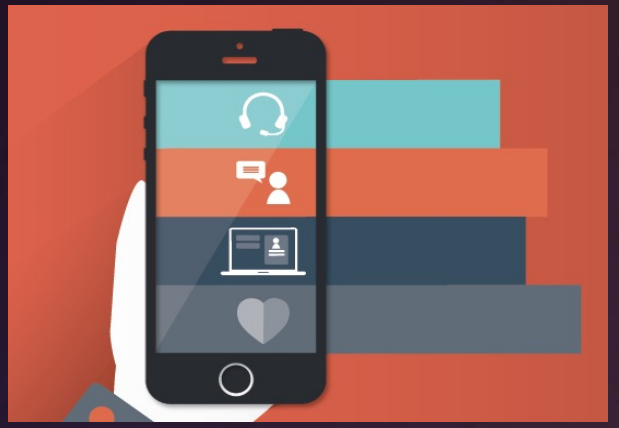
- Failure to operationalize policy
- Failure to document process
- Failure to maintain audit log of compliance to delete information

Retention Regulations Based on Context of Collection

RECRUITING RECORDS

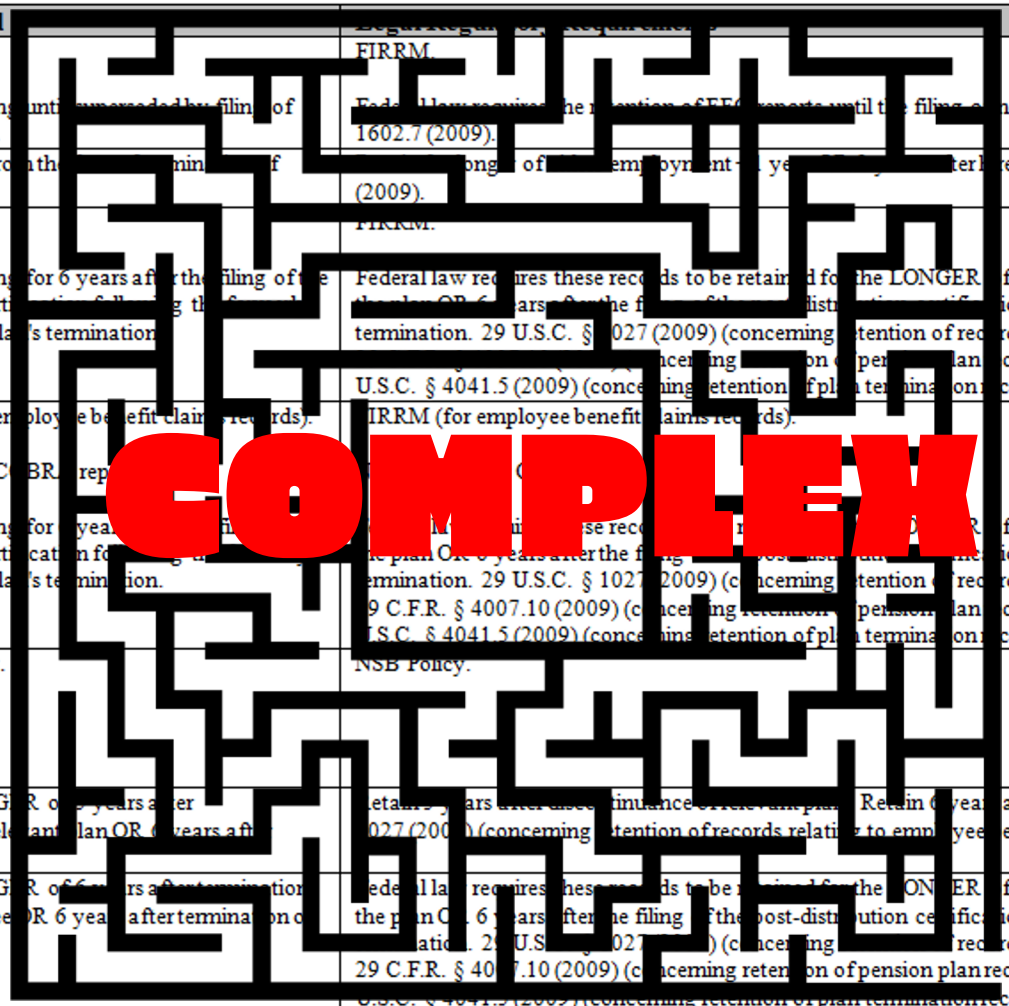
BENEFITS ENROLLMENT

CUSTOMER **SERVICE**



ABC Company's Records Retention Schedule

Record Category	Retention Period	Legal Requirements	Custodian
EEO-1 and EEO-2 Employer Information Reports and Affirmative Action Reports	Retain 10 years. CONSIDER retaining [illegible] new relevant report.	FIRRM. Federal law requires the retention of EEO reports until the filing of new annual reports. 29 C.F.R. § 1602.7 (2009).	Human Resources
I-9 Immigration Forms	Retain for 3 years from the [illegible] relevant employee.	[illegible] longer of [illegible] employment + 1 year [illegible] later [illegible]. 8 C.F.R. § 274A.2(b)(2)(i)(A) (2009).	Human Resources
Employee Benefit Plan Records (Plan Statements and Descriptions, Annual Reports)	Retain 7 years. CONSIDER retaining for 6 years after the filing of the post-distribution certification following the plan's ongoing or frozen plan's termination.	FIRRM. Federal law requires these records to be retained for the LONGER of 6 years after either the filing of the plan OR 6 years after the filing of the post-distribution certification following the plan's termination. 29 U.S.C. § 1027 (2009) (concerning retention of records relating to employee benefits); 29 C.F.R. § 4007.10 (2009) (concerning retention of pension plan records subject to ERISA); 29 U.S.C. § 4041.5 (2009) (concerning retention of plan termination records subject to ERISA).	Human Resources
Employee-Specific Benefit Records (Claim Records, COBRA Records, 401(k) Records, Life Insurance Distribution Records)	Retain 7 years (for employee benefit claim records). Retain 3 years (for COBRA records). CONSIDER retaining for 6 years after the filing of the post-distribution certification following the plan's ongoing or frozen plan's termination.	FIRRM (for employee benefit claims records). [illegible] these records [illegible] the LONGER of 6 years after either the filing of the plan OR 6 years after the filing of the post-distribution certification following the plan's termination. 29 U.S.C. § 1027 (2009) (concerning retention of records relating to employee benefits); 29 C.F.R. § 4007.10 (2009) (concerning retention of pension plan records subject to ERISA); 29 U.S.C. § 4041.5 (2009) (concerning retention of plan termination records subject to ERISA).	Human Resources
Employee Benefit Account Records (Files and Deferred Vested Files, Records Regarding Loans to Employees, Officers, and Directors, Thrift Plan A1 Reports)	Retain permanently.	NSB Policy.	Human Resources
Employee Benefit Plan Annual Reports (Form 5500s) and Supporting Documentation	Retain for the LONGER of [illegible] years after discontinuance of relevant plan OR [illegible] years after relevant filing.	[illegible] years after discontinuance of relevant plan. Retain [illegible] years after relevant filing. 29 U.S.C. § 1027 (2009) (concerning retention of records relating to employee benefits).	Human Resources
HIPAA Compliance Records	Retain for the LONGER of [illegible] years after termination of relevant employee OR 6 years after termination of relevant plan.	Federal law requires these records to be retained for the LONGER of 6 years after either the filing of the plan OR 6 years after the filing of the post-distribution certification following the plan's termination. 29 U.S.C. § 1027 (2009) (concerning retention of records relating to employee benefits); 29 C.F.R. § 4007.10 (2009) (concerning retention of pension plan records subject to ERISA); 29 U.S.C. § 4041.5 (2009) (concerning retention of plan termination records subject to ERISA).	Human Resources
HIPAA Disclosure Records	Retain for the LONGER of 6 years after the creation of the record OR 6 years after the program to which the record relates is no longer in effect.	Retain for the LONGER of 6 years after the creation of the relevant record OR 6 years after the program to which the relevant record relates is no longer in effect. 45 C.F.R. §§ 164.105(c), 164.316(b), 164.530(j) (2009).	Human Resources

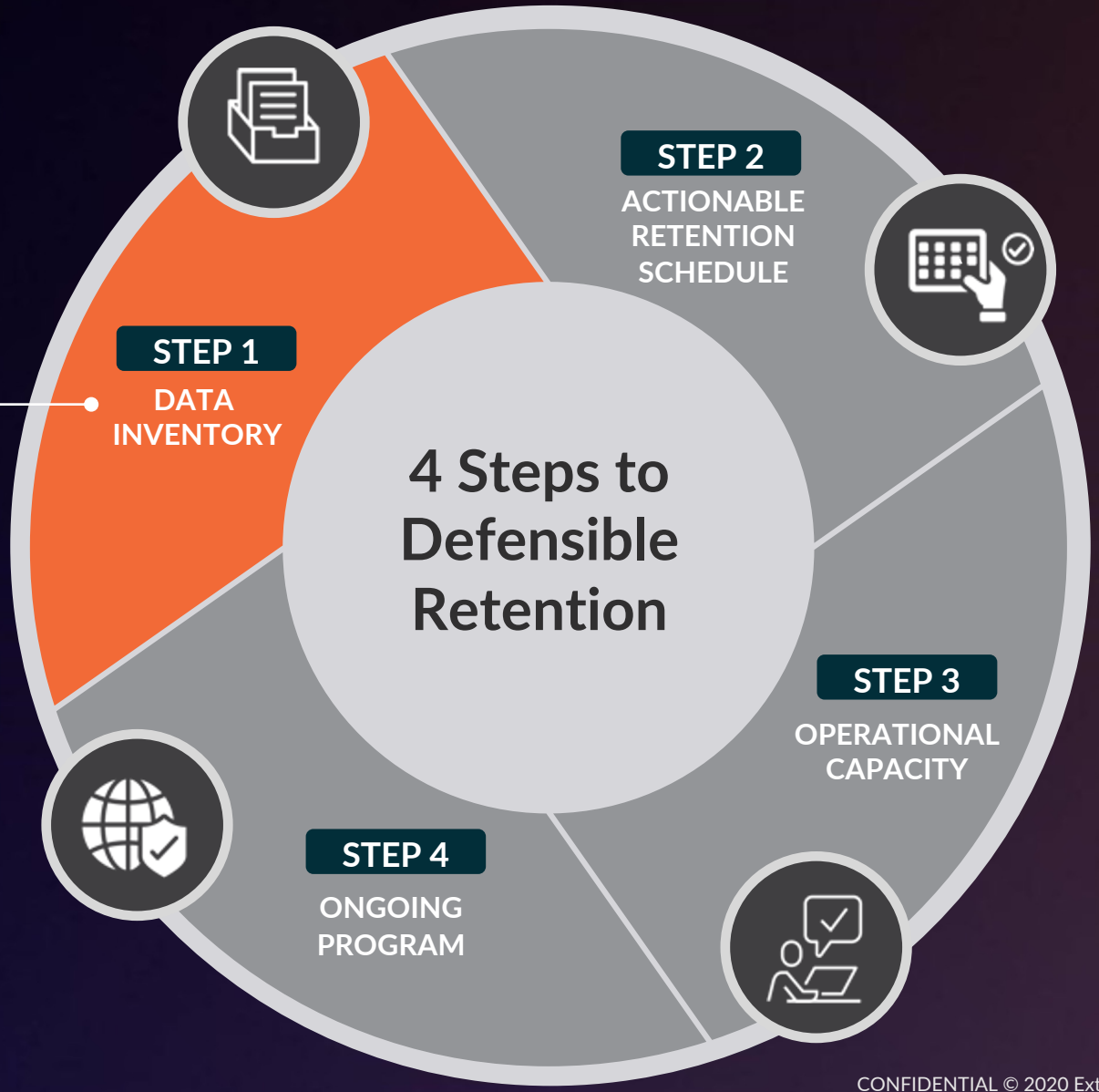


4 Steps to Defensible Data Retention

The Foundation for Defensible Retention & Deletion

Three Types of Data Inventory

1. Asset Inventory
2. Process Inventory
3. Records Inventory



Linking Personal Data to Retention Requirements

	CONSUMER DATA	EMPLOYMENT/CORPORATE DATA
APPLICABILITY	GLBA	HIPAA, NAIC National Association of Insurance Commissioners, FEDERAL TRADE COMMISSION
DATA SUBJECTS	Consumers	Current Employees | Past Employees | Job Candidates | Beneficiaries |
DATA ELEMENTS	Account # | Alias | Email Address | Preferences | Attitudes | Geolocation | IP Address | Cookie ID	Social Security # | Drivers' License # | Biometric Identifier | Aptitudes | Bank Routing # | Military Status | Certifications
COLLECTION	Mobile App, Web, Email, Phone	Web Form, Email, Paper Form
DEPARTMENTS	Marketing | Digital Engagement | Product Development | Customer Service | Research & Development	Benefits | Payroll | Recruiting | EH&S | Training & Development | Employee Relations
APPLICATIONS	salesforce, SalesLoft, Magento, snowflake	SAP, workday, ORACLE, KRONOS
LOCATIONS	Office 365, SharePoint, Laptops	Office 365, box, SharePoint, Laptops, File Cabinets
THIRD PARTIES	sproutsocial, SILVERPOP, shopify, Five9	ADP, LabCorp, Cigna, IRON MOUNTAIN
RETENTION	Customer Orders Customer Complaints Warranty Information	Payroll Records Personnel Records Recruiting Records AUT 7 Years BEL 5 Years NLD 5 Years ITA 5 Years USA 7 Years

Linking Personal Data to Retention Requirements

Data Map | Personal Data Processi

PROCESSING ACTIVITY: HR ONBOARDING

COUNTRY: UNITED STATES

Purpose of Processing		C P
Associated Data Elements	Biometric	N
	Genetic	N
	Protected Health	C
	Sensitive Personal	C
	Personal Information	A
		N
		G
		P
Data Subjects		C
Types of Notice Provided		D
Consent Received from Subject		Y

Data Map | Personal Data Processing Activities

ABC COMPANY

PROCESSING ACTIVITY: HR ONBOARDING

COUNTRY: UNITED STATES

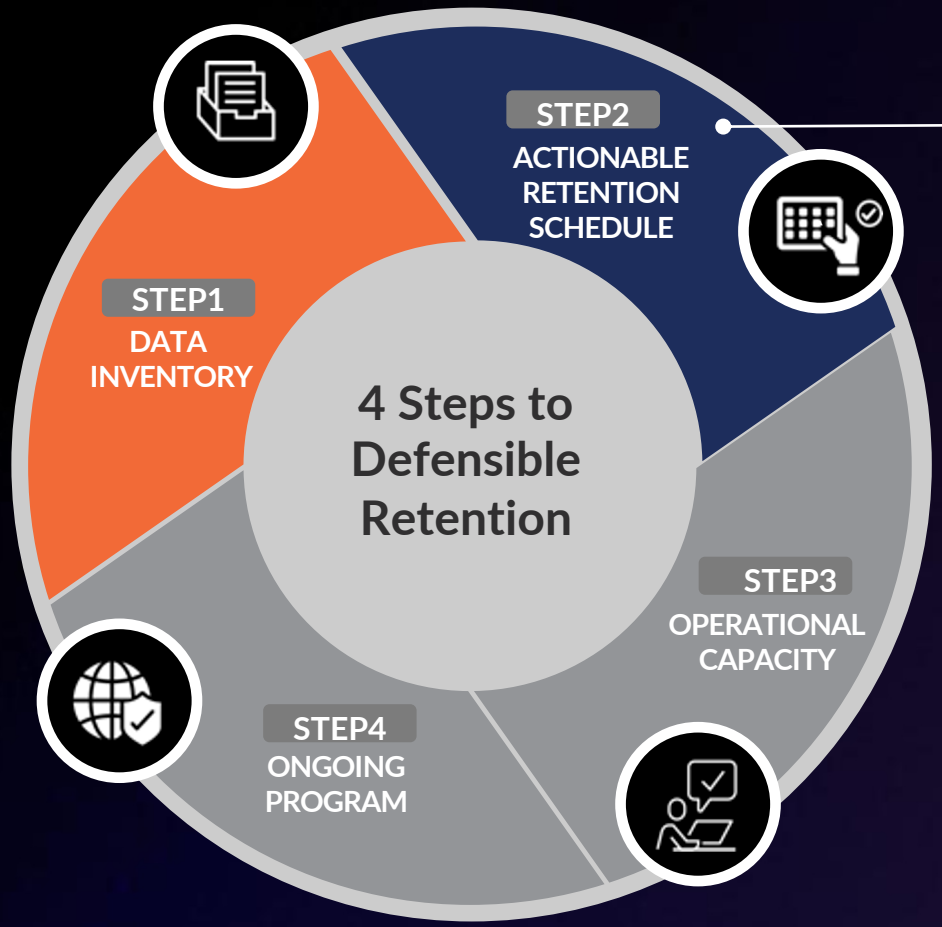
Movement, Access & Sharing

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

Exterro 60 days to CPRA Readiness



- Data Retention Policy & Scheduling Logic
- Records Types Linked to Record of Processing Activities & Applications
- Completed within Exterro Privacy Platform
- Retention Risk Analysis Report
  - Gaps
  - Risks
  - Next Steps

Global Retention Considerations

Benefit Enrollment & Participation Records

Reported Retention
-(9), 0(7), 1(1), 2(3), 5(1), PERM(9)

Employee Medical Records

Reported Retention
-(8), 0(4), 1(2), 4(1), 5(5), 7(3), 10(3), PERM(16)

Employment Equality Compliance Records

Reported Retention
-(1), 0(1), 2(1), PERM(2)

Operational Capacity

- Risk Reduction requires defensibility
- Must be SOP
- The technical challenge is not complexity but volume

• ERP • CRM • Loyalty	• Data Lake • ODS • Marketing	• Email • Website • Chat logs	• POS • Field Service

Track Your Legal Holds

- ✓ Initiate a Legal Hold Notice when practicable upon anticipation of litigation
- ✓ Don’t over-preserve
  - Don’t follow a “fear-based” strategy
  - Use spreadsheets or software to track legal holds
- ✓ Promptly lift legal holds when matters end
  - Go back to deleting data that is outdated

Ongoing Program Construction

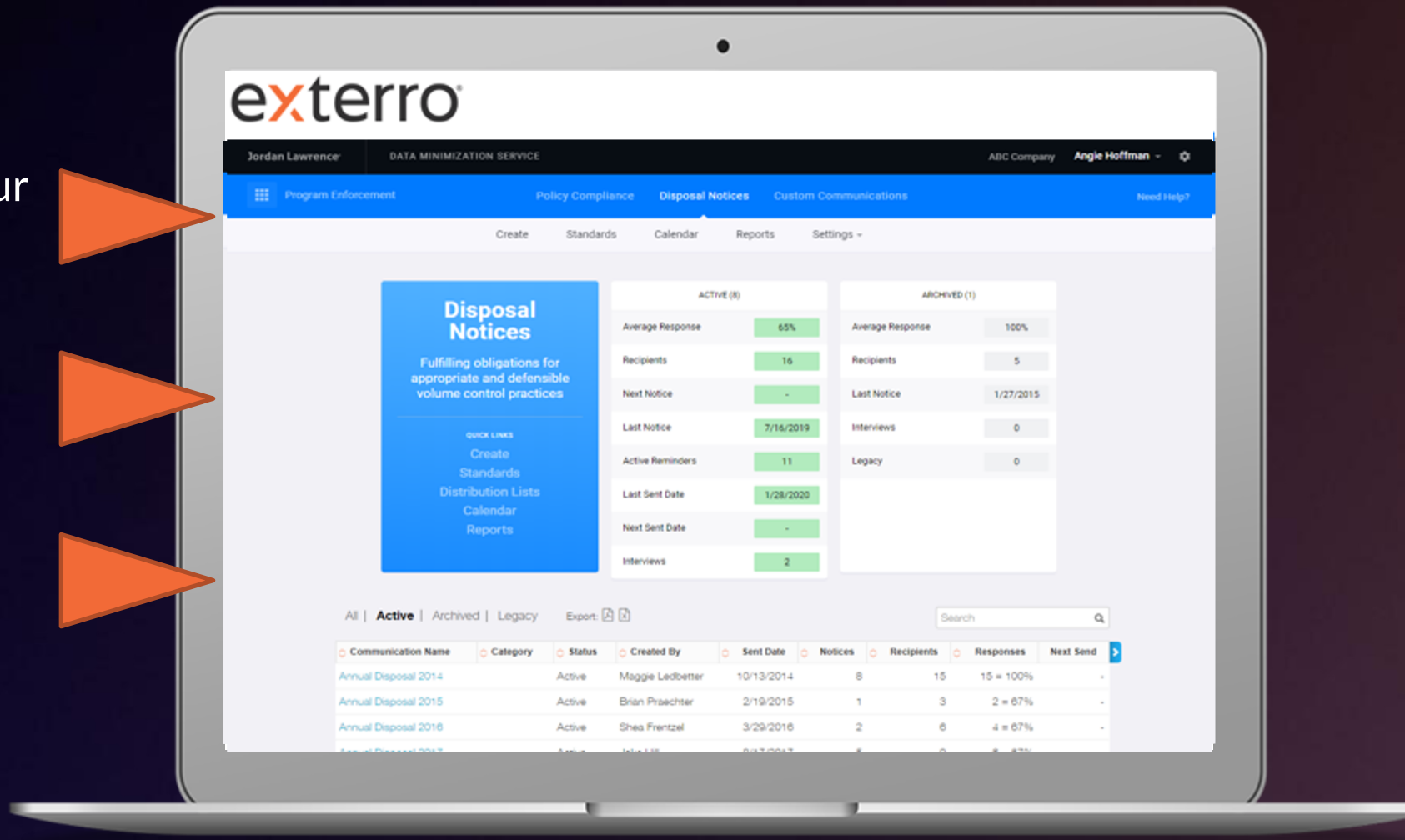
- Program leadership and ownership/RACI
- Staffing
- Budget
- KPIs and objectives
- Automation
  - Information Governance
  - Retention Schedule updates

Ongoing Program Construction

Centralized management of your retention standards

Regular notices at scheduled intervals

Disposal notices to employees noting their records retention requirements



Automation - Key to an Effective Retention Process

Centralized Data Inventory Linking All Critical Elements

- Record Types
- Retention Requirements
- Processing Activities
- Third Parties
- Applications
- Media Types

Connect Data Inventory to Global Library of Retention Requirements

Centralize & Memorialize Retention Schedules & Decisions

Automate Triggers to Kickoff Retention Clock

Activate Retention Decisions through Automated Workflows

Dynamic & Instantaneous Reporting for Internal & External Stakeholders

Complete Audit Log

exterro Data Retention & Deletion

QUESTIONS?

Thank You!

Robert Fowler
Director of Strategic Partnerships, Exterro
Robert.Fowler@exterro.com

Mary Blatch
Regulatory Counsel and Data Privacy Officer
CFA Institute
Mary.Blatch@cfainstitute.org

Iliana Peters
Shareholder
Polsinelli
ipeters@polsinelli.com