ACC Association of Corporate Counsel
GREATER PHILADELPHIA

DATA PRIVACY & CYBERSECURITY

The Tipping Point?

Jordan Lawrence®
an exterro company

Presenters:

Robert Fowler, CIPP-US
Director of Strategic Partnerships

Jordan Lawrence®
an exterro company

Phil Yannella, Partner
Practice Leader: Privacy and Data Security Group and
E-Discovery and Data Management Group

Ballard Spahr LLP

ACC Association of Corporate Counsel
GREATER PHILADELPHIA


WELCOME TO
DATA SECURITY &
PRIVACY COMPLIANCE

In The Beginning…

(GDPR)
General Data Protection Regulation

Purpose & Intent:

1. Protect Personal Data
2. Use Personal Data Appropriately

Assumption…

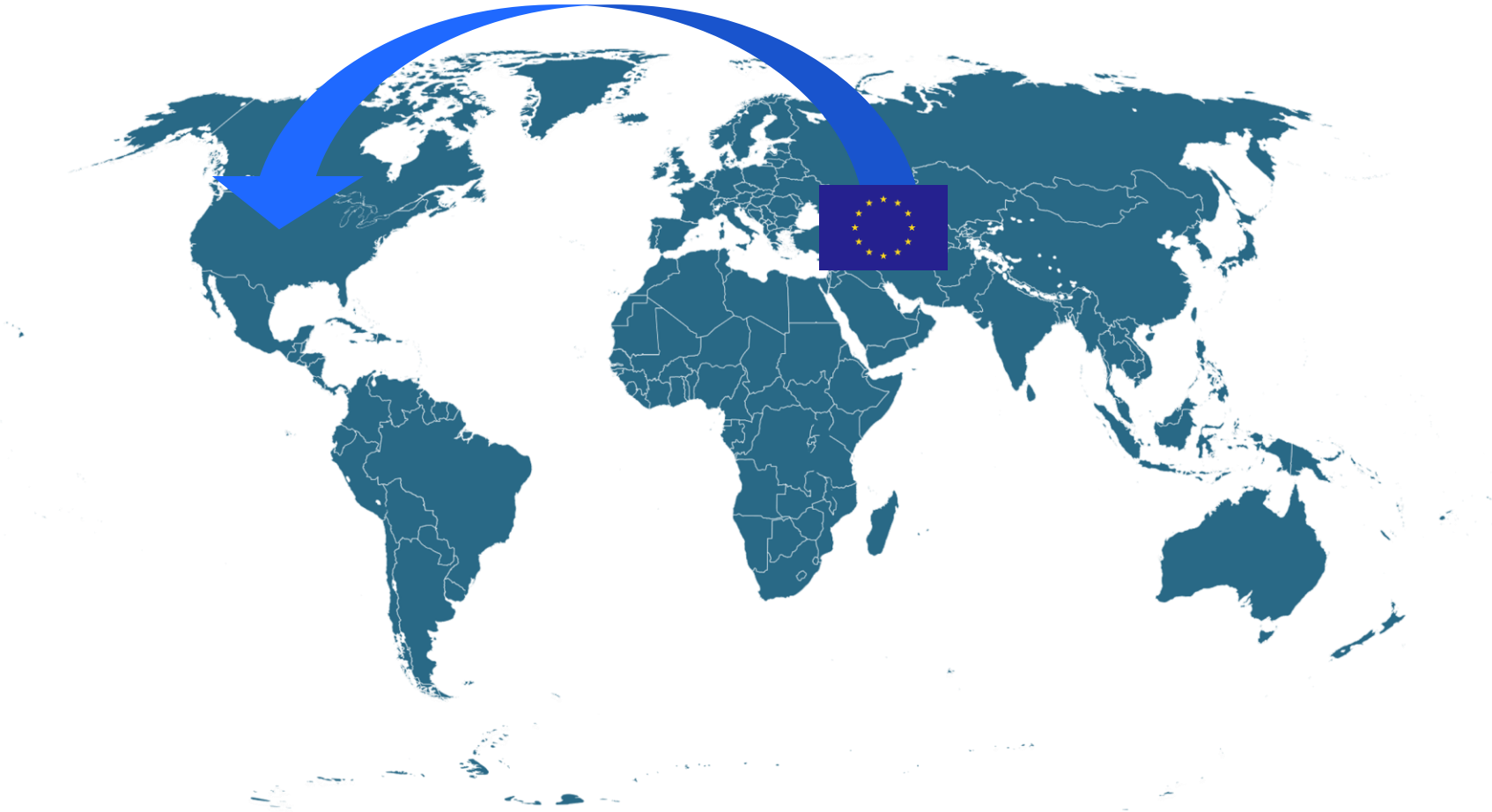
Companies know everything about their data.

- 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

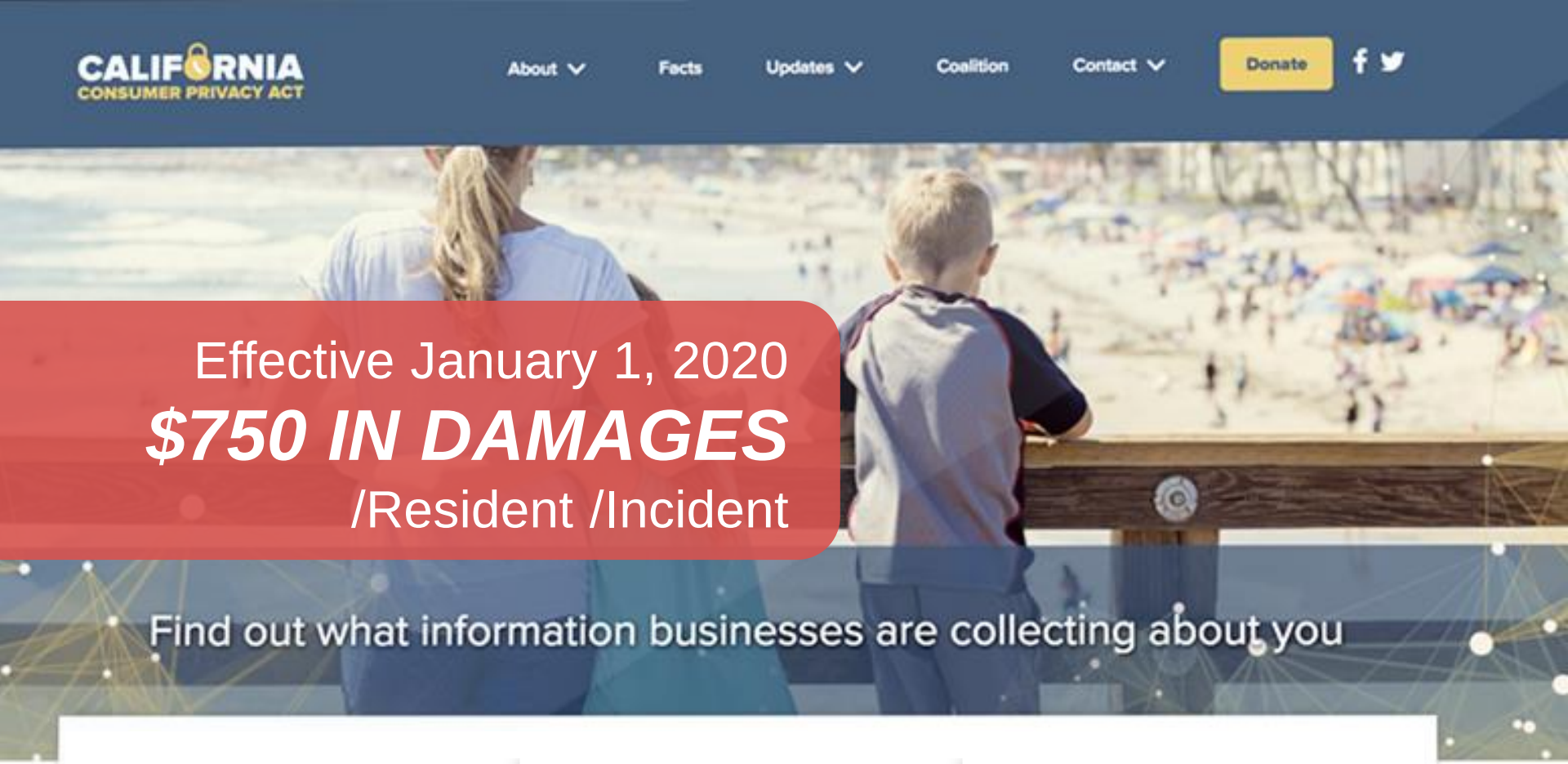
Bureaucratic Enforcement

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

Privacy Regulations Come To The U.S.



Jordan Lawrence
an exterro company



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

Jordan Lawrence
an exterro company

The perfect storm.

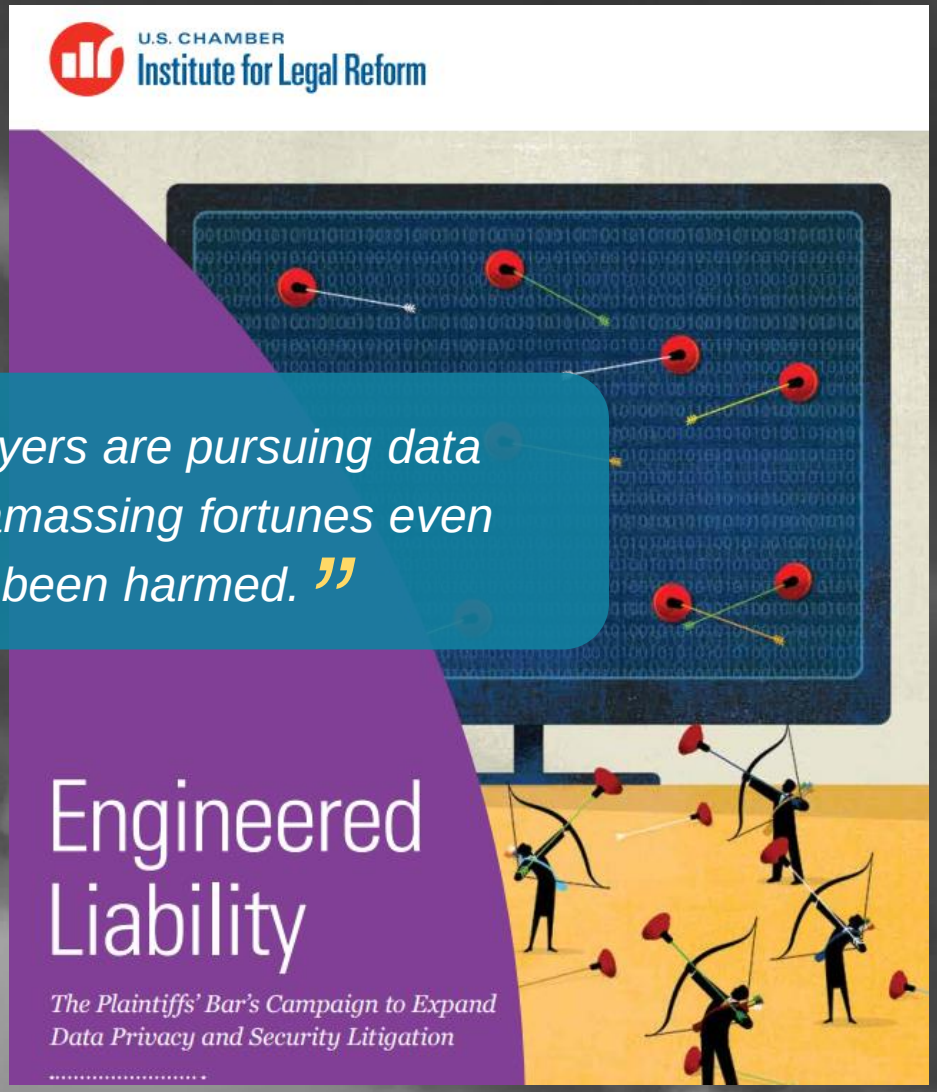
Lack of Data Governance Practices

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.”



Executive Summary

U.S. CHAMBER
Institute for Legal Reform

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?

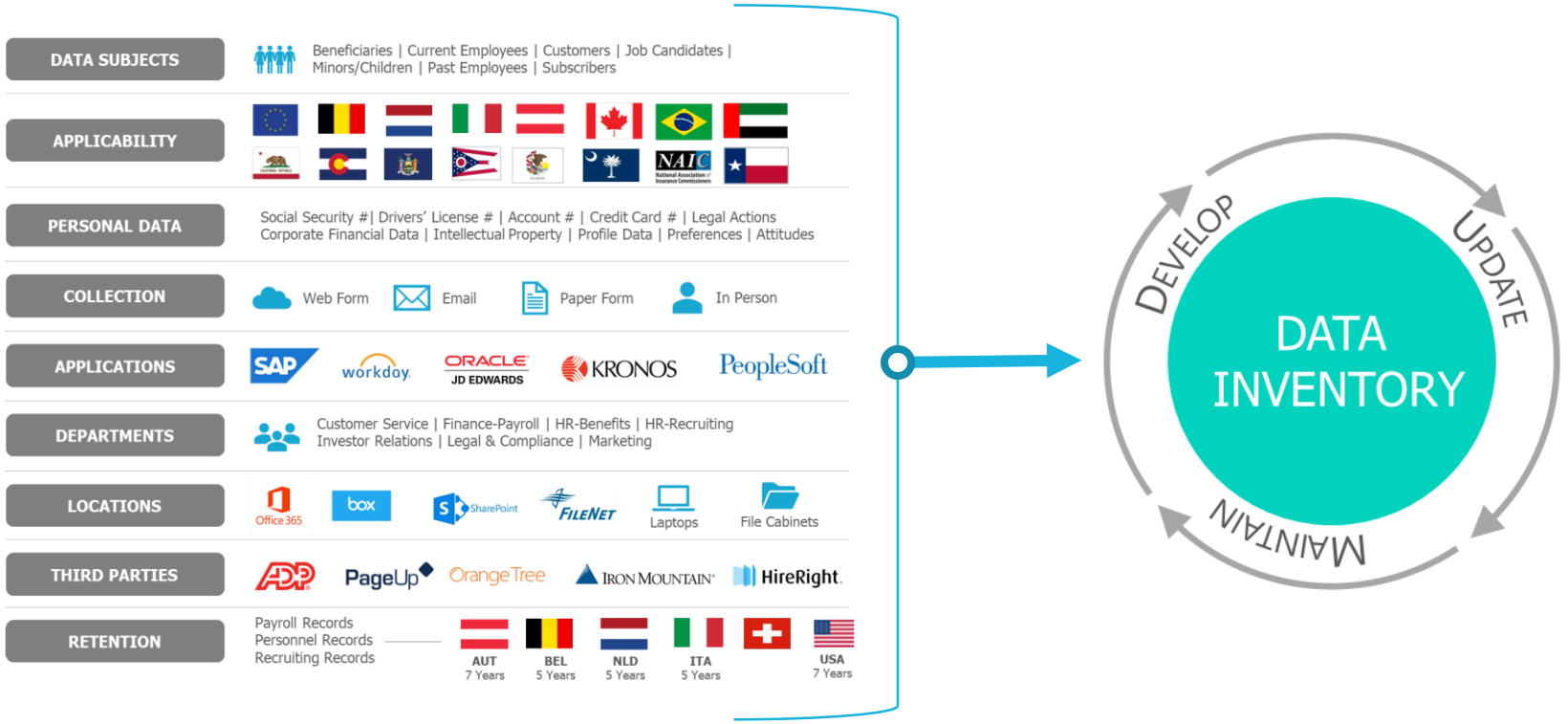
Compliance begins with a data inventory.

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	SAP · workday. · ORACLE JD EDWARDS · KRONOS · PeopleSoft
DEPARTMENTS	Customer Service | Finance-Payroll | HR-Benefits | HR-Recruiting Investor Relations | Legal & Compliance | Marketing
LOCATIONS	Office 365 · box · SharePoint · FileNet · Laptops · File Cabinets
THIRD PARTIES	ADP · PageUp · OrangeTree · Iron Mountain · HireRight
RETENTION	Payroll Records Personnel Records Recruiting Records

AUT	BEL	NLD	ITA	CHE	USA
7 Years	5 Years	5 Years	5 Years	5 Years	7 Years

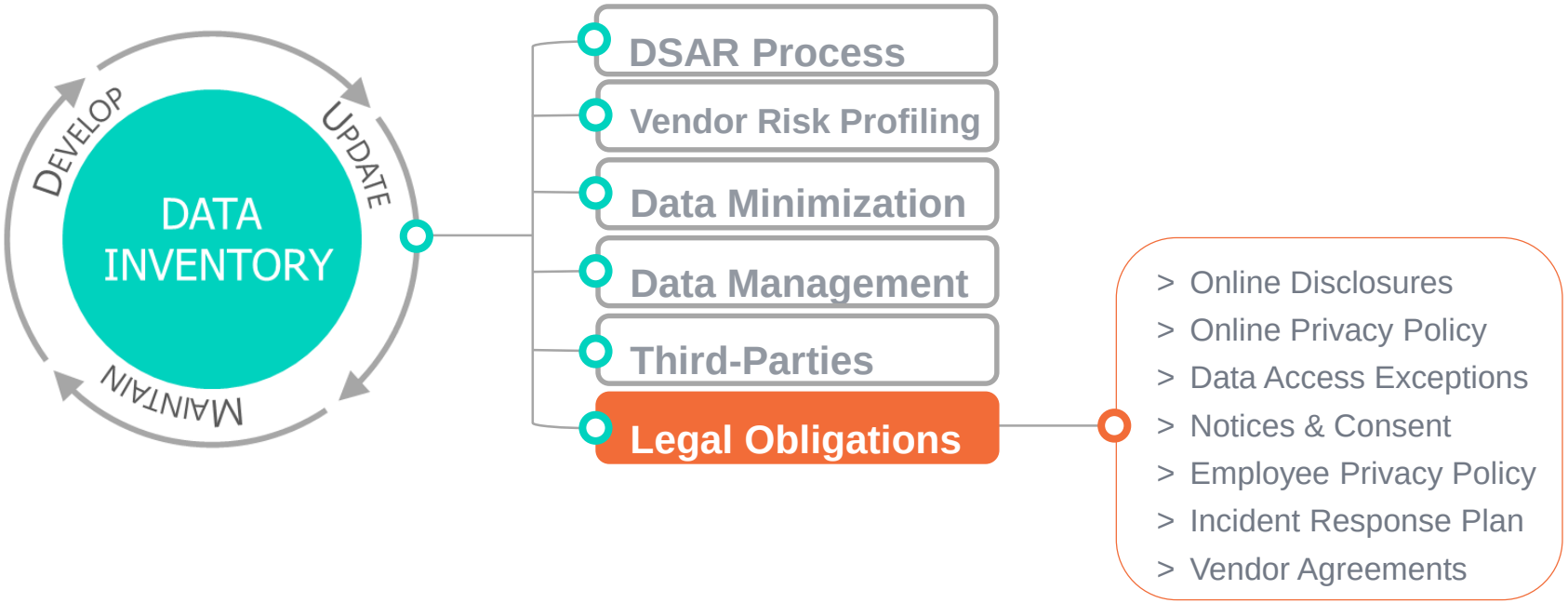
Jordan Lawrence
an exterro company

Data Inventory Must Be Sustainable



Jordan Lawrence
an exterro company

Informs Critical Compliance Requirements



Ethical Considerations

- ABA Model Rule 1.1 (Competence)
  - To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, ***including the benefits and risks associated with relevant technology***, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

- Understanding technology is critical to understanding legal implications of data mapping
  - Cookie Compliance
  - Anonymization
  - Data Breach Response

GDPR Article 30| Record of Processing Activities

ABC COMPANY

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	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	
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

ABC COMPANY

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

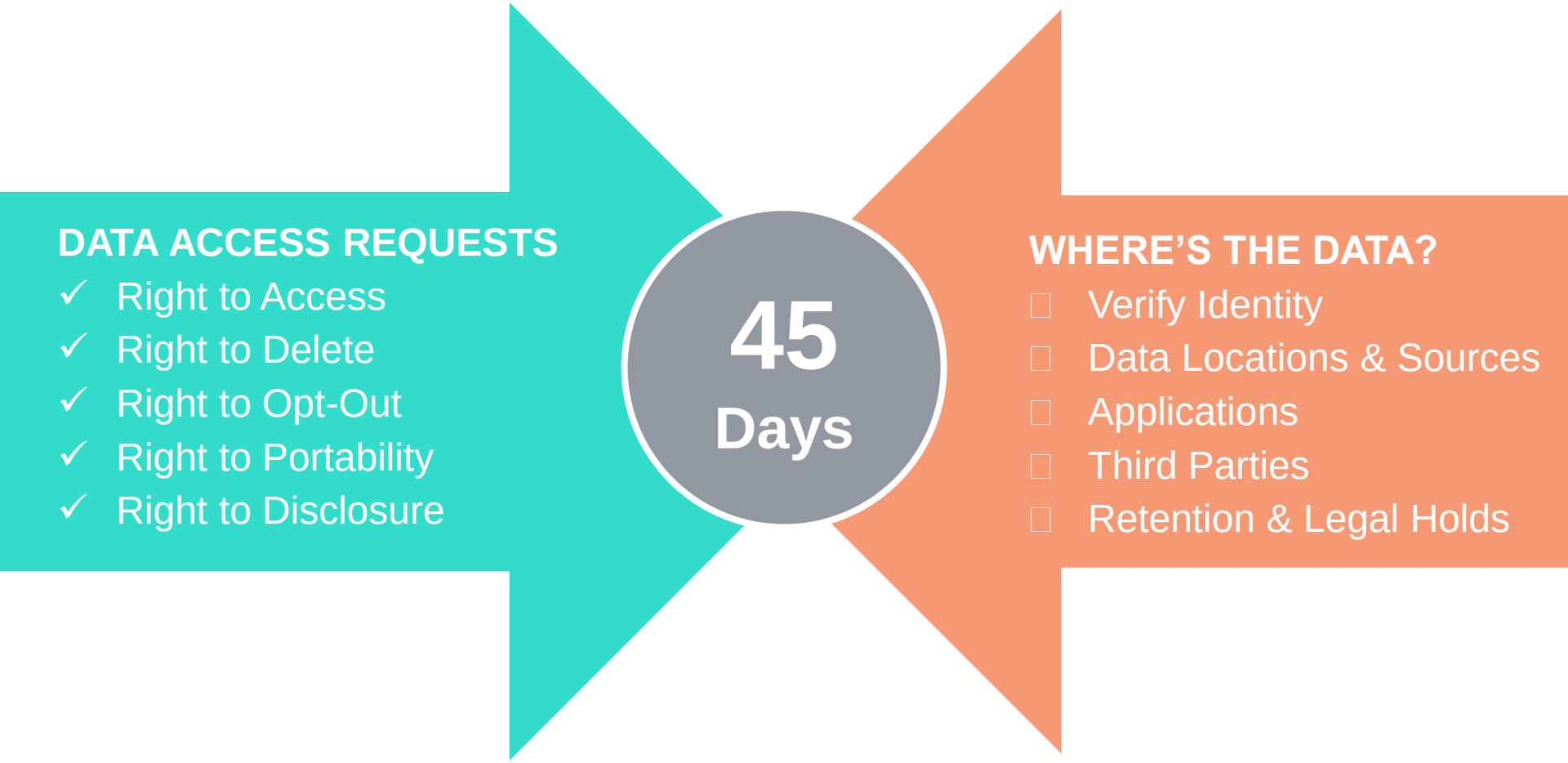
Purpose of Processing		Compliance with a legal obligation, Necessary for legitimate interests, Performance of a contract, Protection of vital interests of data subject			
Associated Data Elements	Biometric	NONE			
	Genetic	NONE			
	Protected Health	Occupational Health Report	Dates of Service	Diagnosis	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

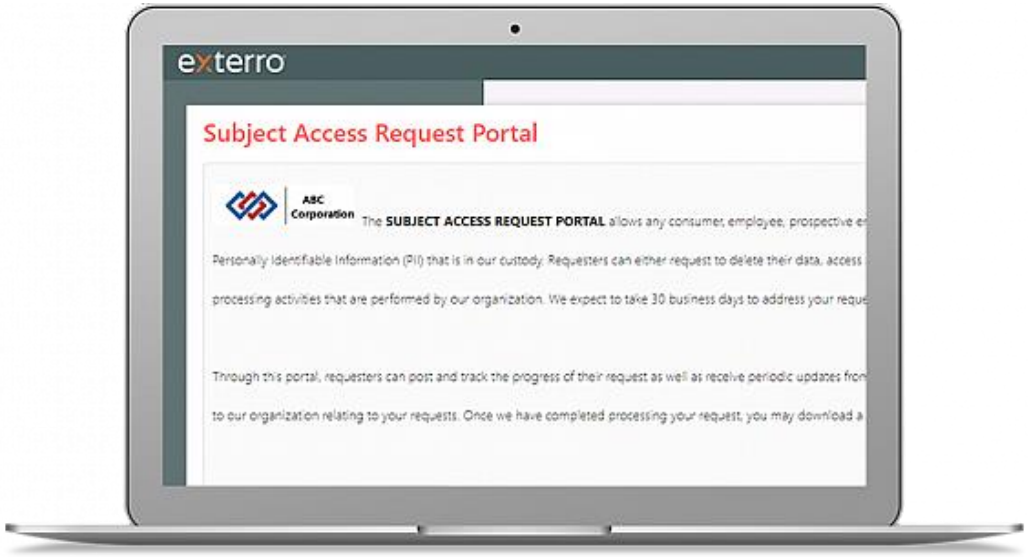


The outlook is grim…

- 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**

Gartner Research | **How to Prepare for the CCPA & Navigate Consumer Privacy Rights**

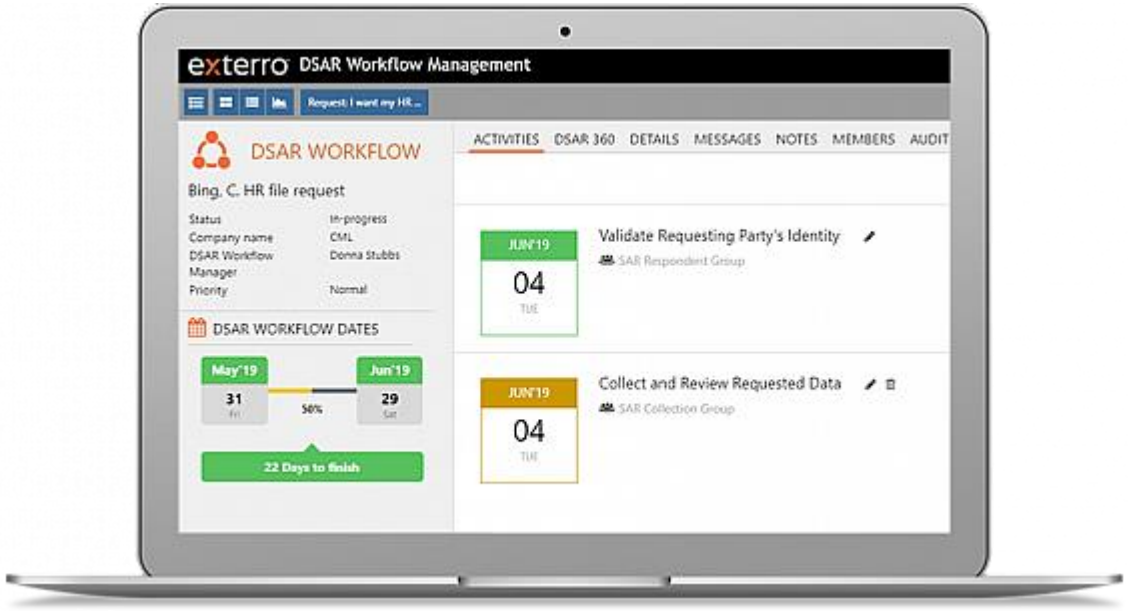
Well-Documented Process to Manage Requests



- Empower consumers to easily request data
- Keep data subjects informed about their requests
- Ensure consistency across the process

Configurable, Automated Workflows

- Track tasks and activities
- Notify appropriate personnel
- Mange Timelines
- Fulfill Verified Requests



Jordan Lawrence
an exterro company

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.

Data Risk in the Third-Party Eco System | **Ponemon Institute**

Jordan Lawrence
an exterro company

VENDOR RISK PROFILE

Identify Regulatory Applicability & Risks

Vendors Accessing Personal Data

INFO CUBIC BACKGROUND CHECKS · EY · aetna · iCIMS · HireRight · PageUp · ADP · AltusPartners THE POWER OF OBJECTIVITY · HubSpot · CROWN WORLD MOBILITY · Alere eScreen · NAVEX GLOBAL · OrangeTree · LabCorp · CHUBB

Vendors Accessing Systems

AIR INFORMATICS · 3D · ProData · SAFEMARK SYSTEMS

Vendors With No Access

resultspositive · RPT · qualtrics · ADART

Jordan Lawrence
an exterro company

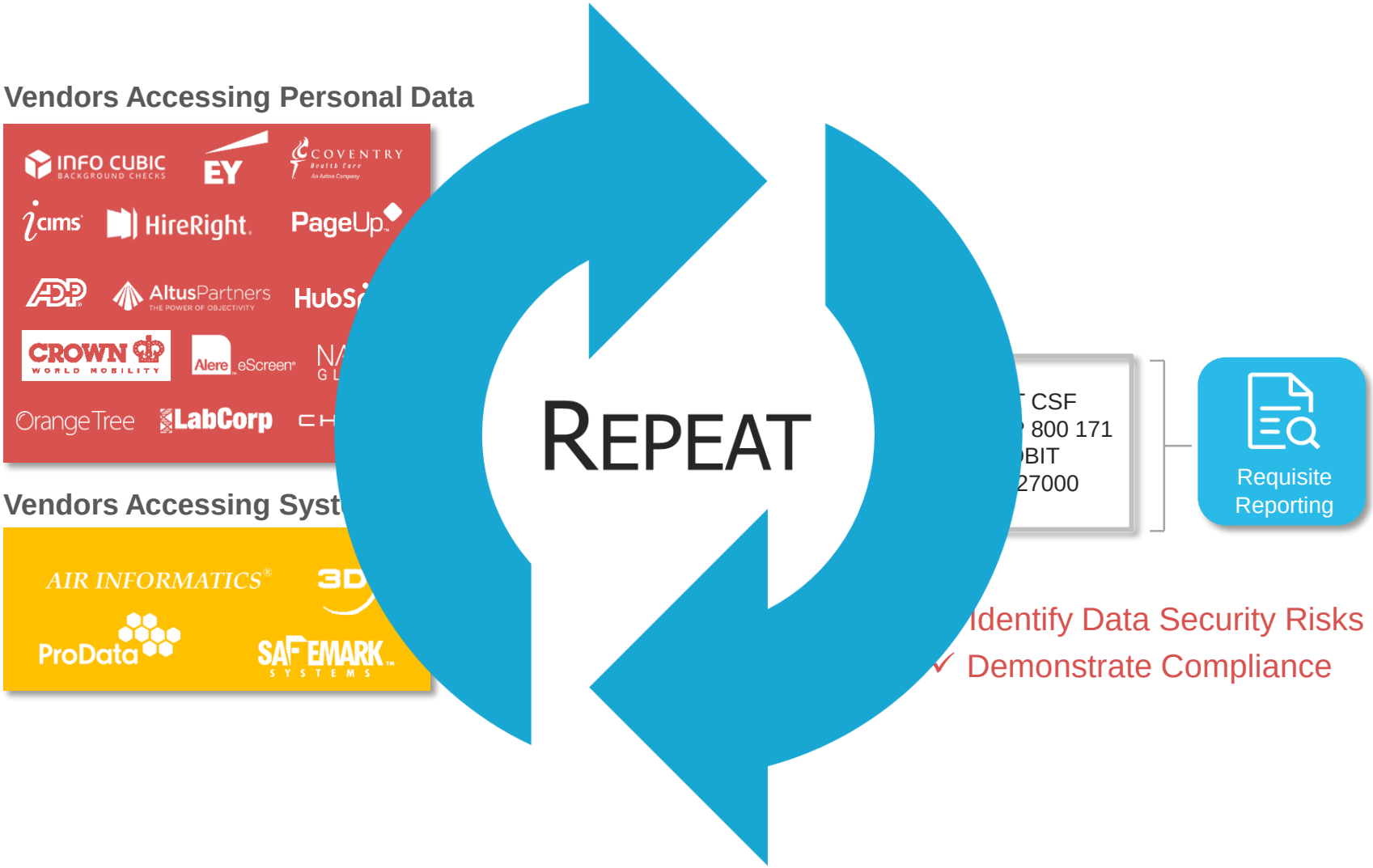
Evaluate Regulatory Applicability

ABC Company

Access to Personal Data Report

ACC VENDOR RISK SERVICE℠
Powered by Jordan Lawrence®

Vendor Name	Last Assessment	Assessment Name	Heatmap Score	Sensitive Data
A.B.Stearn	08/07/2017	Vendor Risk Profile	27 2 7	☐ BIO ☑ EMP ☑ PFI ☑ PII ☐ SI
API Logistics	09/05/2017	Vendor Risk Profile	30 1 2	☐ BIO ☐ EMP ☐ PFI ☐ PII ☐ SI
BND	09/01/2017	Vendor Risk Profile	27 2 5	☐ BIO ☑ EMP ☑ PFI ☑ PII ☐ SI
Ballard Marketing	07/27/2017	Vendor Risk Profile	28 2 3	☐ BIO ☐ EMP ☐ PFI ☑ PII ☐ SI
Cambridge Financials	07/13/2017	Vendor Risk Profile	23 4 6	☐ BIO ☐ EMP ☐ PFI ☐ PII ☐ SI
City Capital Bank	09/01/2017	Vendor Risk Profile	26 10 11	☐ BIO ☑ EMP ☑ PFI ☑ PII ☑ SI
Cubicle.com	08/18/2017	Vendor Risk Profile	23 15 4	☑ BIO ☑ EMP ☑ PFI ☑ PII ☑ SI
Design Heating & Cooling	07/20/2017	Vendor Risk Profile	28 3 2	☐ BIO ☐ EMP ☐ PFI ☐ PII ☐ SI
Infinite Analytics	09/25/2017	Vendor Risk Profile	26 6 4	☐ BIO ☑ EMP ☐ PFI ☑ PII ☐ SI



Assess Security & Compliance Readiness

ACC VENDOR RISK SERVICE℠
Powered by Jordan Lawrence®

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 jartors@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

ACCEPTED	MODERATE	HIGH
160	66	36

Access and Control Levels

DATA PROTECTION OFFICER: Bill Kennedy, bkennedy@abc.com

ACCESS LEVELS

- [x] Direct access to our personal data
- [ ] Direct access with our corporate netword
- [x] Indirect access within our corporate network
- [ ] Physical access within our corporate facilities

SECURITY CONTROLS

- [x] Data Encryption
- [ ] Routine Deletion
- [x] Incident detection and reponse
- [ ] 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	

Processing Activities

This vendor assists in and/or processing data related to the following processing activities:

Fourth Party Processing

Number of Sub-Processors that Process or Store Personal Data: 12

Jordan Lawrence®
an exterro company

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

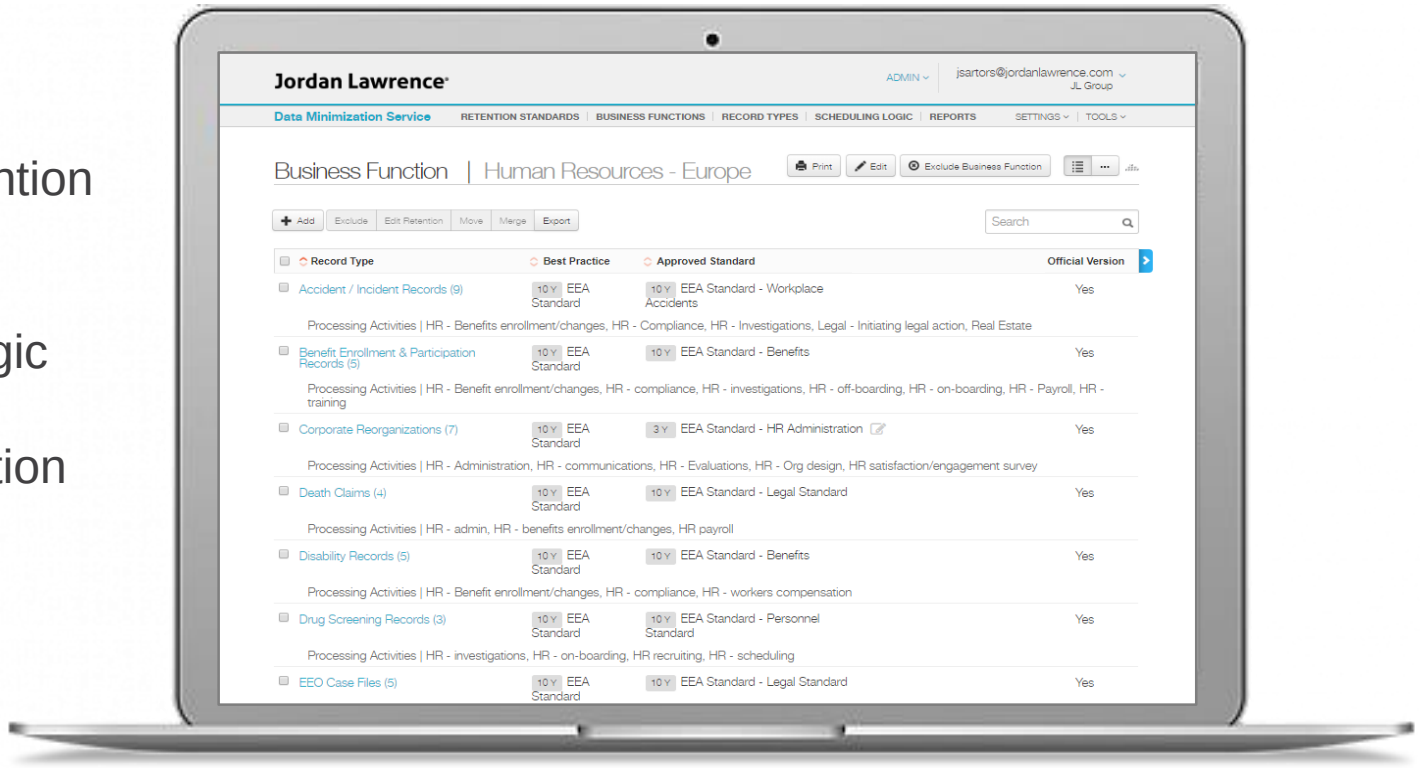
- ✓ Program Training
- ✓ Attestation
- ✓ Email
- ✓ File Share
- ✓ Structured Data
- ✓ Paper Records

MAINTAIN

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

Connect Personal Data to Retention Requirements

- Manage Retention Requirements
- Document Logic
- Develop Deletion Strategies



Jordan Lawrence
an exterro company

Questions?

Robert Fowler, CIPP-US
Director of Strategic Partnerships
Jordan Lawrence®
an exterro company

Phil Yannella, Partner
Practice Leader: Privacy and Data Security Group and
E-Discovery and Data Management Group
Ballard Spahr LLP