

Alleviating Data Privacy Concerns with Knowing Your Data

exterro®



Speakers:



Robert Fowler,
Director of Strategic Partnerships,
Exterro



Michael Kallens,
Associate General Counsel –
Ethics Compliance, Nasdaq



Audrey Jean,
SVP, Privacy Officer &
Senior Associate General Counsel,
AARP

In this webcast, our panel will review...

New regulatory mandates requiring a new approach to maintaining corporate data

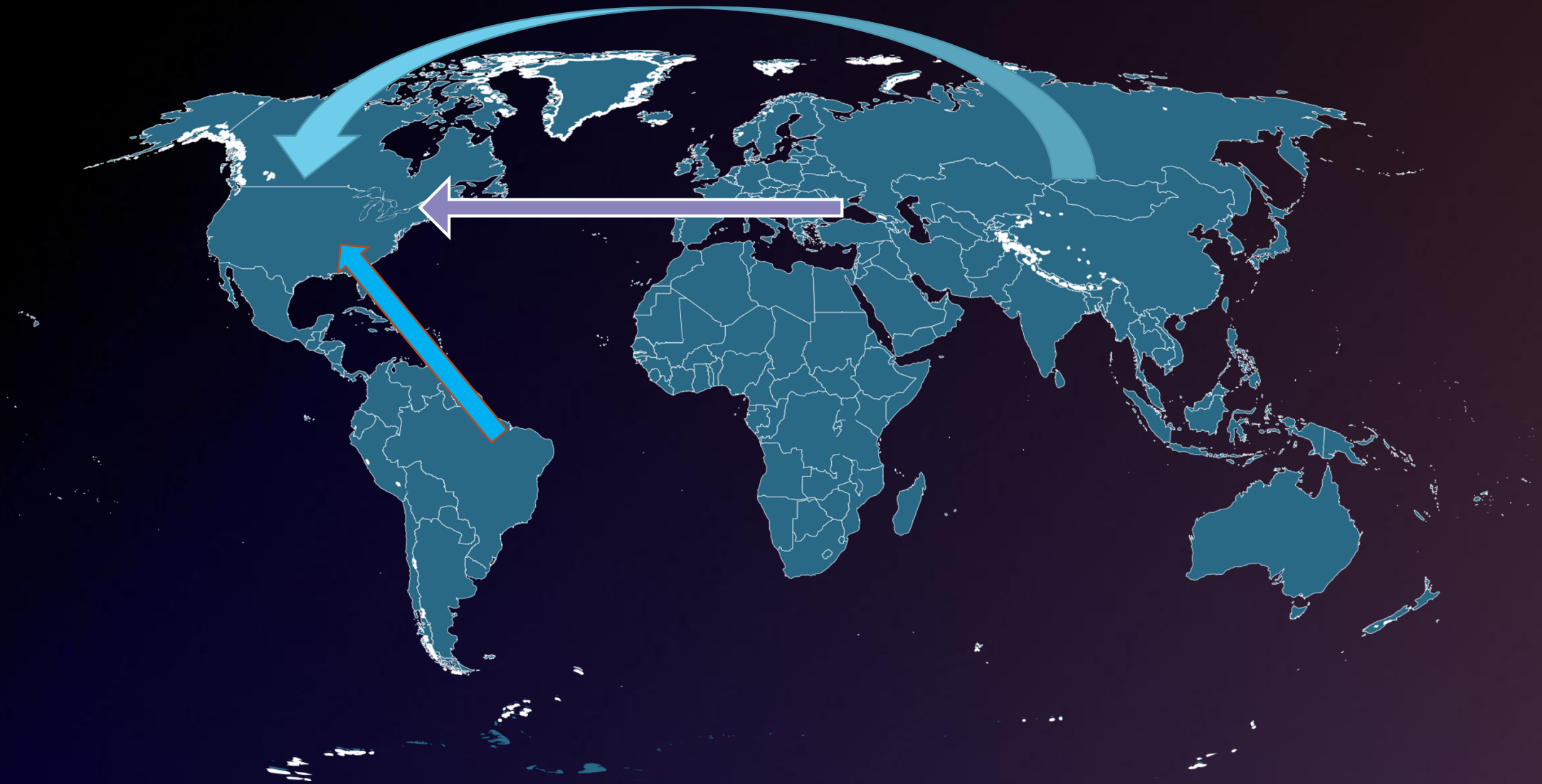
Best practices to ensure a defensible and compliant process

Use cases for leveraging technology to help develop a data inventory and to defensibly minimize data

Today's Complex Data Environment



Migrating from Abroad to the US



Pioneering US Privacy Laws – CCPA



A New Era of Data Privacy Rights

1. Right to Know Data Collected & Purpose
2. Right to Access Data
3. Right to Delete Data
4. Right to Know Categories of Third Parties
5. Right to Opt-Out of Sale
6. Right to Equal Treatment



Plaintiffs' Attorneys Lay Groundwork for BROAD PRIVATE RIGHT OF ACTION...

21

class actions filed referencing
CCPA **since January 1**

90%

of actions claim **negligence
or non-data breach claims**
as primary theory



CCPA 2.0

California Privacy Rights Act

[Ballot Initiative]

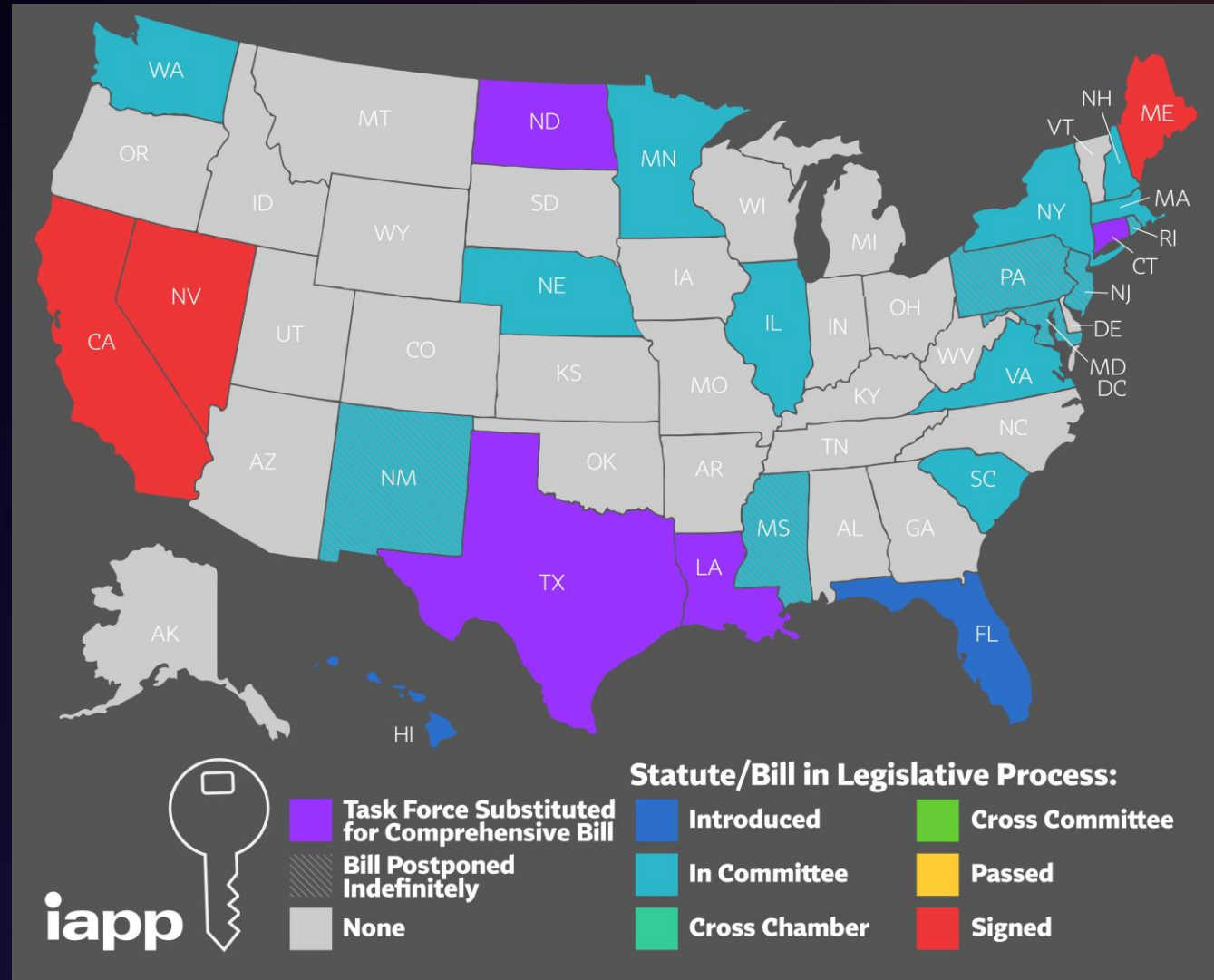
CALIFORNIANS FOR CONSUMER PRIVACY

Data Privacy Law Comparison

Components	GDPR (EU Law)	CCPA	CPRA	Components	GDPR (EU Law)	CCPA	CPRA
Right to Know What Information a Business has Collected About You				Storage Limitation: Right to Prevent Companies from Storing Info Longer than Necessary			
Right to Say No to Sale of Your Info				Data Minimization: Right to Prevent Companies from Collecting More Info than Necessary			
Right to Delete Your Information				Right to Opt Out of Advertisers Using Precise Geolocation (< than 1/3 mile)			
Data Security: Businesses Required to Keep Your Info Safe				Ability to Override Privacy in Emergencies (Threat of Injury/ Death to a Consumer)			
Data Portability: Right to Access Your Information in Portable Format				Provides Transparency around "Profiling" and "Automated Decision Making"			
Special Protection for Minors				Establishes Dedicated Data Protection Agency to Protect Consumers			
Requires Easy "Do Not Sell My Info" Button for Consumers				Restrictions on Onward Transfer to Protect Personal Information			
Provides Ability to Browse with No Pop-ups or Sale of Your Information				Requires High Risk Data Processors to Perform Regular Cybersecurity Audits			
Penalties if Email Plus Password Stolen due to Negligence				Requires High Risk Data Processors to Perform Regular Risk Assessments			
Right to Restrict Use of Your Sensitive Personal Information				Appoints Chief Auditor with Power to Audit Businesses' Data Practices			
Right to Correct Your Data				Protects California Privacy Law from being Weakened in Legislature	N/A		

What other states will follow?

STATE COMPREHENSIV E PRIVACY LAW COMPARISON



Key Challenges for Creating and Maintaining Your Data Inventory



5 Primary Challenges

The “Time Suck”



Accounting for ALL Data Sources



Updating the Data Inventory



Data Fields Required by New Regulations



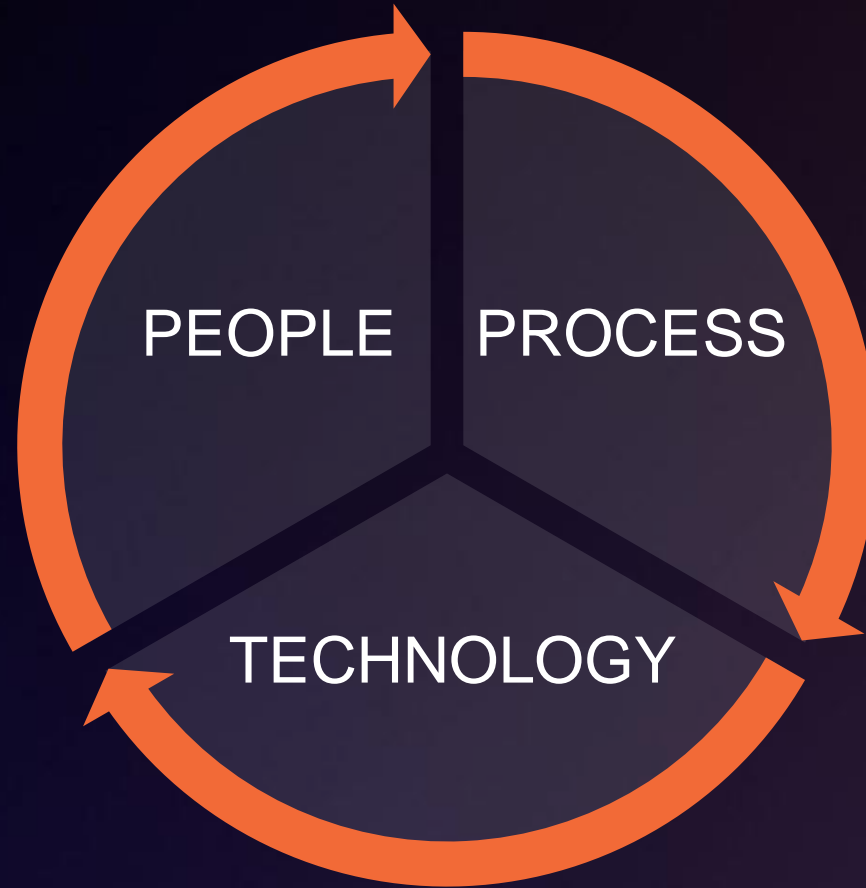
Identifying the Right
Stakeholders/Departments



How to Develop a Data Inventory at Your Organization



3 Key Components



The Foundation for Defensible Compliance



DATA SUBJECTS	 Customers Current Employees Past Employees Job Candidates Minors/Children Beneficiaries Contractors
APPLICABILITY	           
DATA ELEMENTS	Social Security Number Drivers' License Number Account Number Credit Card # Biometric Religion Political Affiliations Aptitudes Preferences Attitudes
COLLECTION	 Web Form  Email  Paper Form  Phone
DEPARTMENTS	 HR - Benefits Finance - Payroll HR – Recruiting Legal & Compliance Marketing
APPLICATIONS	    
LOCATIONS	     Laptops  File Cabinets
THIRD PARTIES	    
RETENTION	Payroll Records Personnel Records Recruiting Records  AUT 7 Years  BEL 5 Years  NLD 5 Years  ITA 5 Years  USA 7 Years

Data Map | Personal Data Processing Activities

PROCESSING ACTIVITY: HR ONBOARDING
COUNTRY: UNITED STATES

Purpose of Processing
Associated Data Elements
Data Subjects
Types of Notice Provided
Consent Received from Subject

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

Informs Compliance Roadmap



- ✓ DSAR Processes
- ✓ Vendor Risk Profiling
- ✓ Data Retention/Minimization
- ✓ Notices & Disclosures
- ✓ Privacy Policy
- ✓ Employee Privacy Policy
- ✓ Incident Response
- ✓ Vendor Agreements



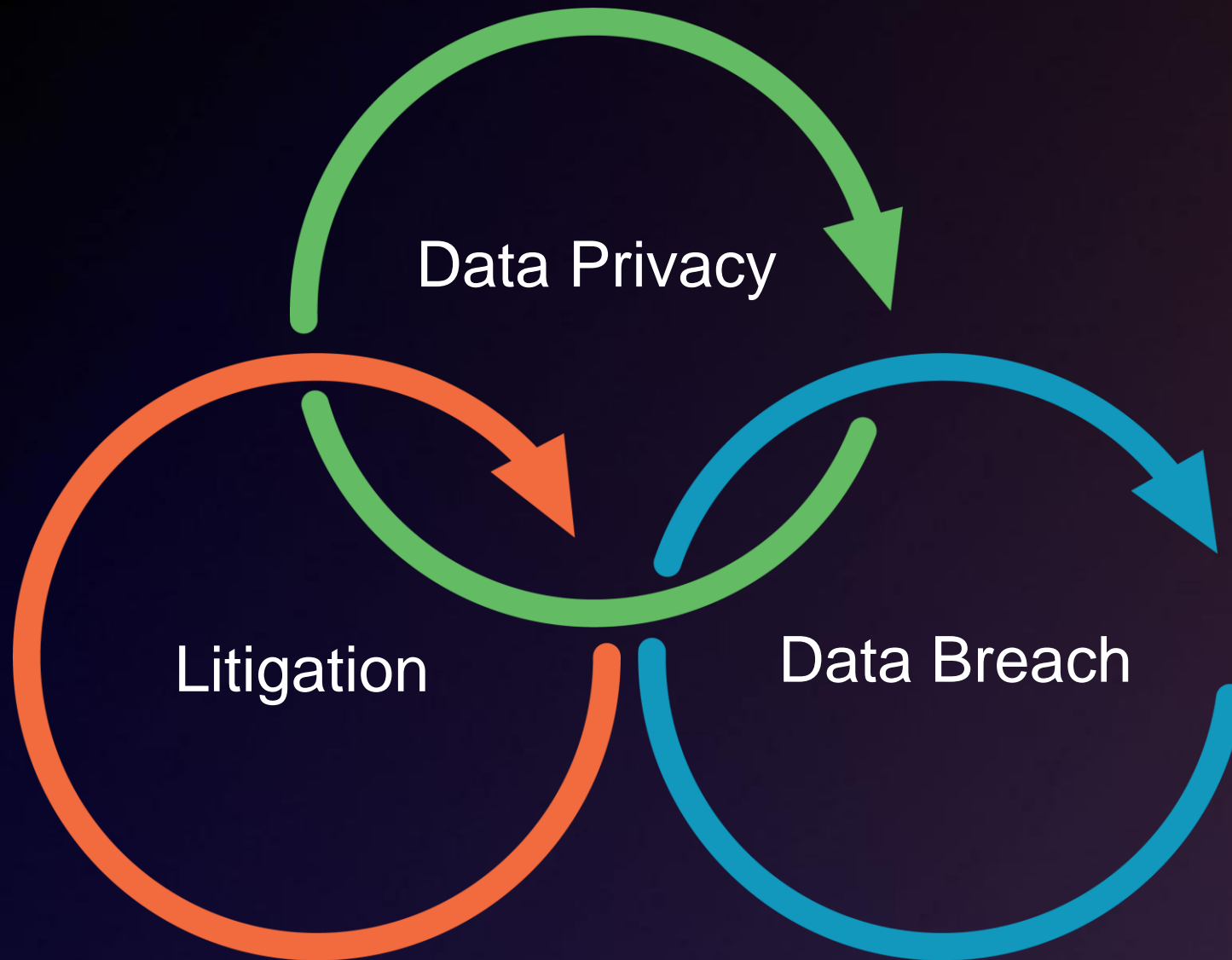
Process – 10 Key Questions to Ask About Your Data Inventory

1. Is it easy to filter and identify data based on any parameter, including regulatory statutes?
2. Where is the data coming from (what is the source for information)?
3. Is it easy to update, maintain, and ensure that the data is accurate?
4. Is the data able to be identified by record type, regulatory standard, and other variables?
5. Does it contain all your organization's data?
6. Can it include third parties that collect and store data on your behalf?
7. Can you identify the data subjects by how they interact with your business?
8. Can you identify where in your business process that data is stored?
9. Can you identify the business purpose for collecting an individual's personal information?
10. Can you identify the collection methods of that personal information?



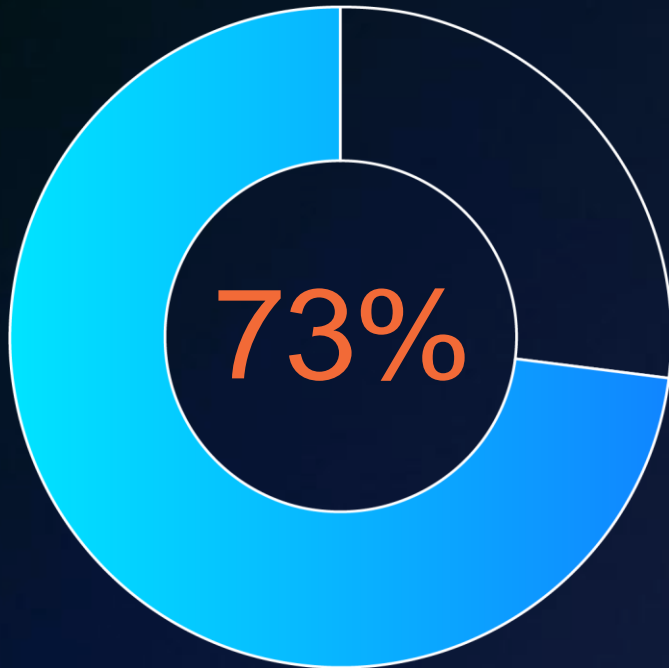
Why Minimize Your Data?

Why Minimize Your Data?



Litigation

DOCUMENT REVIEW
IS THE BIGGEST



COST DURING E-
DISCOVERY



LESS DATA,
LESS TO REVIEW

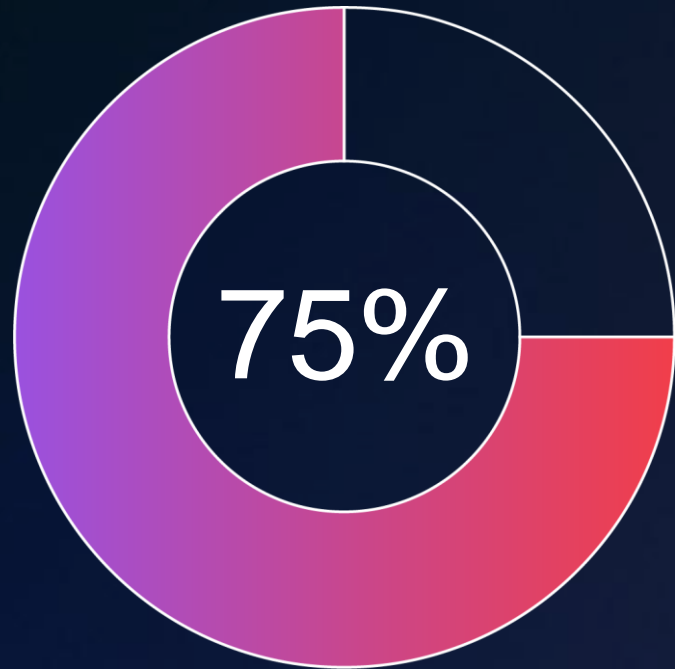


EMAIL IS THE KEY



Data Privacy

Most companies vastly
over-retain records and an
average of



of that contains **Personal Data**



Minimize
Collection



Dispose when
bargain for
collection has
been fulfilled



Financial Consequences of a Data Breach



DATA BREACH

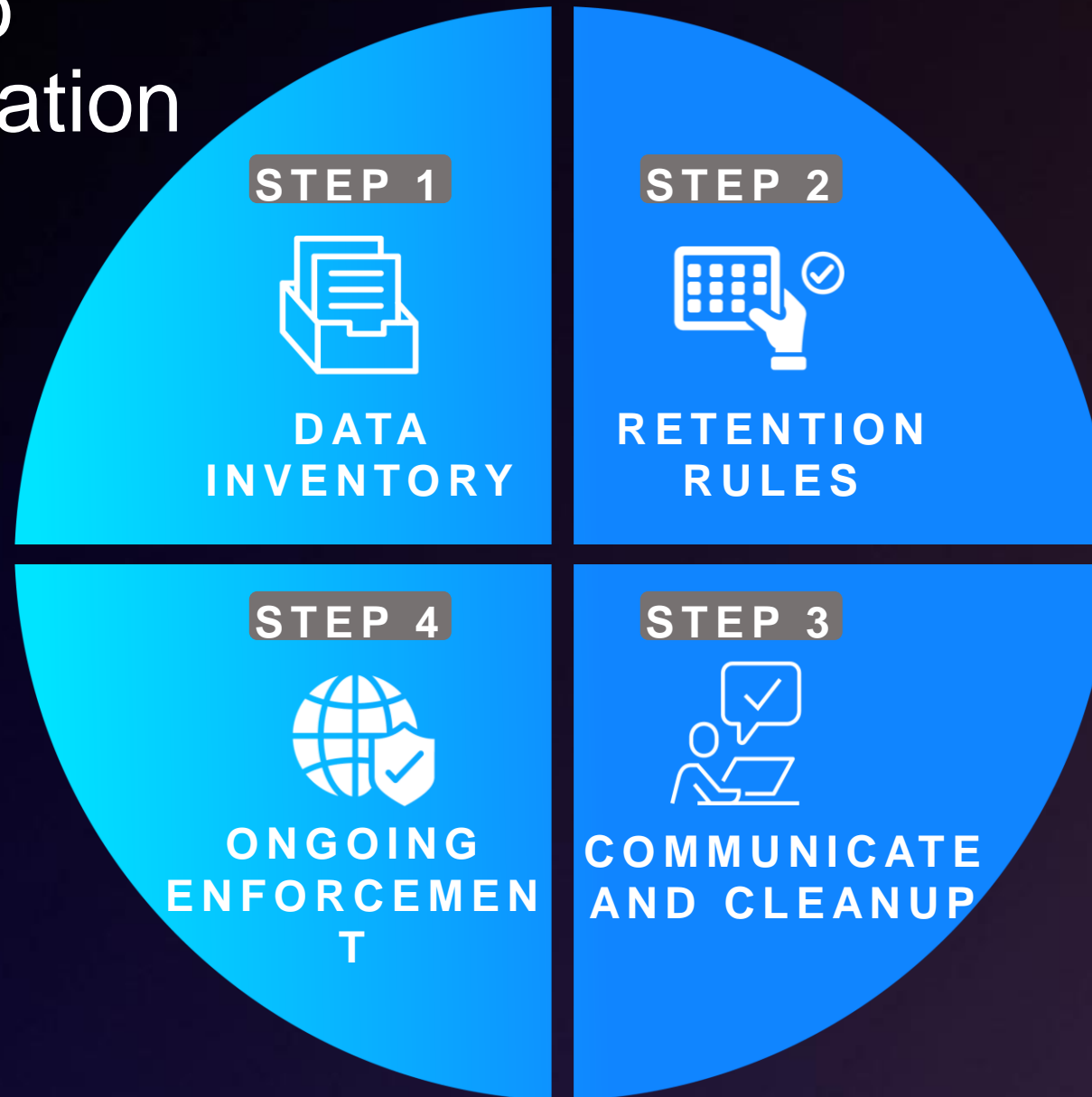


PER DATA SUBJECT






- **10,000 CA RESIDENTS: \$1 to \$7.5 million**
- **100,000 CA RESIDENTS: \$10 to \$75 million**
- **1,000,000 CA RESIDENTS: \$100 to \$750 million**
- **10,000,000 CA RESIDENTS: \$1 to \$7.5 billion**



Four Steps to Data Minimization



Global Retention Considerations

Retention Standards By Record Type																	
Benefit Enrollment & Participation Records	Reported Retention -(9), 0(7), 1(1), 2(3), 5(1), PERM(9)																
		AUT 7 BEL 10 BGR 50 CHE 10 CZE 10 DEU 6 DNK 10 ESP 15 EST - FIN 10 FRA 5 GBR 6 HUN 5 IRL 6															
Employee Medical Records	Reported Retention -(8), 0(4), 1(2), 4(1), 5(5), 7(3), 10(3), PERM(16)																
		USA 6 ISL 7 ITA 10 LIE 30 LTU - LUX 30 LVA - NLD 5 NOR 10 POL 10 PRT 20 ROU 10 SVK 3 SW 10 UKR 6															
Employment Equality Compliance Records	Reported Retention -(1), 0(1), 2(1), PERM(2)																
		AUT 25 BEL 10 BGR 5 CHE 10 CZE 3 DEU 10 DNK 10 ESP 15 EST 3 FIN 10 FRA 5 GBR 6 HUN 5 IRL 6															
																	
		USA 10 ISL 4 ITA 10 LIE 30 LTU 10 LUX 30 LVA 10 NLD 5 NOR 10 POL 10 PRT 20 ROU 10 SVK 3 SW 3 UKR 3															

Page 4 of 25

A Clear Path to Data Minimization

DEVELOP

- ✓ Retention Schedules
- ✓ Scheduling Logic
- ✓ Policies
- ✓ Deletion Strategies
- ✓ Hold Process

IMPLEMENT

- ✓ Program Training
- ✓ Attestation
- ✓ Email
- ✓ File Share
- ✓ Structured Data
- ✓ Paper Records

MAINTAIN

- ✓ Audit Trail
- ✓ Documentation
- ✓ Policies
- ✓ Program Monitoring
- ✓ Program Updates
- ✓ Annual Review



Executive Summary: Your Guide to Defensible Data Practices

1. Know Your Data: Adequate Risk Assessment Begins with Visibility
2. Practice What You Preach: Maintaining and Updating Data-Related Policies & Procedures Drives Performance
3. Perfect Practice Makes Perfect Play: Employee Training Drives Muscle Memory (+ It's the Law)
4. Show Your Work: Compliance Efforts that are Repeatable, Sustainable and Demonstrable are also Defensible
5. Future Proof Your Compliance Approach

Thank you!



Robert Fowler,
robert.fowler@exterro.com



Michael Kallens,
michael.kallens@nasdaq.com



Audrey Jean,
ajeane@aarp.org