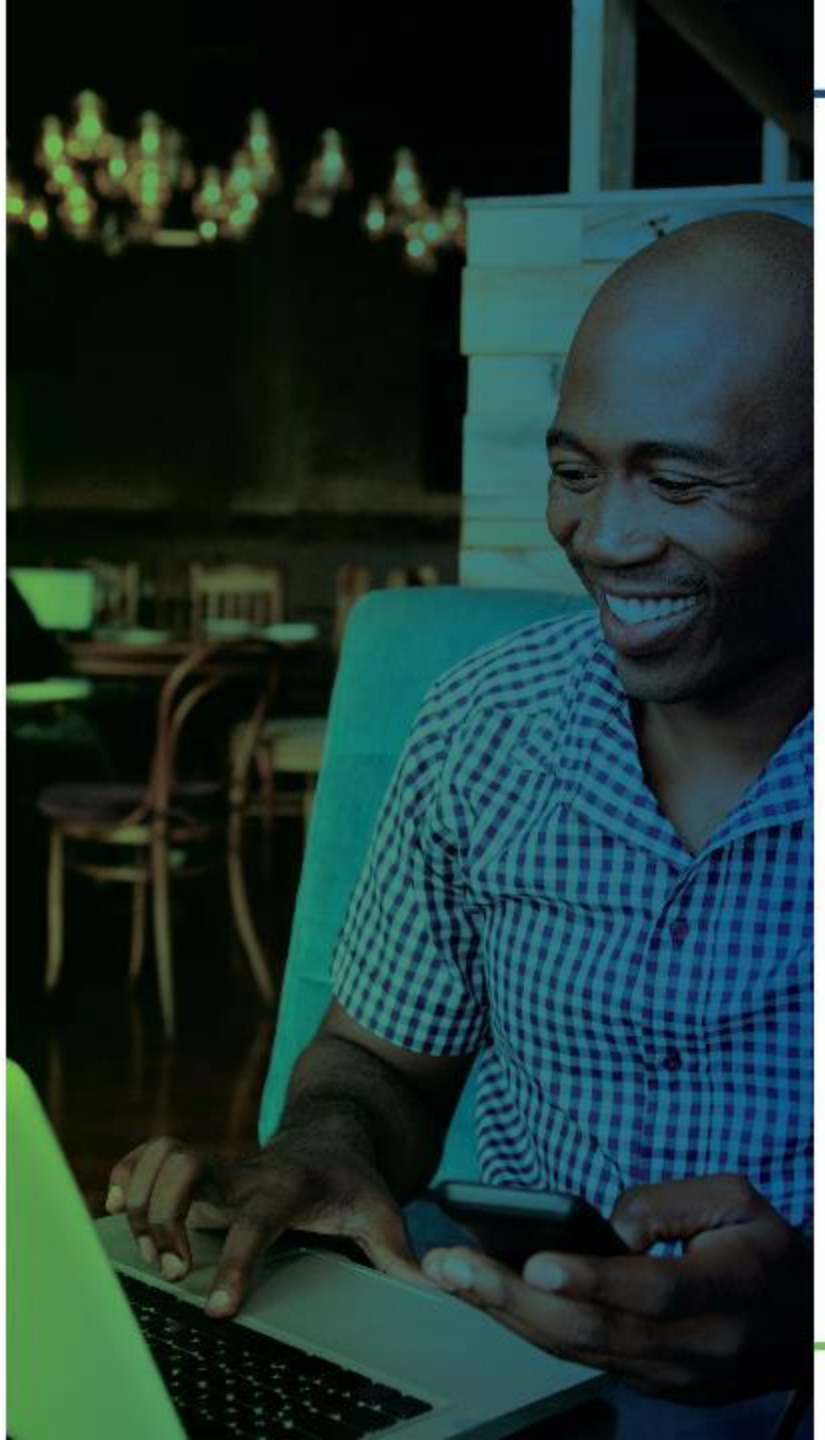


Mastering Data Inventories: Strategic privacy compliance and data governance

Wednesday, 24 January
08:00-09:00 PST
11:00-12:00 EST
17:00-18:00 CET

Welcome & Introductions

Fahad Diwan,
JD, FIP, CIPP/C, CIPP/M

Director of Privacy & Data Governance Products

Exterro

Michael Hellbusch,
CIPP/E, CIPP/US, CIPM

Data Privacy and Cybersecurity Partner

Rutan & Tucker

THE ONLY PLATFORM TO BRING IT ALL TOGETHER

Agenda

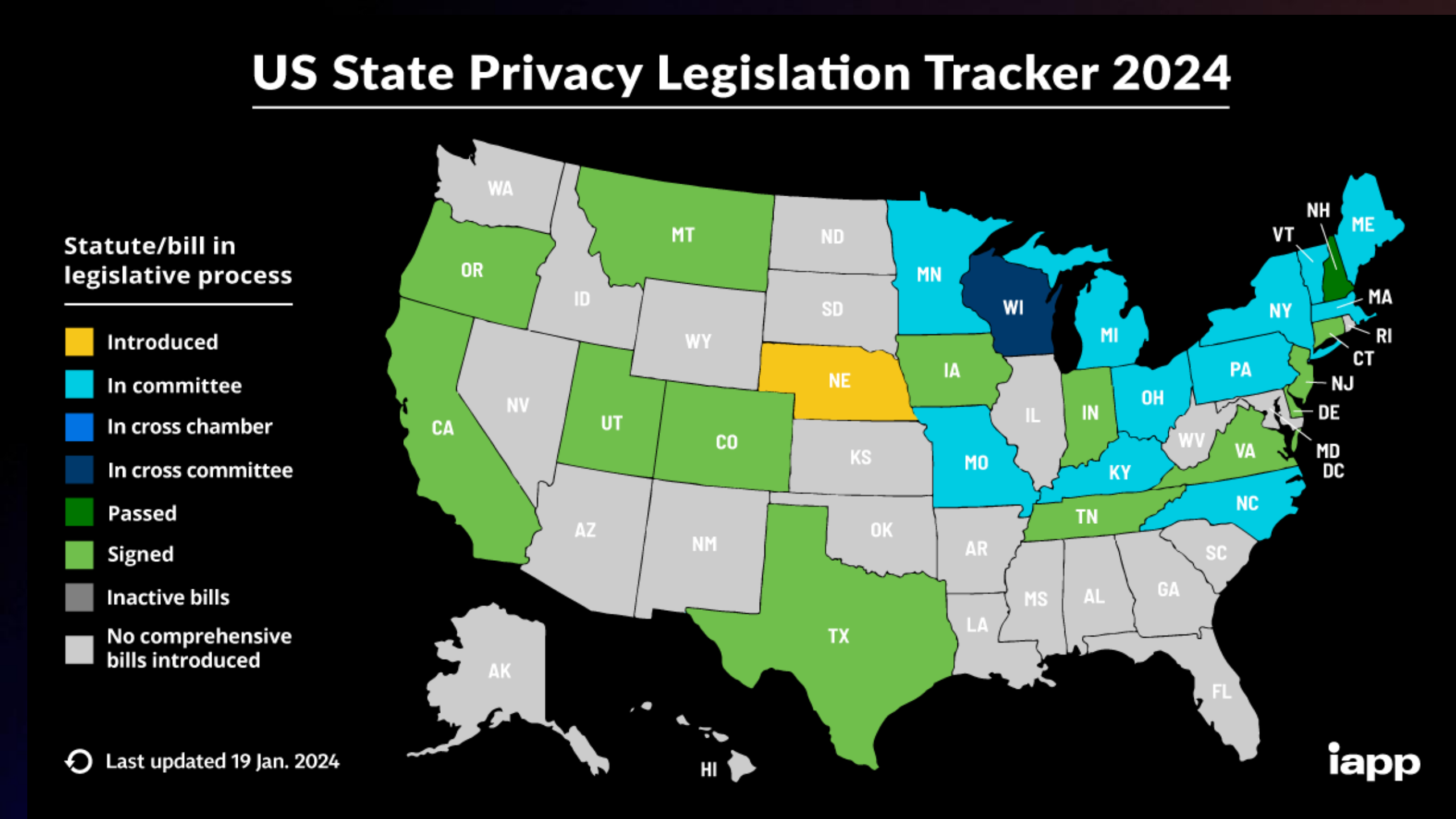
- Overview & Recent Developments in Data Laws
- Convergence to Data Risk Management
- Best Practices

Overview & Recent Developments in Data Laws

Privacy Law Developments

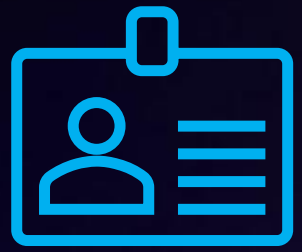
- State Privacy Law Patchwork
- Categorizing Personal Data
- Jurisdictions, sensitive, children, etc.
- Other privacy laws
- CIPA/Wiretapping, VPPA
- Privacy Impact Assessments
- Vendor management

US State Privacy Legislation Tracker 2024



Regulation by Industry

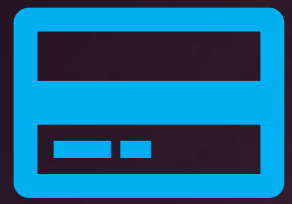
Finance



Employees

Children

Health



Credit

Privacy Law Developments

- CPPA Risk Assessment Regulations (DRAFT)
  - Applicable for selling/sharing, sensitive PI, automated decision-making, children's data, AI training.
  - Required for each processing activity.
  - Include a description of how the business will processing the personal information, including how the business will collect, use, disclose, and retain the personal information used in the processing activity.
  - Business must consider negative impacts (harms) from the processing activity to consumers' privacy.

Data Security Developments

- Emerging cybersecurity regulations
  - E.g., CCPA Regs, SEC Cybersecurity Rule
- Enforcement Actions
- Takeaways

CCPA Cybersecurity Regs (Draft)

- Cybersecurity Audit required for every business whose processing presents "significant risk" to consumer's security. Significant risks, include:
  - Deriving 50% of annual revenues from selling/sharing
  - Large amounts of data processing per year
  - Processing large amounts of sensitive personal information
  - Processing large amounts personal information of children

CCPA Cybersecurity Regs (Draft)

- Annual Audits for covered businesses
- External auditor or internal “independent” auditor
- Audit must assess and document how cybersecurity program:
  - Protects against unauthorized access, destruction, use, etc.
  - Protects against loss of availability
  - Protects against harms associated with security incident
- Regulations require personal information inventories, classification, tagging.

SEC Cybersecurity Regulations

- 2 primary components:
  - Disclosure of Material Cybersecurity Incidents
    - Filed on Form 8-k within four (4) business days of determining material incident.
  - Annual Disclosure of Cybersecurity Risk Management, Strategy, and Governance.
    - Requires a comprehensive disclosure of processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats.

EyeMed Vision Care LLC - NY DFS Consent Order

- EyeMed is a regulated entity subject to the NY Cybersecurity Regulation.
- Regulations requires all DFS-Regulated entities to establish cybersecurity program to protect Nonpublic Information (NPI).
- Regulation requires multi-factor authentication (MFA) for access to internal networks from an external network (i.e. email accounts).
- Regulation also requires data minimization on NPI.
- EyeMed email account compromised via phishing email.
  - No MFA, 9 employees with access to account using same username and password.
  - Intrusion lasted for one week.
  - Threat actor had ability to exfiltrate the documents and information in the mailbox during time of access.

EyeMed Vision Care LLC - NY DFS Consent Order

- Finding: EyeMed
  - Failed to Implement MFA
  - Failed to conduct risk assessments
  - Failed to limit user access to systems
  - Failed to safely dispose of NPI that is no longer necessary
  - Improperly certified compliance with Cybersecurity Regulation
- Settlement:
  - $4.5 million penalty
    - DFS noted EyeMed's "commendable cooperation" when considering penalty amount.
  - Conduct risk assessment and provide action plan to address risks.
  - "Full and complete cooperation" with DFS.

EyeMed Vision Care LLC - NY DFS Consent Order

- Takeaways:
  - Data inventories require determination of all applicable laws/regulations (especially for email).
  - Retention and data destruction policies are necessary and informed by regulation (e.g., statutory retention and/or “necessary” test)
  - Data inventories inform risk assessments and analysis.
  - Data inventory is a multi-disciplinary project.
  - Non-compliance may result in fines/penalties even if no demonstrable harm (i.e. risk of exfiltration vs. actual exfiltration).

AI Developments

- AI Governance requires data inventory
  - Inventory of Data Input
  - Identification of Data Output
  - Automated Decision-making
  - Risk Assessment and Management
  - Opt-Out Rights
  - Elimination of Bias
  - Understanding Logic of AI/ADM

Convergence to Data Risk Management

Laying the Foundation

WHO

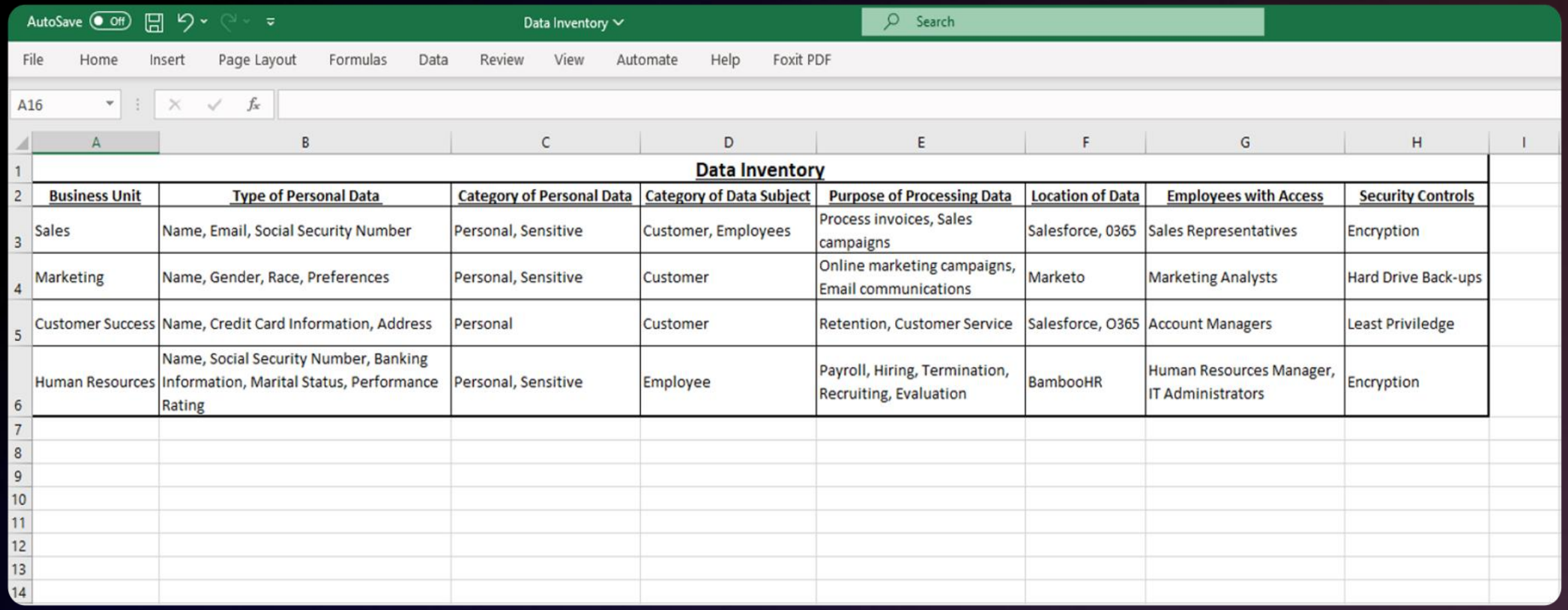
WHAT

WHEN

WHERE

WHY

Manual Data Inventory



AutoSave Off | Data Inventory | Search

File Home Insert Page Layout Formulas Data Review View Automate Help Foxit PDF

A16

Data Inventory

Business Unit	Type of Personal Data	Category of Personal Data	Category of Data Subject	Purpose of Processing Data	Location of Data	Employees with Access	Security Controls
Sales	Name, Email, Social Security Number	Personal, Sensitive	Customer, Employees	Process invoices, Sales campaigns	Salesforce, 0365	Sales Representatives	Encryption
Marketing	Name, Gender, Race, Preferences	Personal, Sensitive	Customer	Online marketing campaigns, Email communications	Marketo	Marketing Analysts	Hard Drive Back-ups
Customer Success	Name, Credit Card Information, Address	Personal	Customer	Retention, Customer Service	Salesforce, O365	Account Managers	Least Priviledge
Human Resources	Name, Social Security Number, Banking Information, Marital Status, Performance Rating	Personal, Sensitive	Employee	Payroll, Hiring, Termination, Recruiting, Evaluation	BambooHR	Human Resources Manager, IT Administrators	Encryption

Manual Data Inventory

Time Intensive

High Effort

Incomplete & Inaccurate

Out-of-Date

Data Discovery

- IAPP Definition:
  - “Data discovery tends to be an automated technology that helps organizations determine and classify what kind of personal data they possess to help manage privacy risk and compliance.”
- Discovers and classifies personal and sensitive data
- Good solutions:
  - Discover data across the organizational landscape
  - Provide additional contextual information
- Great solutions:
  - Part of a comprehensive data risk management platform

Benefits of Data Discovery

Manual Approach

- Time-Intensive
- High Effort
- Incomplete & Inaccurate
- Out-of-Date

Data Discovery

- Quick
- Streamlined
- Complete & Accurate
- Up-to-Date

Best Practices

Break Down the Silos

- Privacy can no longer be a siloed function
- Data Discovery requires cross-organizational support
- Must work with data stakeholders across the organization

Best Practices

- Focusing on managing data risk
- Start with data discovery
- Procuring platform vs. point solutions
- Working cross-functionally

Cross-Functional

- Privacy
- Data Security
- Data Governance
- E-Discovery
- Digital Forensics
- AI Governance

Questions?

Fahad Diwan,
JD, FIP, CIPP/C, CIPP/M

Director of Privacy & Data Governance Products

Exterro

Michael Hellbusch,
CIPP/E, CIPP/US, CIPM

Data Privacy and Cybersecurity Partner

Rutan & Tucker

Web Conference
Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: https://iapp.questionpro.com/t/AOhP6Z1Ctz

Thank you in advance!

For more information: www.iapp.org

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration will automatically receive credit. If another certified professional has participated in the program but is not the named participant then the individual may submit for credit by submitting the continuing education application form here: submit for CPE credits.

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other
IAPP Web Conferences or recordings
or to obtain a copy of the slide presentation please
contact:

livewebconteam@iapp.org