

RACE TO THE FINISH

2-MORNING CLE EVENT **JAN 27-28, 2021**

Acc Association of
Corporate Counsel
SAN FRANCISCO BAY AREA

TODAY'S DATA GOVERNANCE...
Lost in Translation

exterro[®]





Leader in E-Discovery, Data Inventory, Data Retention, Data Privacy & Cybersecurity Compliance

Years in Market:

- Exterro 15 +
- Jordan Lawrence 30 +
- 500+ Global Clients



Gartner®

COOL
VENDOR
2011

Gartner®

COOL
VENDOR
2020



Speakers:



Rebecca Perry CIPP/US/G
Director of Strategic Partnerships
Exterro



Fotis Konstantinidis
Managing Director, Head of AI and
Digital Transformation
Stout



Devika Kornbacher CIPP/US
Partner
Vinson & Elkins



SHIFTING REGULATORY LANDSCAPE

Poll

What data privacy regulation is your biggest concern in 2021?

- A. California Consumer Privacy Act (CCPA)
- B. California Privacy Rights Act (CPRA)
- C. Schrems II
- D. Other global regulations
- E. All of the above

Rapidly Expanding Data Privacy Regulations



Pioneering US Privacy Laws

- Toughest privacy law in the U.S.
- More control and oversight by the consumer over their personal information
- New obligations for businesses related to notice, disclosure, and response to consumer requests
- Effective January 1, 2020
- Enforcement July 1, 2020



CCPA 2.0

California Privacy Rights Act

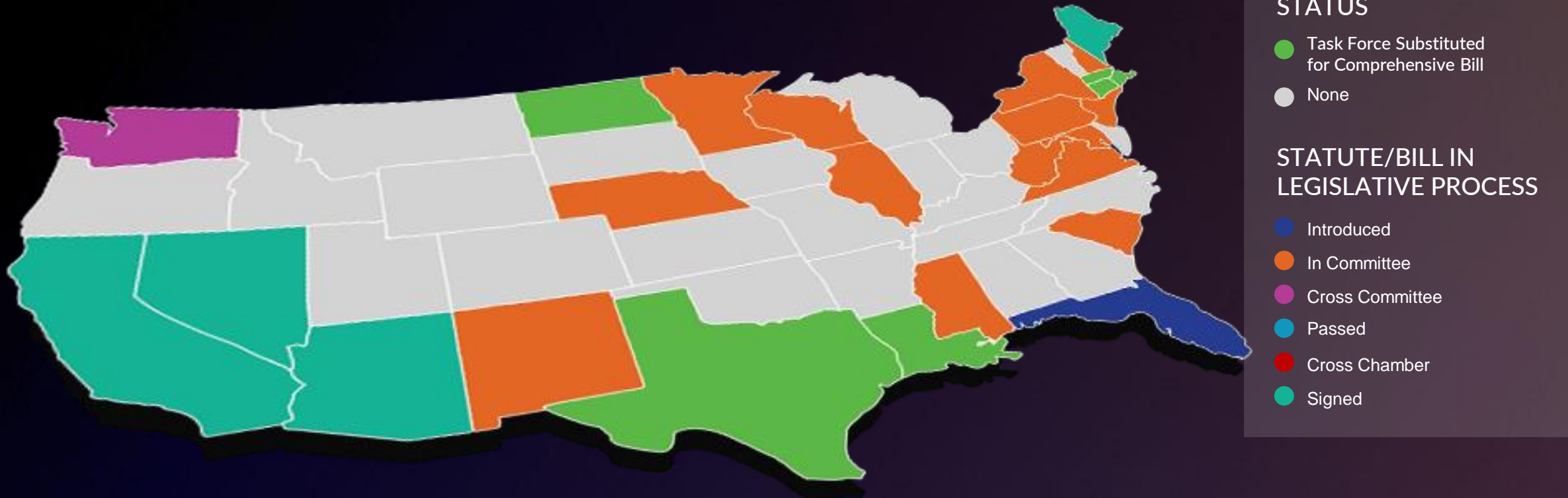
Will go into effect January 2023

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 Your 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?



LEARN MORE

<https://www.exterro.com/comprehensive-state-privacy-law-comparison/>



Poll

How familiar are you with the Schrems II decision?

- A. Not at all
- B. I've heard about it
- C. I've spent hours analyzing it

At what stage is your organization in making changes in response to the Schrems II decision?

- A. Still thinking
- B. Early stages
- C. Almost there

EU Ruling/Schrems II Case



What does this ruling mean
for your organization?



EU – U.S. Legal Transfer Mechanisms

Pre-Schrems II

Binding Corporate Rules
Express Consent
Binding and enforceable
commitment to apply appropriate
safeguards (e.g., Standard
Contractual Clauses)
EU-U.S. Privacy Shield

Post-Schrems II*

Binding Corporate Rules with
assessment and suspension/
termination rights
Express Consent
Binding and enforceable commitment
to apply appropriate safeguards (e.g.,
Standard Contractual Clauses), with
assessment, notice and
suspension/termination rights
~~EU-U.S. Privacy Shield~~

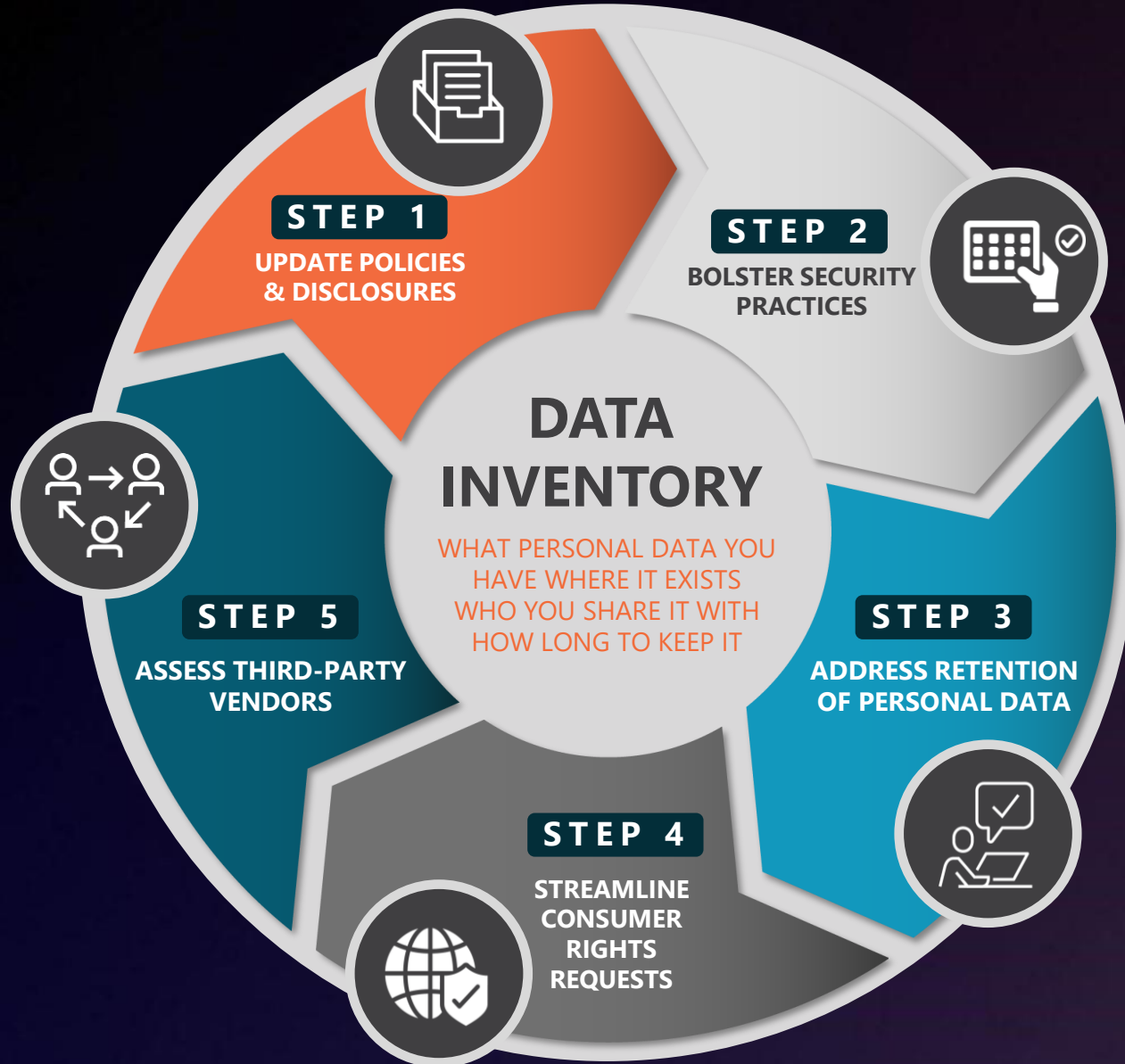




Streamlining Compliance to Mitigate Risks & Limit Liability






















































The Foundation for Defensible Compliance



Data Inventory Informs Compliance



	CONSUMER DATA	EMPLOYMENT/CORPORATE DATA
APPLICABILITY	           	  
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	   	   
LOCATIONS		    
THIRD PARTIES	   	   
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

Data Map | Personal Data Processing Activities

PROCESSING ACTIVITY: HR ONBOARDING
COUNTRY: UNITED STATES

Purpose of Processing

Associated Data Elements
Bio
G
Protected
Sensitive Pe
Personal Infor

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

Over Retaining Personal Data Is A Liability

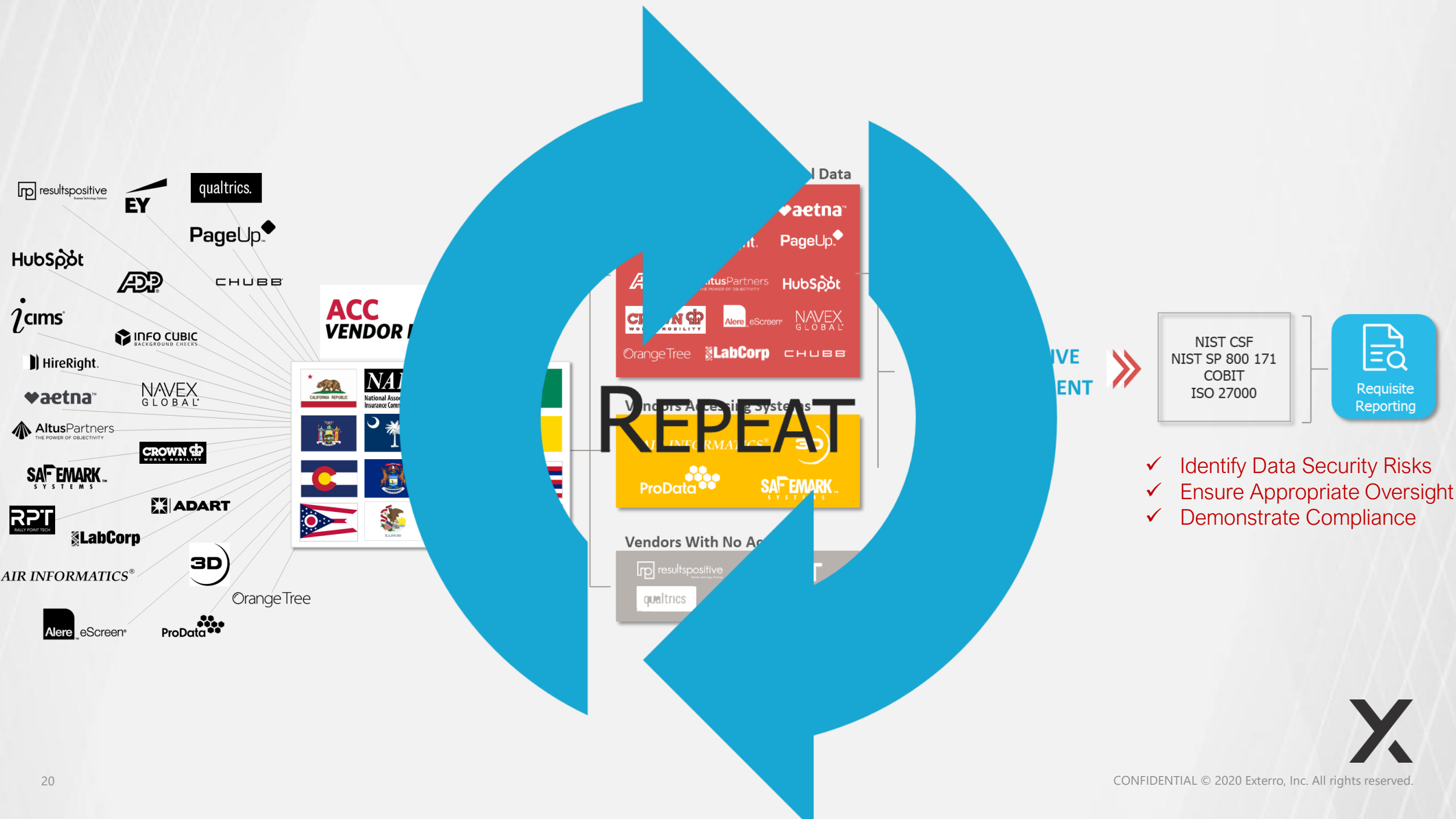


75%
OF RECORD TYPES
WITH PERSONAL DATA
ARE **OVER RETAINED**

Re-Assessing Vendor Relationships

- 1 Who are our vendors?
- 2 Which ones touch our data?
- 3 What specific data do they touch?
- 4 Which ones are relevant to GDPR?
- 5 How are our vendors protecting our data?





Legal's Role:

- ✓ Document Diligence
- ✓ Get the right contracts in place
- ✓ Surface Data Protection Risks
- ✓ Work with IT to Remediate Risks
- ✓ Produce Requisite Reporting

Vendor Data Protection & Security Diligence Review

Vendor Name | Rack TechnologiesHeat 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

1606636

ACCEPTEDMODERATEHIGH

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 reponse
☐ Regular Risk Assessments

Data Processed, Accessed or Stored

PERSONAL DATA

PERSONAL

Birth DateFirst/Last NameGender

Marital StatusPhone NumberSSN

PERSONAL FINANCIAL

Tax Info.

EMPLOYMENT

Employee ID

SPECIAL CATEGORIES DATA - GDPR ARTICLE 9

SENSITIVE PERSONAL

Blood TypeEthnic Origin/Race

PROTECTED HEALTH

Dates of Service

Processing Activities

Fourth Party Processing

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

Number of Sub-Processors that Process or Store Personal Data

12



PANIC



VS.

PREPARED



Questions...

For further information please contact:

Rebecca Perry

rebecca.perry@exterro.com

Fotis Konstantinidis

fkonstantinidis@stout.com

Devika Kornbacher

dkornbacher@velaw.com

exterro[®]