



SUSTAINABLE COMPLIANCE WITH DATA PRIVACY & CYBERSECURITY REGULATIONS

Meeting Your Obligations, Protecting Your Company

Presented by:

Jordan Lawrence®
an **exterro** company

SPEAKERS



Robert Fowler, CIPP-US
Director of Strategic Partnerships

Jordan Lawrence®



Audrey Jean
VP, Privacy Officer & Associate General Counsel



Troy Cahill
General Counsel and Corporate Secretary





In The Beginning...

(GDPR)
General Data Protection Regulation



Purpose & Intent:

1. Protect Personal Data
2. Use Personal Data Appropriately

Assumption...

Companies know everything about their data.



Fines up to 4%
Annual Global Revenue

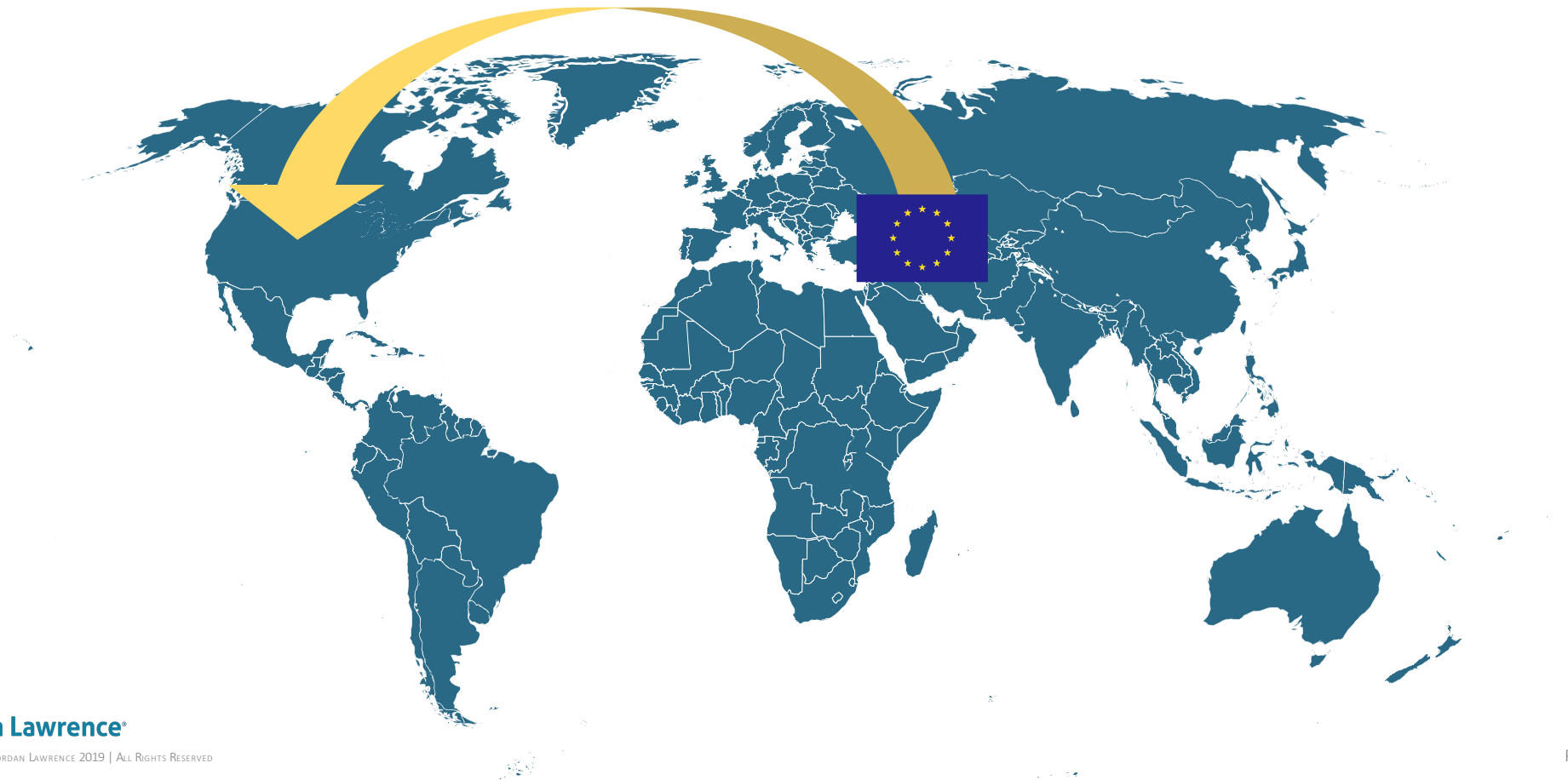
- What Personal Data is Collected
- Business Purpose for Collection
- Right to Access Data
- Right to Opt-Out
- Right to Request Deletion
- Right to Data Portability
- Right to Compensation

Bureaucratic Enforcement



- Enforced by Data Protection Authorities
- Heavy Compliance Documentation
- Regulatory Investigations
- Breach Notification Required
- Cease Processing Order

Privacy Regulations Come To The U.S.



Private Right of Action *\$750 IN DAMAGES* /Resident /Incident

Find out what information businesses are collecting about you

1

Gives You Ownership

Protect your right to tell a business not to share or sell your personal information.

[Learn More](#)

2

Gives You Control

Gain control over the personal information that is collected about you.

[Learn More](#)

3

Gives You Security

Hold businesses responsible for safeguarding your personal information.

[Learn More](#)

Potential Wave of Litigation

BREACHES SUDDENLY HAVE GREAT POTENTIAL FOR PLAINTIFFS' ATTORNEYS:

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

Expanding Data Privacy & Cybersecurity Regulations



The background of the slide is a dramatic, black and white photograph of dark, heavy storm clouds. The clouds are textured and layered, with some light breaking through near the bottom, creating a sense of depth and intensity. The overall mood is ominous and powerful, fitting the 'perfect storm' theme.

The perfect storm.

Lack of Data Governance Practices

Broader Definition of Personal Data

Increased Liability

Energetic Litigation Bar

“Class action lawyers are pursuing data privacy cases and amassing fortunes even where no one has been harmed.”

Engineered Liability

The Plaintiffs' Bar's Campaign to Expand Data Privacy and Security Litigation



Executive Summary



When the prospect of large monetary settlements is on the table, no business sector is secure from plaintiffs' attorneys. In this pattern, there is a growing campaign by the plaintiffs' bar to target data privacy and security in the hopes of striking it rich in a new goldmine on the level of the asbestos litigation of the 1970s, 80s, and 90s.

Bet-The-Job Questions...

- 1 Do we really know where all personal and sensitive data exists?
- 2 Can we respond compliantly and cost-effectively to data access requests?
- 3 Which of our vendors have our personal data?
- 4 Do we retain any personal data longer than necessary?

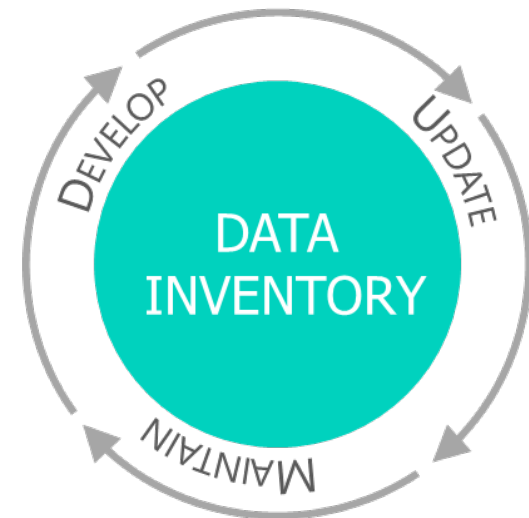
1

**Do we really know
where all personal
data exists?**

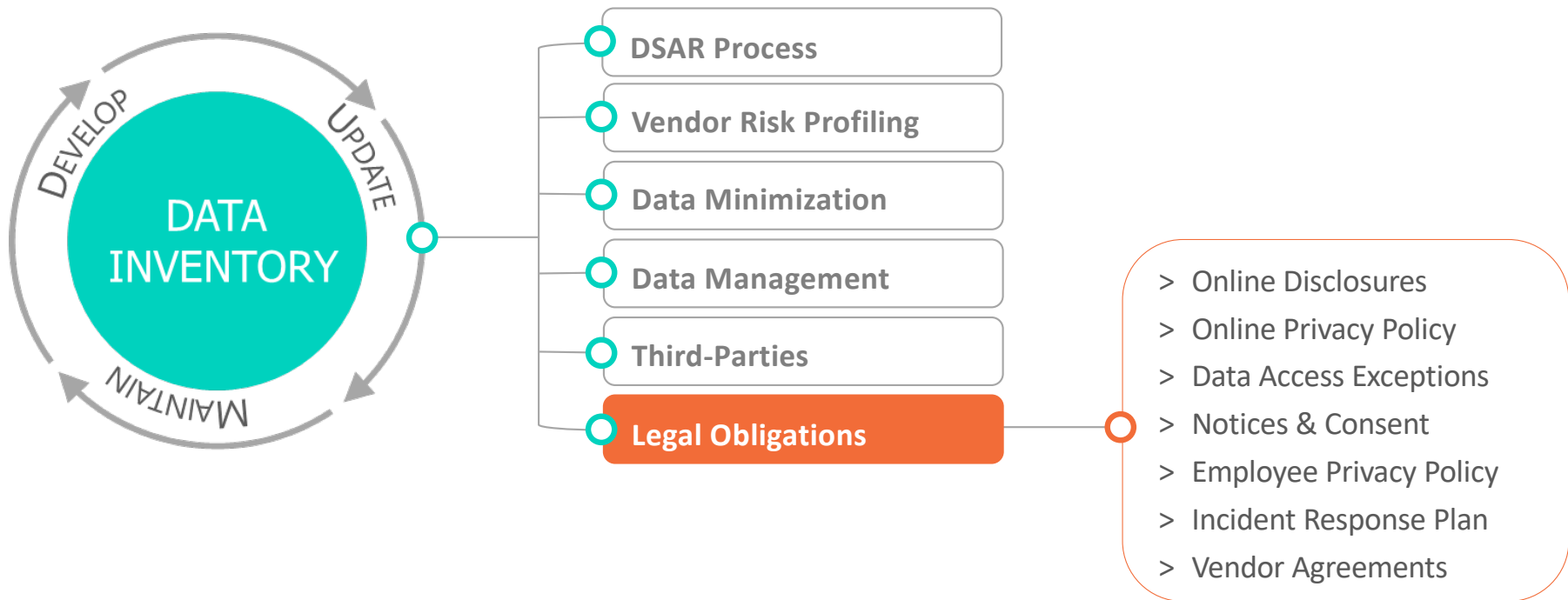
Compliance begins with
a data inventory.

DATA SUBJECTS	 Beneficiaries Current Employees Customers Job Candidates Minors/Children Past Employees Subscribers
APPLICABILITY	
PERSONAL DATA	Social Security # Drivers' License # Account # Credit Card # Legal Actions Corporate Financial Data Intellectual Property Profile Data Preferences Attitudes
COLLECTION	 Web Form  Email  Paper Form  In Person
APPLICATIONS	    
DEPARTMENTS	 Customer Service Finance-Payroll HR-Benefits HR-Recruiting Investor Relations Legal & Compliance Marketing
LOCATIONS	     Laptops  File Cabinets
THIRD PARTIES	    
RETENTION	Payroll Records Personnel Records Recruiting Records  <div> <div>AUT 7 Years</div> <div>BEL 5 Years</div> <div>NLD 5 Years</div> <div>ITA 5 Years</div> <div>CHE 5 Years</div> <div>USA 7 Years</div> </div>

Data Inventory Must Be Sustainable



Informs Critical Compliance Requirements



GDPR Article 30 | RECORD OF PROCESSING ACTIVITIES



PROCESSING ACTIVITY: HR ONBOARDING

COUNTRY: UNITED KINGDOM

GDPR Reference/Description		Required Information			
30 – 1(A)	Controller Contact Details	Joanna Drummond +44 (0) 20 7350 6144 jdrummond@globalmfgco.com			
30 – 1(A)	Data Protection Officer Contact Details	Aaron Johnson +1 636 527 3001 ajohnson@globalmfgco.com			
30 – 1(B)	Purpose of Processing	Compliance with a legal obligation, Necessary for legitimate interests, Performance of a contract, Protection of vital interests of data subject			
30 – 1(C)	Data Processed	Biometric	NONE		
		Genetic	NONE		
		Protected Health	Occupational Health Report	Dates of Service	Diagnosis
		Sensitive Personal Personal Information	Criminal Records	Ethnic Origin/Race	Health Status
			Age	Education	Occupation
			Nat'l Insurance #	Birth Certificate	Birth Date
			Gender	Email Address	Physical Address
			Passport #	Marital Status	Phone Number
30 – 1(C)	Data Subjects	Current Employees, Dependents/Beneficiaries, Job Candidates, Past Employees, Minors/Children			
30 – 1(C)	Types of Notice Provided	Don't Know			
30 – 1(C)	EEA Resident	Yes			
30 – 1(C)	Consent Received from Subject	Don't Know			

Third-Party | EBI BACKGROUND CHECK



OVERVIEW

Departments:	Corp - HRIS, HR - Hiring (Germany), HR - Onboarding, HR - Investigations, Finance - Payroll
Participant Countries:	Argentina, Austria, Belgium, Brazil, France, Germany, Mexico, United Kingdom, United States
Origin Countries:	Argentina, Austria, Belgium, Brazil, France, Germany, Mexico, United Kingdom, United States
Destination Countries:	Germany (5), United States (21)
Processing Activities:	HR - Investigations, HR - Payroll, HR - Onboarding

DATA CATEGORIES

Personal Data:	Birth Date	Citizenship Status	Driver's License #	Email Address	First/Last Name
	Gender	National ID Card #	Passport #	Social Security #	
Demographic Data:	Age	Education	Occupation		
Employment Data:	Background Checks	Employment Status	Veteran Status		
Personal Financial Data:	None				

Data Map | Personal Data Processing Activities



PROCESSING ACTIVITY: HR ONBOARDING

COUNTRY: UNITED STATES

Purpose of Processing		Compliance with a legal obligation, Necessary for legitimate interests, Performance of a contract, Protection of vital interests of data subject			
Associated Data Elements	Biometric	NONE			
	Genetic	NONE			
	Protected Health	Occupational Health Report	Dates of Service	Diagnosis	Disease/Disorder
	Sensitive Personal	Criminal Records	Ethnic Origin/Race	Health Status	
	Personal Information	Age	Education	Occupation	Postal/Country Code
		Nat'l Insurance #	Birth Certificate	Birth Date	Citizenship Status
		Gender	Email Address	Physical Address	First/Last Name
		Passport #	Marital Status	Phone Number	
Data Subjects		Current Employees, Dependents/Beneficiaries, Job Candidates, Past Employees, Minors/Children			
Types of Notice Provided		Don't Know			
Consent Received from Subject		Yes			

2

**Can we respond
compliantly to data
subject access
requests?**

45 days to respond
to a verifiable request.

The Challenge Ahead

DATA ACCESS REQUESTS

- ✓ Right to Access
- ✓ Right to Delete
- ✓ Right to Opt-Out
- ✓ Right to Portability
- ✓ Right to Disclosure

**45
Days**

WHERE'S THE DATA?

- ☐ Verify Identity
- ☐ Data Locations & Sources
- ☐ Applications
- ☐ Third Parties
- ☐ Retention & Legal Holds

The outlook is grim...

- 45% to 85% of companies aren't ready
- 83% need 7 days to respond to one request
- \$1,400 to fulfill a single request
- **5K requests = \$7 Million**

Data Subject Access Request Workflow

Methods to Easily Submit Requests



- Keep Informed
- Request Status

Authenticate Data Subject Identity



- Loyalty Program
- Frequent Flyer
- Recent Order #

Notify Appropriate Personnel



- Configure Workflows
- Ensure Consistency
- Manage Timelines

Search & Collect Personal Information



- Applications
- Third Parties
- Unstructured Data
- Paper Records

Review & Redact Sensitive Information



- Protect Information
- Avoid a Breach

Secure Delivery of Information



- Secure Portal
- Deletion Timeframe

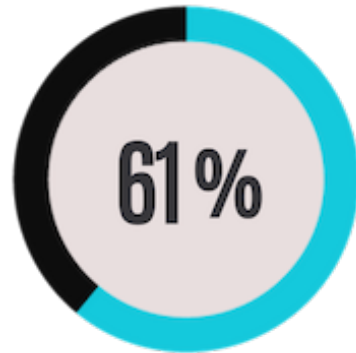
45 Days

3

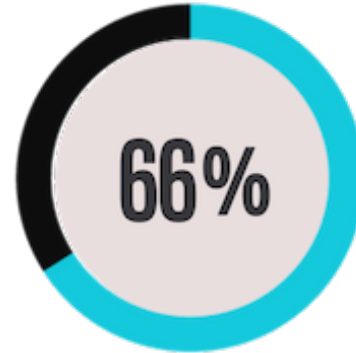
**Which of our
vendors have our
personal data?**

Compliance extends to
your third parties.

Companies lack visibility into the third parties they share personal data with.



experienced a breach
caused by a third party.



don't have an inventory
of their third parties.



VENDOR RISK PROFILE

Identify Regulatory Applicability & Risks



VENDOR RISK PROFILE

Identify Regulatory Applicability & Risks



Vendors Accessing Personal Data



Vendors Accessing Systems



Vendors With No Access



Vendors Accessing Personal Data



Vendors Accessing Systems



COMPREHENSIVE
REPEAT
RISK ASSESSMENT >>

CSF
00 171
IT
000



Requisite
Reporting

Identify Data Security Risks
Demonstrate Compliance

Assess Security & Compliance Readiness



Vendor Data Protection & Security Diligence Review

Vendor Name | Rack Technologies

Heat Triggered By Vendor Responses

CONTACT	Bill Kennedy bkennedy@abc.com	INTERNAL CONTACT	Joe Sartors jsartors@abc.com
CATEGORIES	Tier 2, Cloud	ASSESSMENT	Tier 2
ASSESSMENT COMPLETED	04/30/2018	NEXT ASSESSMENT	04/01/2019
SERVICES PROVIDED	Software development and hosting services		
		ANNUAL SPEND	\$700,000

TOTAL SCORE

HEAT MAP SCORING

160

66

36

ACCEPTED

MODERATE

HIGH

Access and Control Levels

DATA PROTECTION OFFICER Bill Kennedy
bkennedy@abc.com

ACCESS LEVELS

- ☒ Direct access to our personal data
- ☐ Direct access with our corporate network
- ☒ Indirect access within our corporate network
- ☐ Physical access within our corporate facilities

SECURITY CONTROLS

- ☒ Data Encryption
- ☐ Routine Deletion
- ☒ Incident detection and response
- ☐ Regular Risk Assessments

Data Processed, Accessed or Stored

PERSONAL DATA

PERSONAL

Birth Date First/Last Name Gender

Marital Status Phone Number SSN

PERSONAL FINANCIAL

Tax Info.

EMPLOYMENT

Employee ID

SPECIAL CATEGORIES DATA - GDPR ARTICLE 9

SENSITIVE PERSONAL

Blood Type Ethnic Origin/Race

PROTECTED HEALTH

Dates of Service

4

**Are we retaining
any personal data
longer than
necessary?**

Harmonize retention
and legal holds.

A Clear Path to Data Minimization

DEVELOP

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

IMPLEMENT

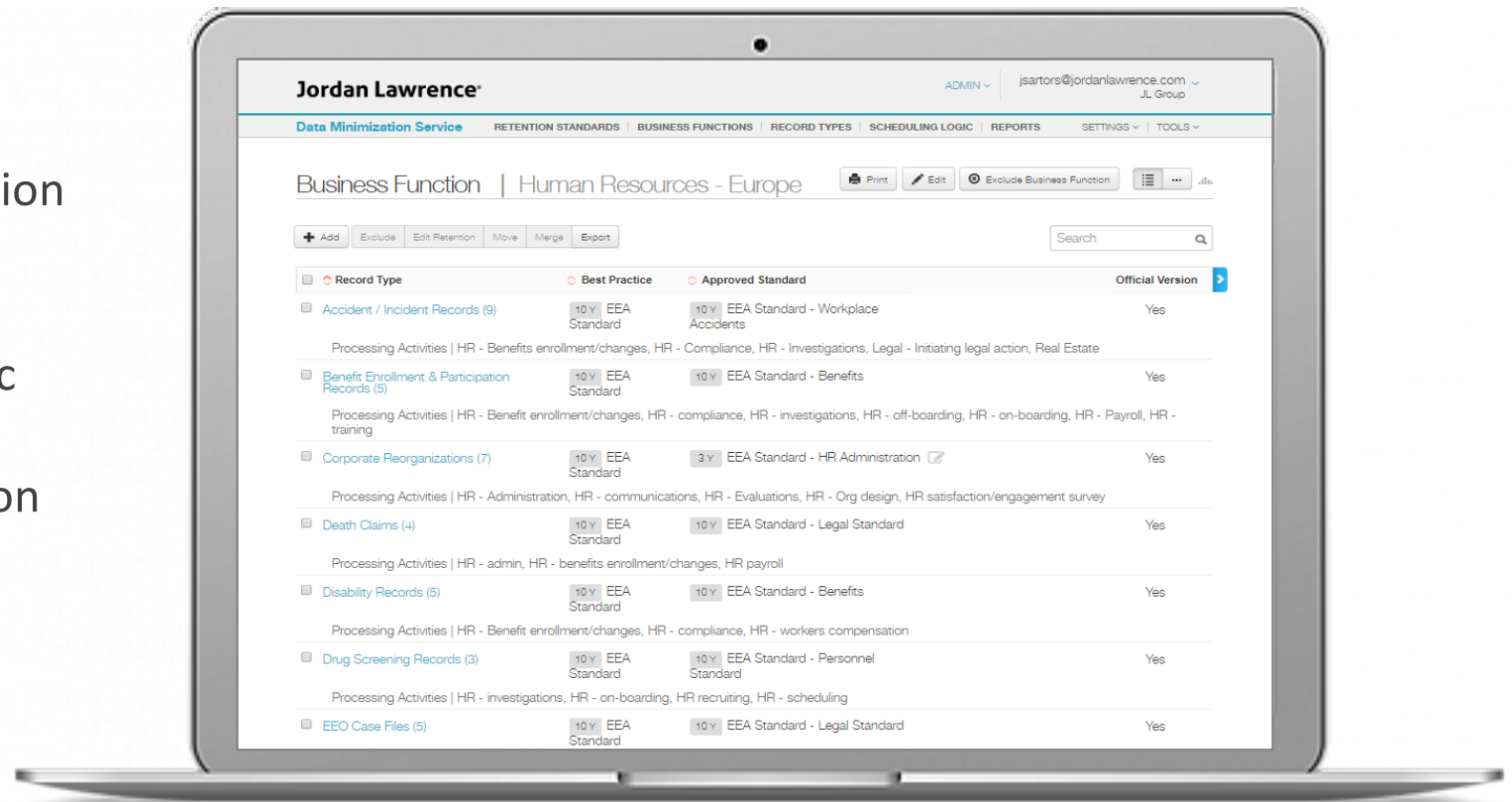
- ✓ Program Training
- ✓ Attestation
- ✓ Email
- ✓ File Share
- ✓ Structured Data
- ✓ Paper Records

MAINTAIN

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

Connect Personal Data to Retention Requirements

- Manage Retention Requirements
- Document Logic
- Develop Deletion Strategies



QUESTIONS



Robert Fowler, CIPP-US
Director of Strategic Partnerships

Jordan Lawrence®



Audrey Jean
VP, Privacy Officer & Associate General Counsel



Troy Cahill
General Counsel and Corporate Secretary

