exterro®

Global privacy and cyber law trends

How data management practices can help meet the challenges of a fragmented global landscape

Welcome and Introductions

Maggie Ledbetter, CIPP-US
Director, Professional Services- Privacy,
Exterro
maggie.ledbetter@exterro.com

Justine Phillips
Privacy and Cybersecurity Partner
Baker McKenzie
Justine.Phillips@bakermckenzie.com

Cynthia Cole
Intellectual Property Partner
Baker McKenzie's
cynthia.cole@bakermckenzie.com

Christine McGrath
Senior Privacy Counsel
Autodesk
christine.mcgrath@autodesk.com

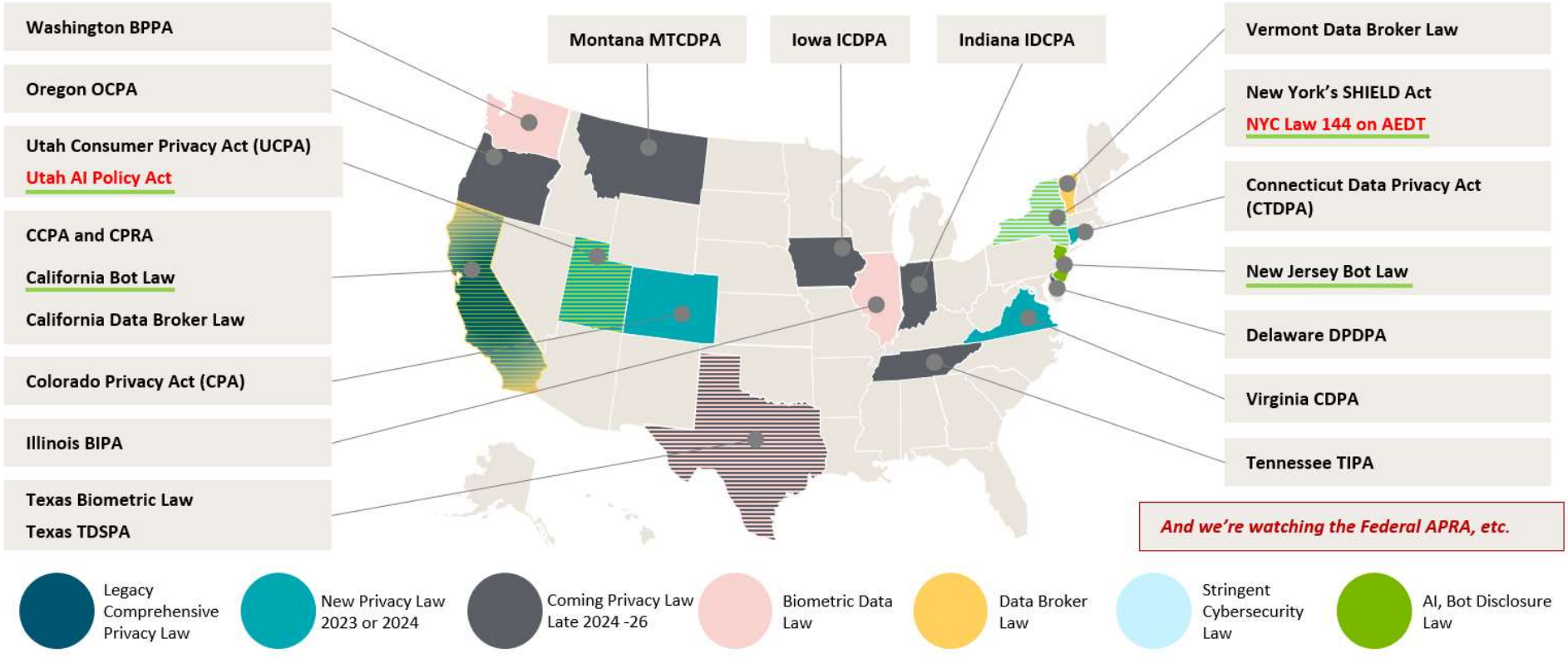
Dawn Maruna
Managing Senior Counsel, Privacy
Palo Alto Networks
dmaruna@paloaltonetworks.com

Agenda

1. Global Data Protection and Cyber Laws and Trends
2. Data Risk Management Strategy
3. Leveraging Tools and Technologies

Global Data Protection and Cyber Laws and Trends

Notable U.S. Privacy & Cyber Laws & Regulations



Noteworthy Global Privacy & Cyber Laws & Regulations

Europe: GDPR, NIS2, DORA

India: DPDP Act

China: CSL, DSL, PIPL

Australia: review of Privacy Act

Brazil: LGPD

Current Client Concerns

Supply chain risk

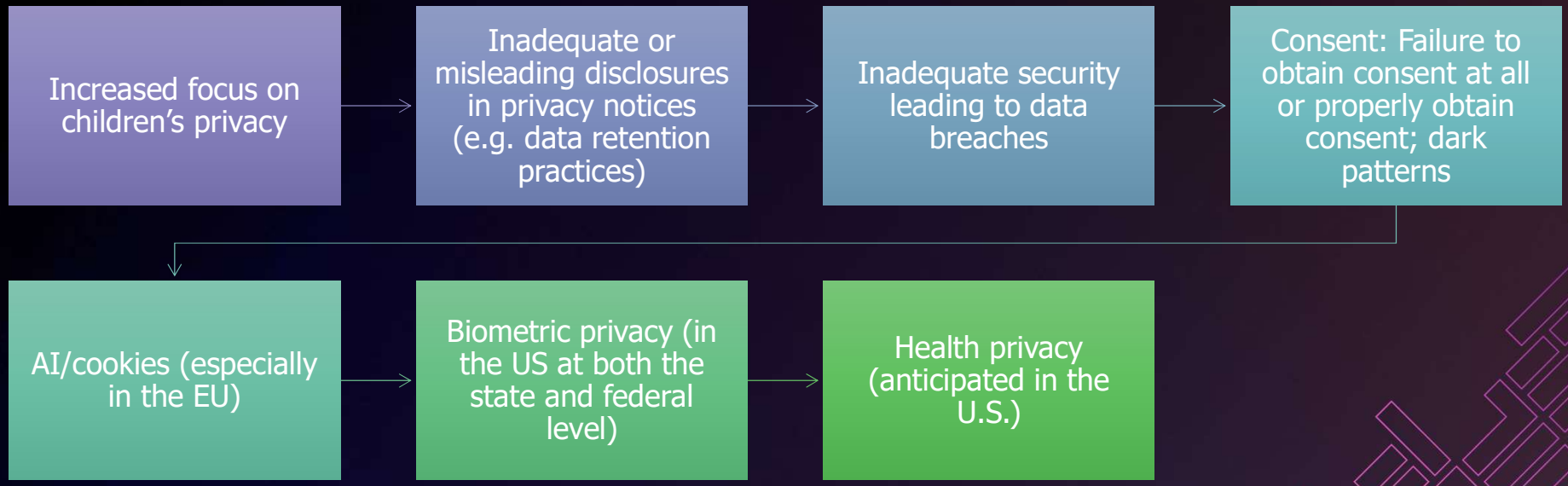
Health data

Litigation risk from web-tracking

Consumer requests

Incident response and cyber resilience

Global Enforcement Trends



Key Principles for Global Privacy Frameworks

Notice

Provide clear and easily understandable information about what personal data is being collected, how it will be used, and any third parties with whom the data may be shared.

Choice

Give individuals the right to make decisions about the collection and use of their personal data.

Purpose Limitation

Specify the purposes for which personal data is collected and ensure data is not used for purposes that are incompatible with the original stated intent.

Accountability

Be prepared to document and demonstrate compliance.

Accuracy

Take reasonable steps to ensure the data is accurate, up-to-date, and relevant.

PETs (Privacy Enhancing Technologies)

Tools designed to protect and enhance individual privacy and mitigate privacy risks (e.g., encryption, anonymization)

Data minimization & Proportionality

Limit personal data collection to what is necessary. Ensure data collection and processing is appropriate and reasonable for the specified purpose.

Storage limitation and Retention

Do not store personal data for longer than necessary for the purposes for which the data was collected. Securely store data before it is permanently deleted or anonymized.

Lawfulness, Fairness, and Transparency

Have a lawful basis, respect individual rights, prevent harm, and openly allow for individuals to make informed decisions about personal data processing.

Global Privacy Requirements

	Protects:	Applies to:	Basis for processing:	Rights:
GDPR	"Data subjects" meaning identifiable natural persons who can be identified by reference to an identifier	"Controllers" that offer goods, services or monitor the behavior of persons in the EU; "Data Processors"	Consent-based (though other bases exist). Consent may be withdrawn at any time.	Transparency; access; correction; deletion; restriction of processing; portability; right to object
CCPA	"Consumers", meaning natural persons who are California residents	Businesses that: (1) operate for profit; (2) determine the purposes/ means of processing; (3) do business in California; and (4) meet one of the processing thresholds	Generally opt-out-based. Only require consent for entering financial incentive program, selling/sharing children's data.	Know; access; portability; deletion; correction; non-discrimination; limit use of sensitive personal information
BIPA	Subjects of biometric identifiers or biometric information	"Private entities" meaning any individual, partnership, corporation, limited liability company, association, or other group	Written consent from subject required before biometric identifier or biometric information is collected	Private right of action
WA MHMD	"Consumers" meaning natural persons who are Washington residents or whose consumer health data is collected in Washington	Persons and businesses that conduct business in Washington and that collect, process, share, or sell consumer health data	Prior opt-in consent required for processing unless the processing is necessary to provide a product or service requested by the consumer	Know; access; obtain list of third party recipients; withdraw consent; deletion

Global Cyber Notification requirements: endless variations

	Applicability	Trigger	Timing
SEC Cyber Rules	Public companies	"Material" incident	Within **4 days** of materiality determination
HIPAA Breach Notification Rule	"Covered Entities" and "Business Associates"	If breach affect 500+ individuals	Without unreasonable delay and in no case later than **60 days** following discovery of breach
Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)**	"Covered Entities" in a critical infrastructure sector	"Substantial cyber incident"	Within **72 hours** of when a covered entity reasonably believes an incident occurred
EU General Data Protection Regulation (GDPR)	Controllers that process EU citizens' personal data	"Personal data breach", unless unlikely to result in a risk to personal rights/freedoms	Within **72 hours** of becoming aware of breach
India's CERT Directions	Service providers, intermediaries, data center, and others	Any real or suspected adverse cybersecurity incident that violates applicable security policy	Within **6 hours** of detection or being notified of incident

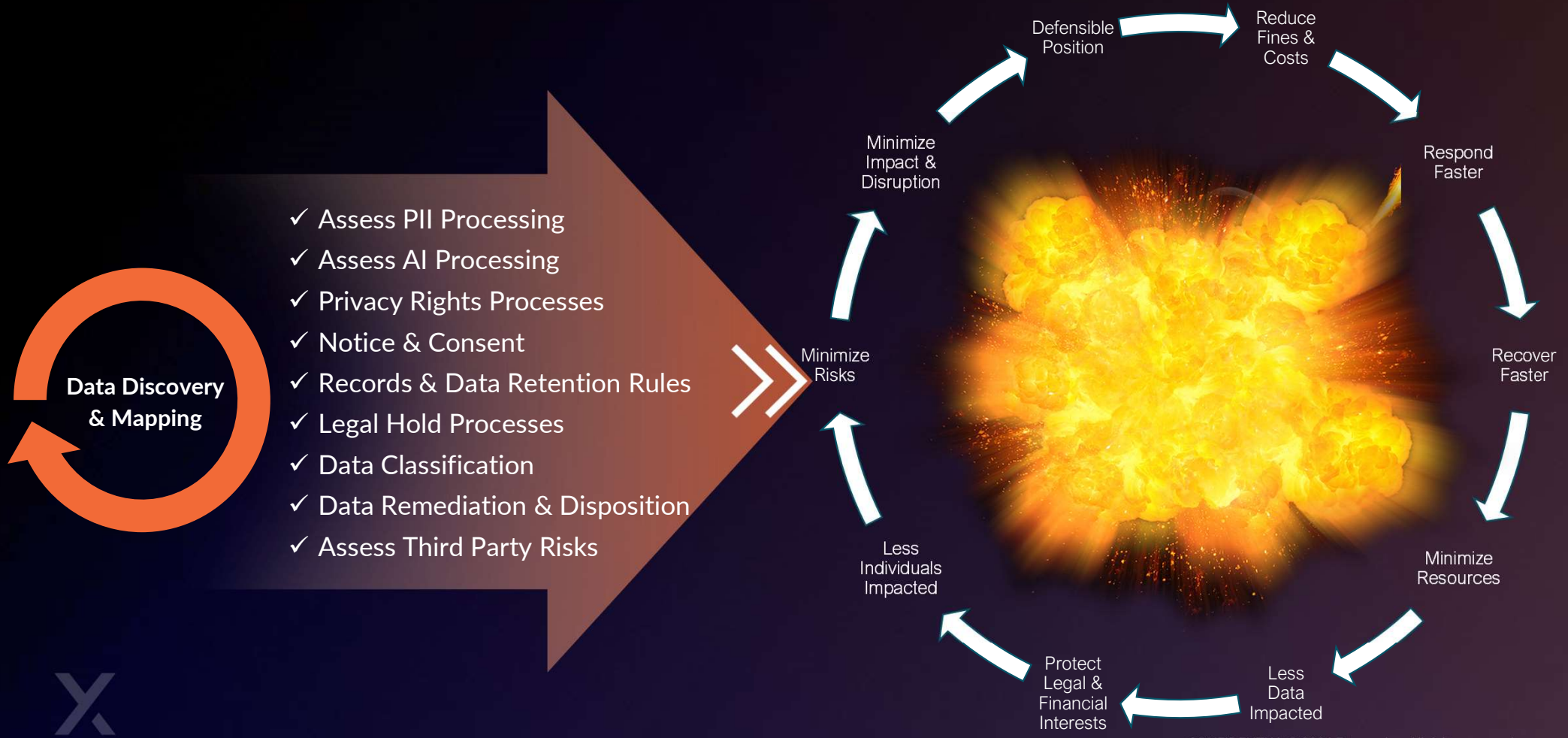
**CIRCIA rulemaking process commenced in March 2024; expected to come into effect by October 2025

Data Risk Management Strategy

Questions

Questions

Impact of a Strong Data Risk Management Strategy



Proactive vs. Reactive Data Risk Management

Leveraging Tools and Technologies

Achieving an Effective Data Risk Management Strategy

Set a Strong Data Governance Foundation

- Develop data inventories and conduct data mapping.
- Define roles and responsibilities.
- Understand legal and regulatory requirements, as well as industry best practices and standards.
- Establish policies, procedures, and guidelines to ensure that data is managed effectively, securely, and in compliance with laws. Address collection, use, storage, sharing, quality, accuracy and record retention.

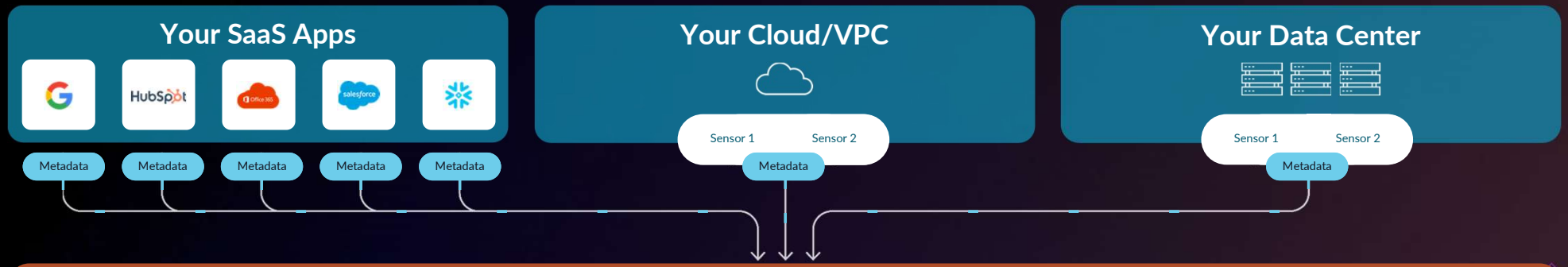
Achieving an Effective Data Risk Management Strategy

Automate with Technology

Set a Strong Data Governance Foundation

- Leverage Technology: Automate and centralize risk management and compliance functions to improve operational efficiencies.
- Automation Tools for Data Governance: Data discovery, classification, mapping, and access control.
- Benefits of Automation: Increased efficiency, accuracy, and consistency in data management, as well as improved compliance and less risk of human error.
- Integrate with Existing Systems and Workflows: To minimize disruption and maximize efficiency.
- Consider: Cost, complexity, and the need for ongoing maintenance and support.

Unleashing The Power of Data Discovery



AI-Powered Data Discovery Technology

Data Inventory / Catalog | Policy & Rules Engine | Reporting | APIs

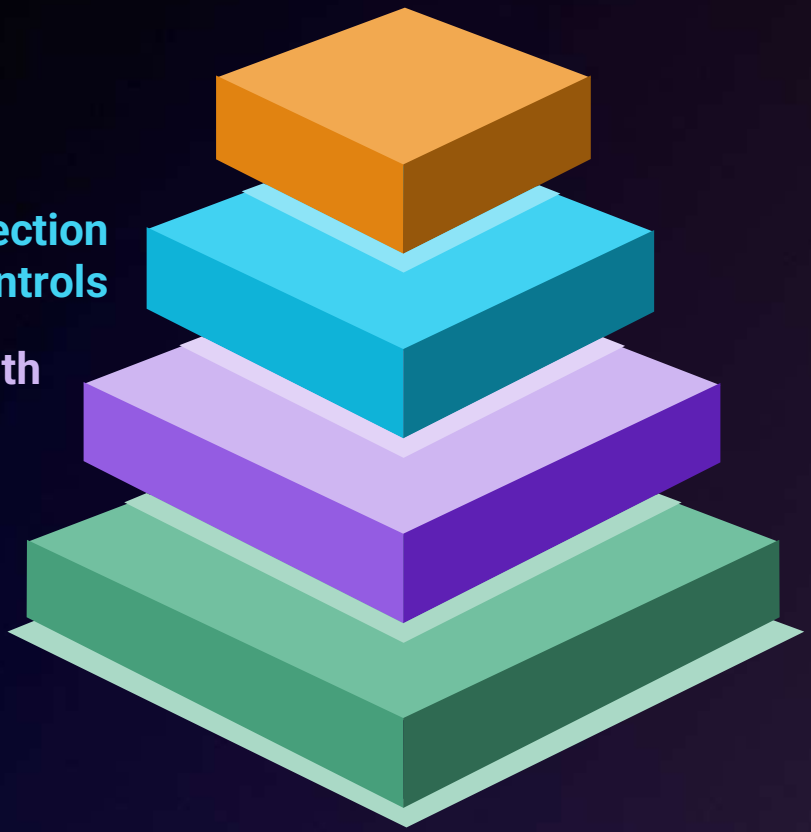
- Data Retention & Deletion
- Legal Holds
- Data Mapping & RoPA
- Privacy Rights Requests

Achieving an Effective Data Risk Management Strategy

Build in Data Protection Controls

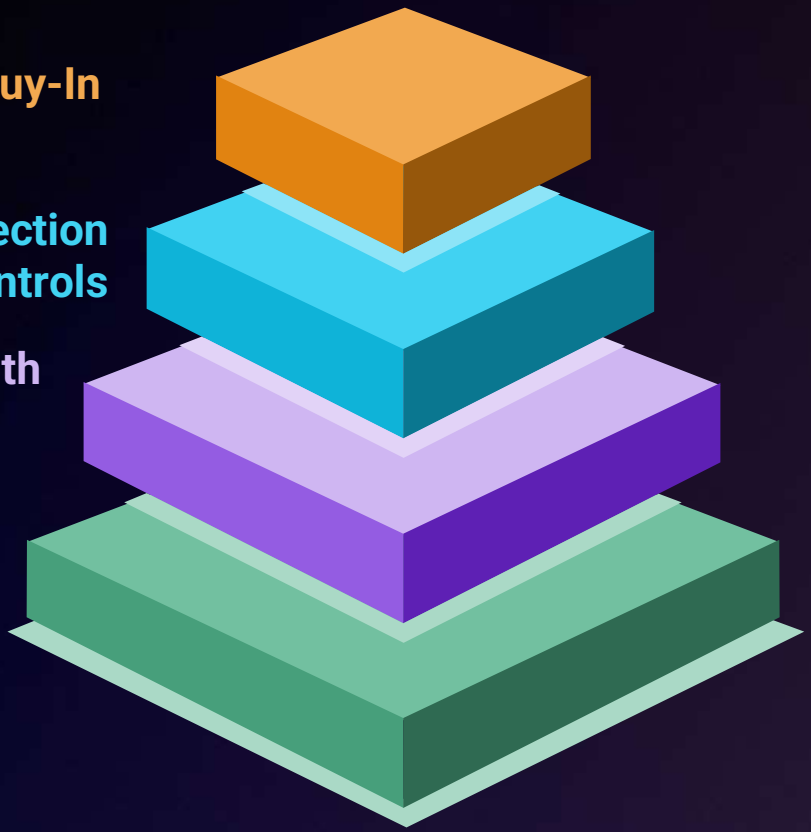
Automate with Technology

Set a Strong Data Governance Foundation



- Implement Privacy & Security By Design.
- Conduct Privacy Impact Assessments and Security Reviews to address dynamic and continuously evolving privacy risks.
- Develop and review contractual controls.
- Data Security Measures: Use robust data security measures, including encryption, access controls, data loss prevention, and network security.
- Data Minimization and Anonymization: Minimize the collection and retention of personal data and use PETs.
- Benefits: Compliance with global regulations and improved data breach response.

Achieving an Effective Data Risk Management Strategy



- Ensure senior management buy-in and support.
- Collaborate with cross-functional stakeholders.
- Build a strong culture of privacy and compliance through education and training.
- Develop a communication strategy.
- Measure and track progress.
- Regularly assess the effectiveness of stakeholder engagement and make adjustments as needed.

A Complete Orchestrated Solution