PROGRAM MATERIALS
Program #3655
March 12, 2026

Building the Data Privacy & AI Governance Foundation: The Four Documents Every Organization Needs

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919

PORZIO

BROMBERG & NEWMAN

Building the Data Privacy & AI Governance Foundation:

The Four Documents Every Organization Needs

Alfred R. Brunetti, Esq. CIPP/US, CIPM

Chair - Data Privacy Practice Group

Variety of Privacy Concepts

Information Privacy

collecting & processing of personal information

Bodily Privacy

physical, biological, behavioral being & activity

Territorial Privacy

intrusion on physical environment, tracking

Communications Privacy

written, electronic, audio

Data Privacy is…

The use and governance of Personal Data

(i.e. *information linked or reasonably linkable to an identified or identifiable person*)

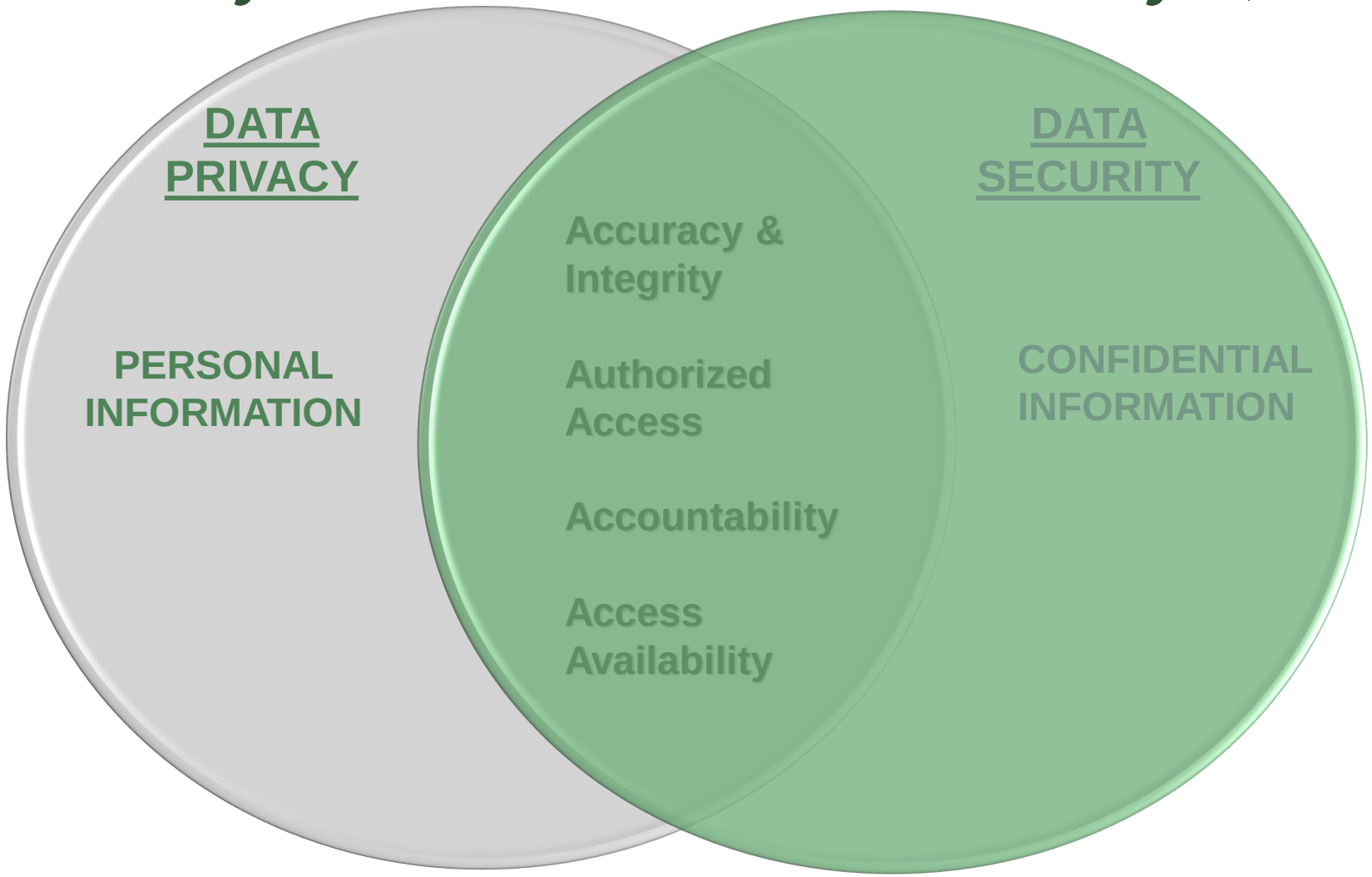
Based upon autonomy and having control over your personal information; how it is collected and how it is used or disseminated.

Rights given to Data Subjects

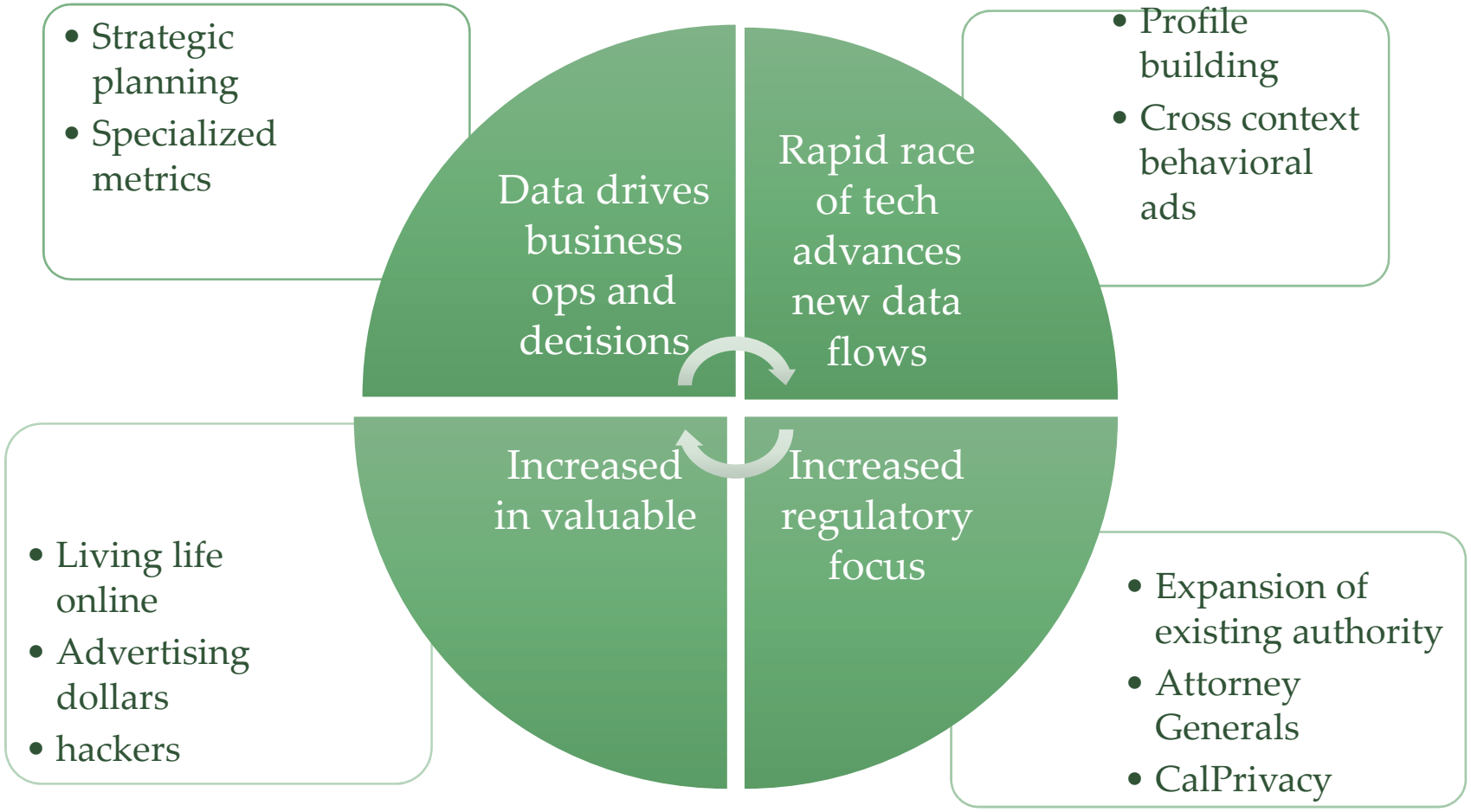
Obligations placed upon Businesses

Attendant **Risk Management**

Data Privacy versus Data Security (InfoSec)



Why Data Governance is so important



U.S. versus EU Privacy Regimes

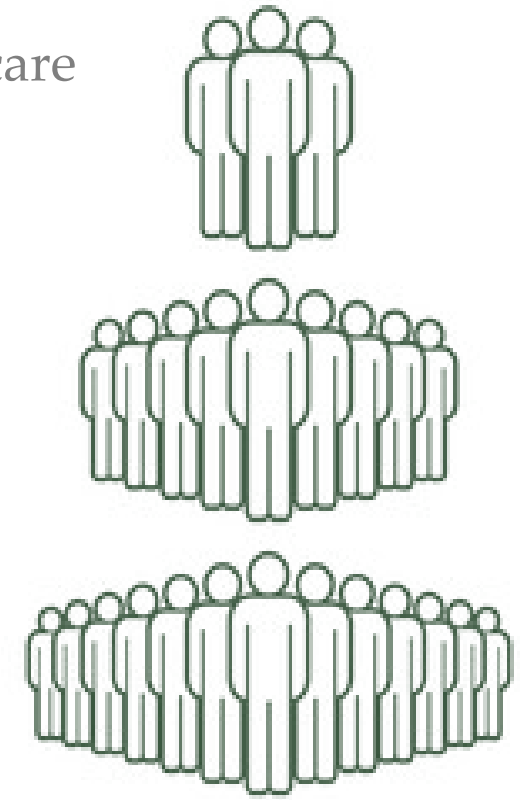
- No comprehensive federal privacy law (as of today)
- Federal privacy laws are sector specific, *e.g.,* HIPAA covers some health data. States continue to pass their own 'comprehensive' consumer data and consumer health data laws.

- European countries enforce a generally common regulation that emphasizes that protecting against the processing of personal data is a fundamental *right*.
- This *right* exists regardless of the sector where the personal data exists.

Sectoral to 'Comprehensive'

Some familiar federal 'sectoral' data laws :

- Health Insurance Portability & Accountability Act of 1996 (HIPAA) - healthcare
- Gramm-Leach Bliley Act (GLBA) - financial / insurance institutions
- Children's Online Privacy Protection Act (COPPA) - children u13
- Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) - commercial email including opt-outs
- Telephone Consumer Protection Act (TCPA) - telemarketing
- Family Educational Rights and Privacy Act (FERPA) - student education records
- Genetic Information Nondiscrimination Act (GINA) - job related decision discrimination



Where Are We Today?

21 separate *'comprehensive'* state data privacy laws

+

sectoral federal schemes

+

more than 140 other country regimes

=

increasing compliance requirements for businesses while offering consumers **more control over their personal data**

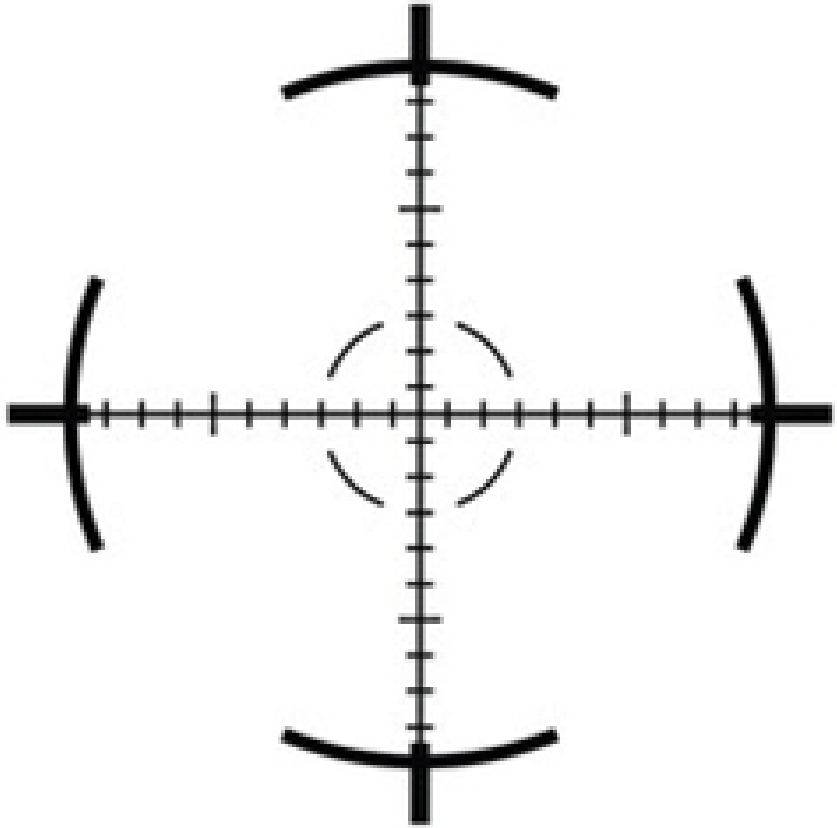
Falling in SCOPE of state comprehensive consumer data privacy laws

Context (personal/household or employment/B2B)

Number (of consumers)

Activity (with the data)

Revenue (total or specific to actions)



An example of complexity: What is Health Data?

Health data is typically any info related to a person's physical or mental health, healthcare services, status or condition

Diagnoses, Treatments, Medical History

Medical Records

Exercise routines, calories logging, etc (think fitness apps or trackers)

Wellness Information

Biological, physiological or behavioral characteristic, patterns, rhythms, scans

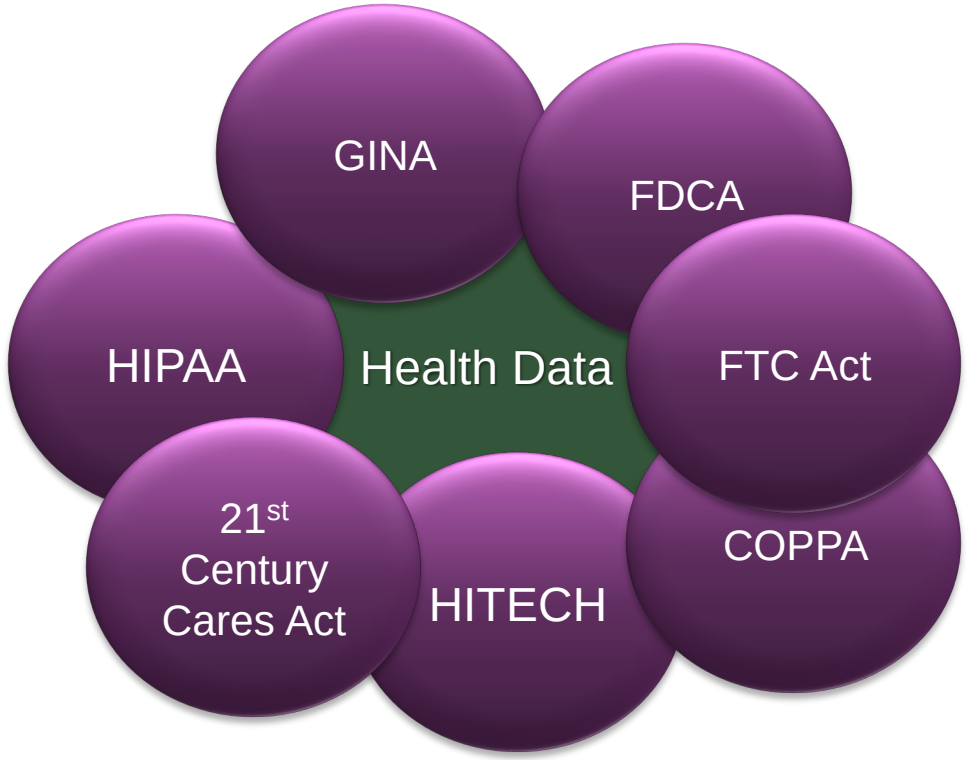
Biometrics

Info revealing health status or history (think geolocation)

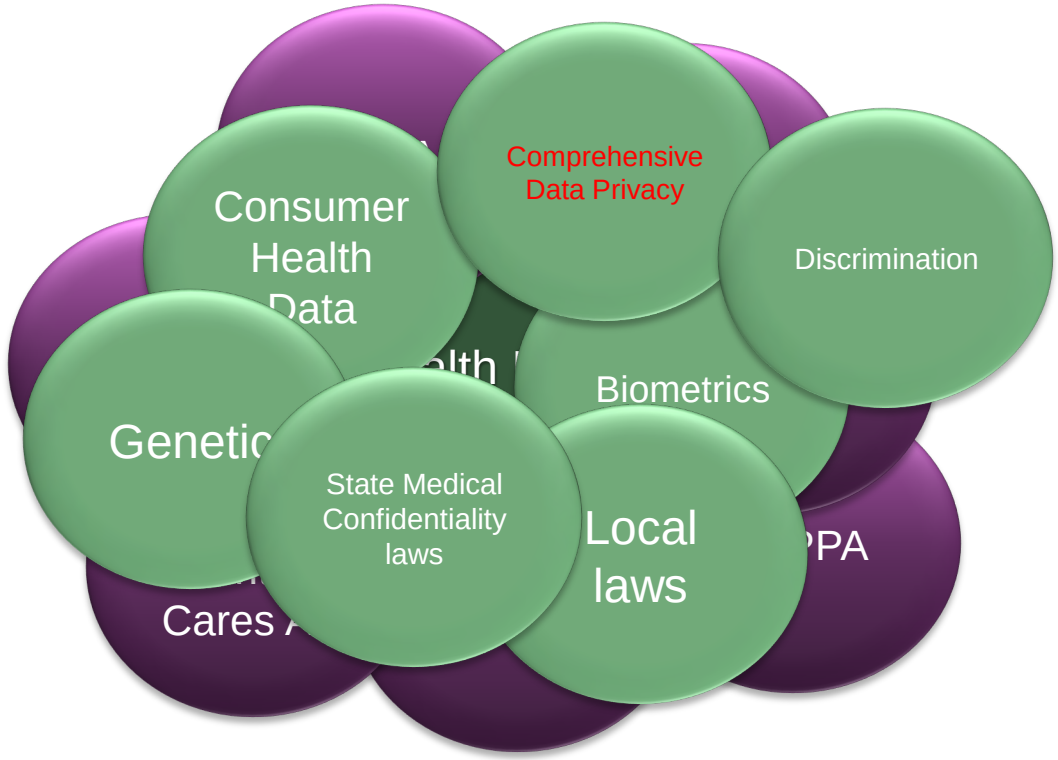
Sensitive Health Indicators

If Health Data was a monolith…

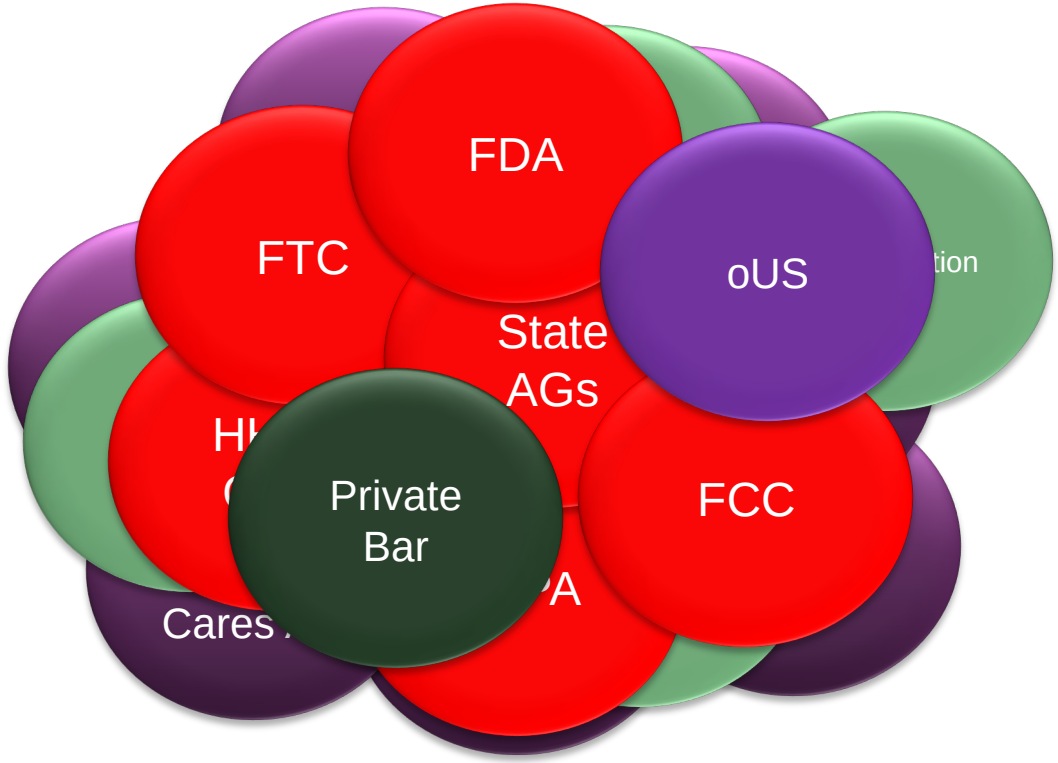
If Health Data was a monolith… FEDERAL LAWS



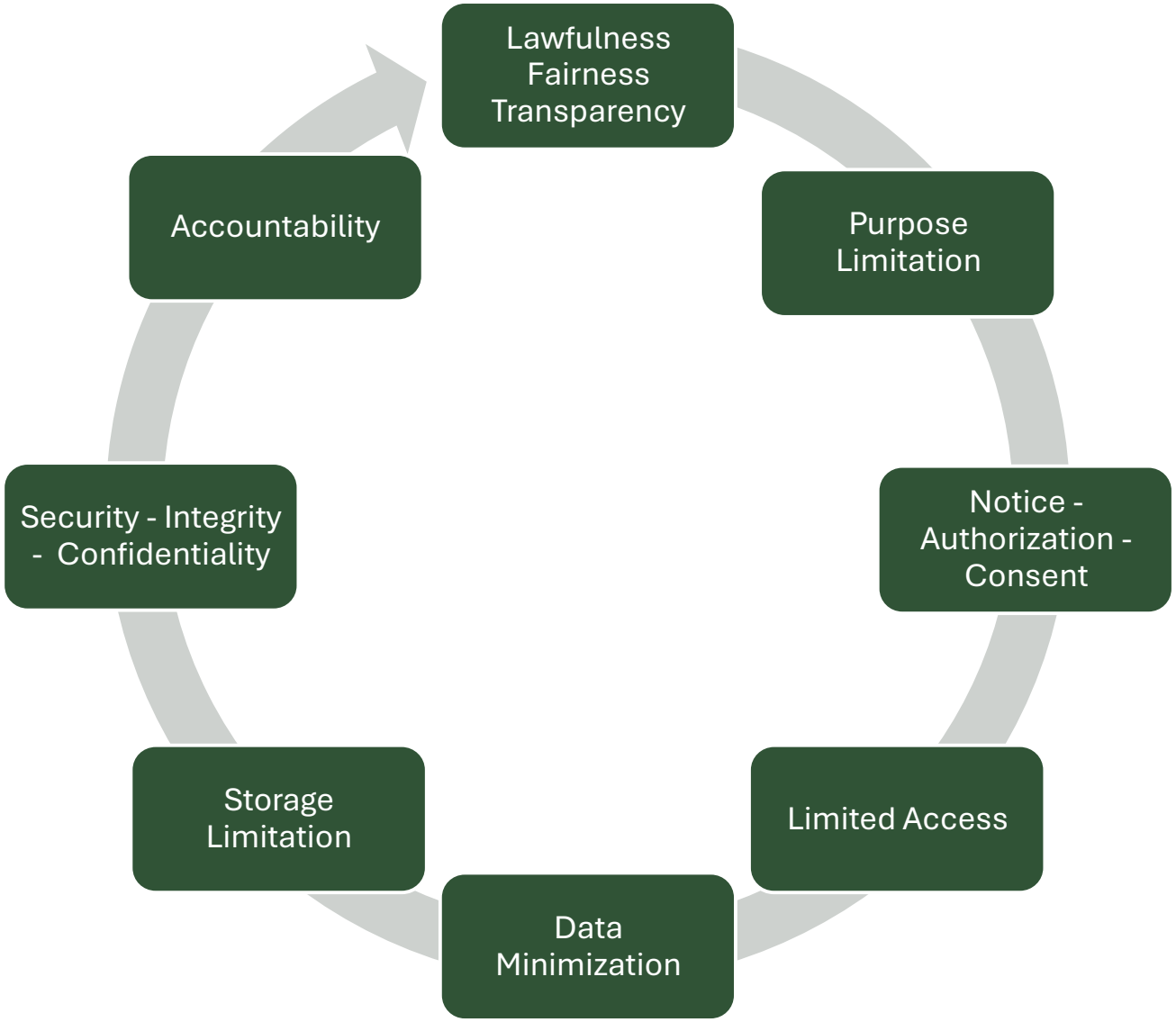
If Health Data was a monolith…STATE LAWS



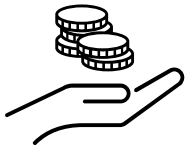
If Health Data was a monolith…
Enforcers & Regulators ++



Principles for Collection & Processing



Hotspots for Personal Data Collection…



Provided Directly

- Directly and voluntarily from the user, with **consent**, when engaging with us or signing up to receive information

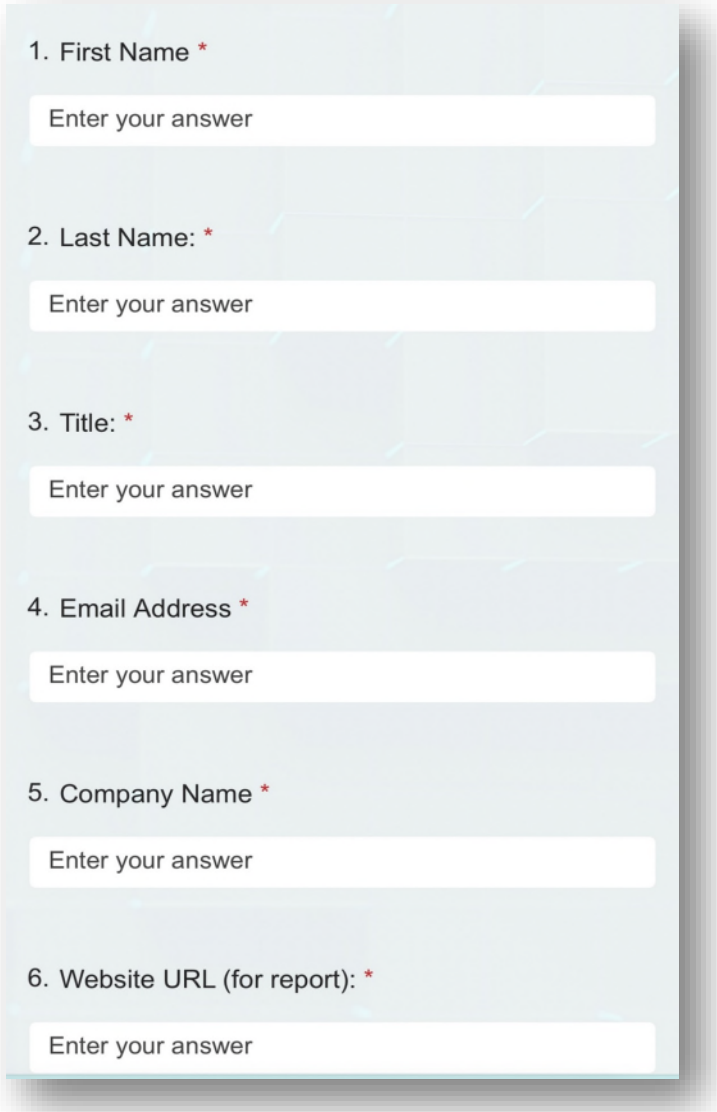
Collected Automatically

- Collected **automatically** by technology when engaging with you online, *e.g.* by way of *cookies* or similar tracking technologies

Third Parties

- Collected from **third parties** acting on our behalf (*e.g.* vendors, co-ops) or publicly available identity sources

Website Tracker Report by Porzio



Domestic Data Privacy Enforcement Building Blocks

‘Comprehensive’ consumer privacy laws + consumer health data laws

Biometric-specific data privacy laws

Federal Agencies enforcing by sector; unfair & deceptive powers; ‘gap fillers’

State Attorneys General; CPPA; HHS/OCR and DOJ enforcements

Class Actions (VPPA / BIPA / wiretap laws, etc)

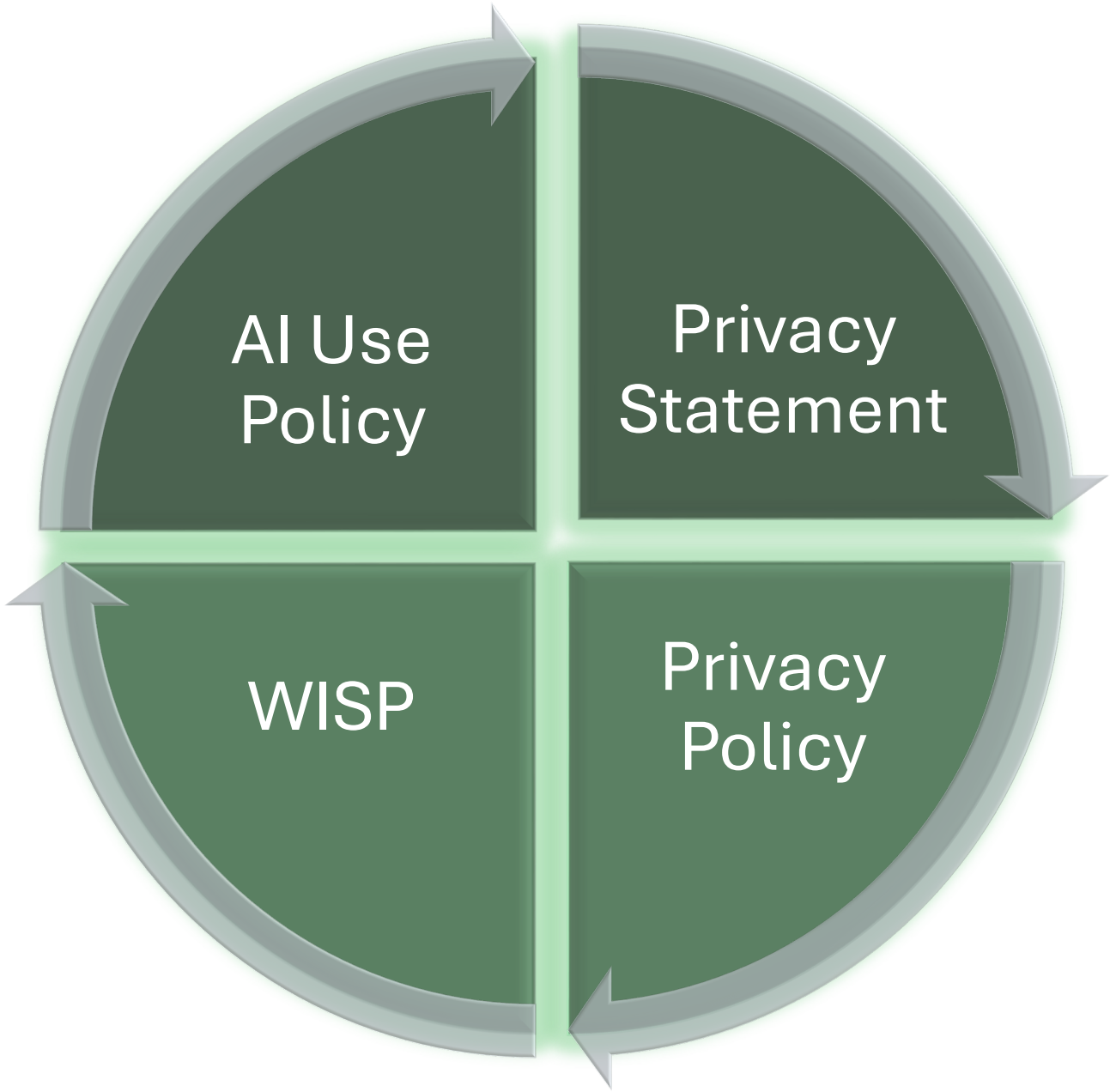
State laws complementary to sectoral federal privacy laws (*e.g.* baby HIPAAs, financial regs, etc)

With Great Data comes Great Responsibility

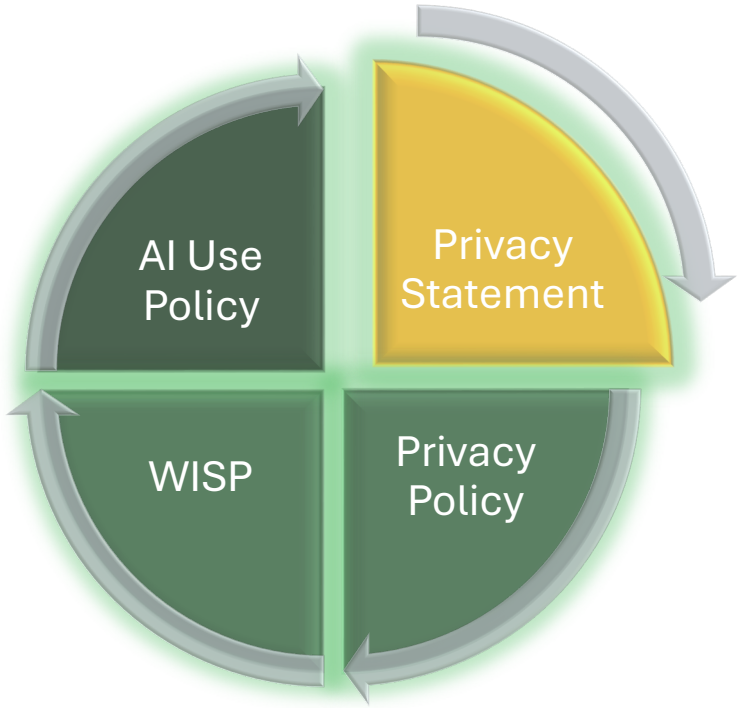
Given the **operational and enforcement landscape**, data privacy is a **top tier concern** when it comes to collecting, using and sharing subject/consumer personal data.

So…what are we to do?

The Foundational Four



Privacy Statement: the external notice



Function:

External transparency-based notice to external individuals (*i.e.* what you tell the World)

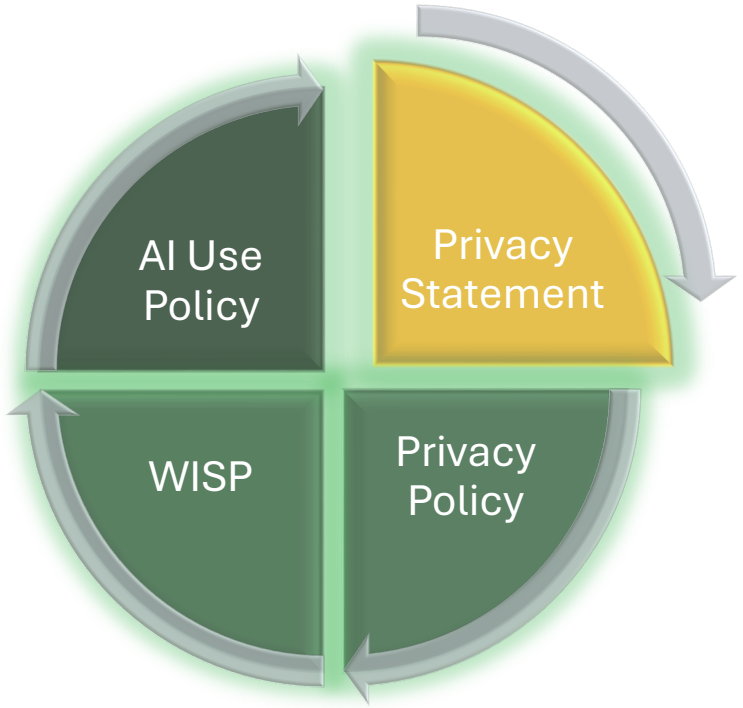
Audience:

- External users
- Customers
- Website/app vistors, etc

How it fits into Governance:

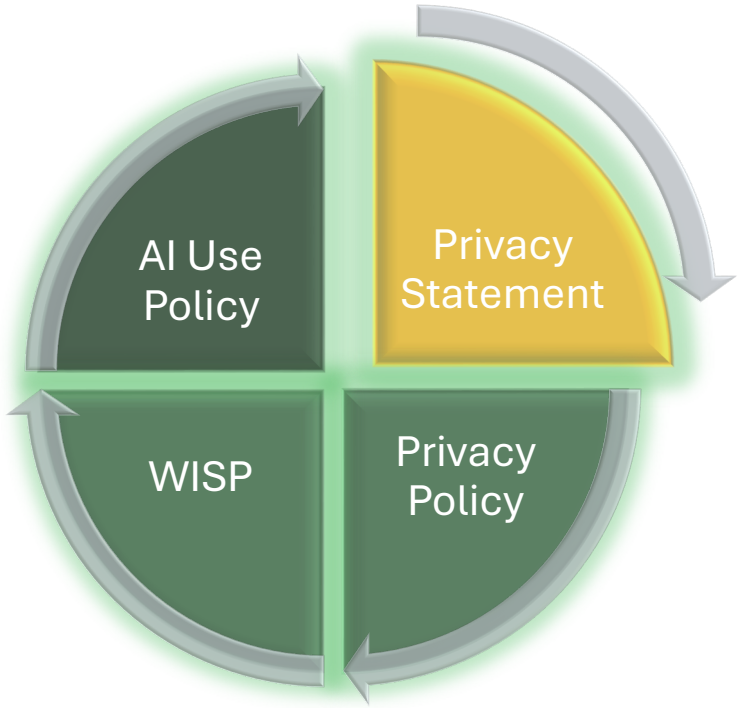
Supports trust by satisfying transparency/notice obligations so long as its accuracy is ensured

Privacy Statement: the elements



- Categories of Personal Data Collected
- Sources of Personal Data
- Business Purpose for Collection & Use
- Categories of Personal Data Disclosed (sold, shared)
- Categories of Third Parties Disclosed to
- Data Minimization & Purpose Limitation
- Retention Periods
- Enumerated Consumer Rights
- Rights & Means to Opt Out
- Accessibility & Format
- Updates
- Notice of Financial Incentive (if any)

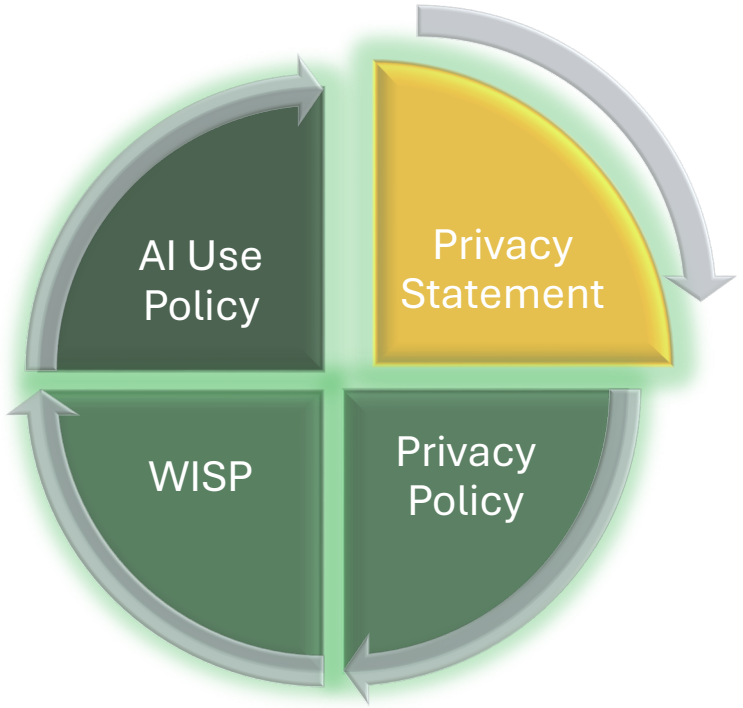
Privacy Statement: the drafting goal…



Artifact Creation

- Beyond simple compliance text, a legal & reputational artifact
- Details matter because Privacy Statements are deficient if too vague or too broad
- Alignment to actual practices is key

Privacy Statement: location in the framework



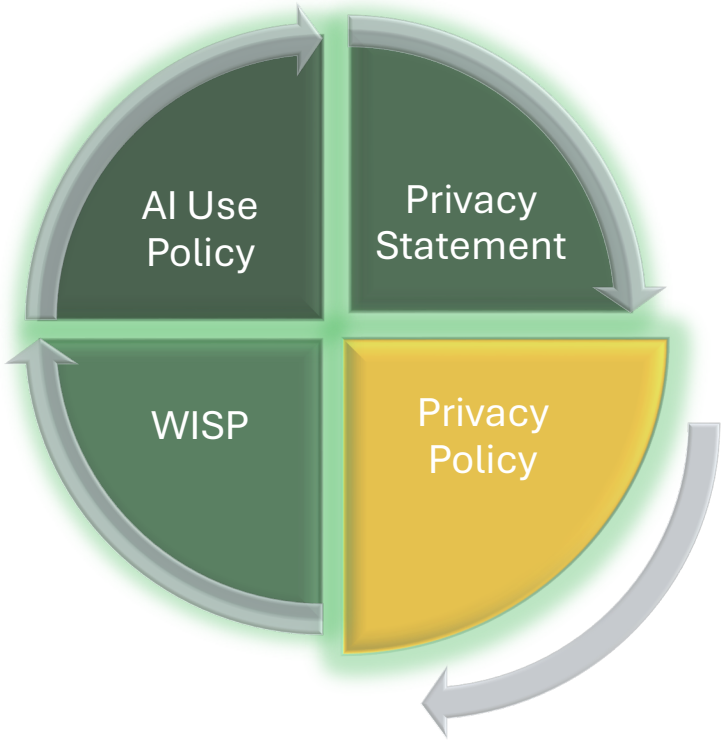
Top Layer of Privacy Program

- Consistency with internal policies and actual procedures & practices is paramount
- Privacy-By-Design begins here
- Risk to credibility, disclosures and liability integrate here

So…what are we to do?

- External Statement

Privacy Policy: how to operate



Function:

Internal operating system for how to handle Personal Data

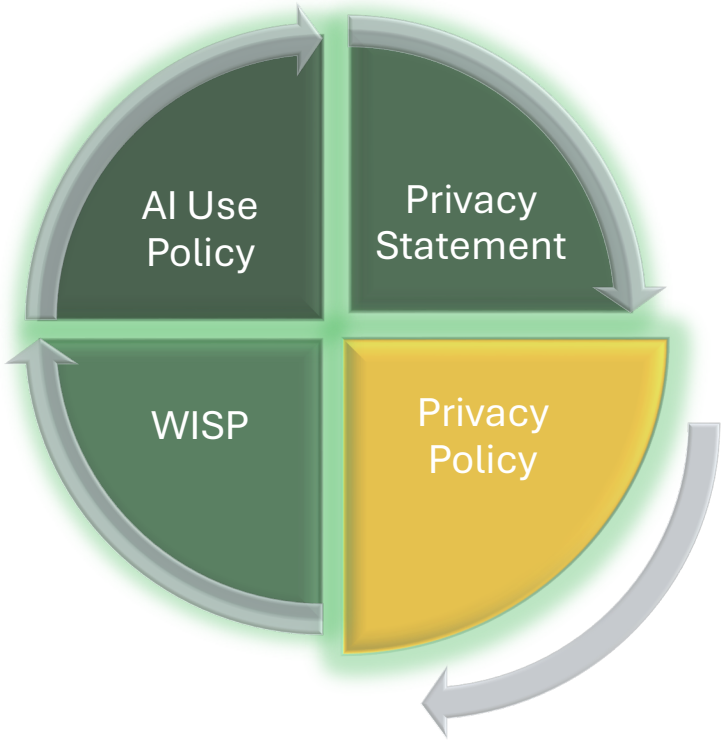
Audience:

- Employees
- Vendors / Service Providers / Contractors,
- internal compliance and business teams

How it fits into Governance:

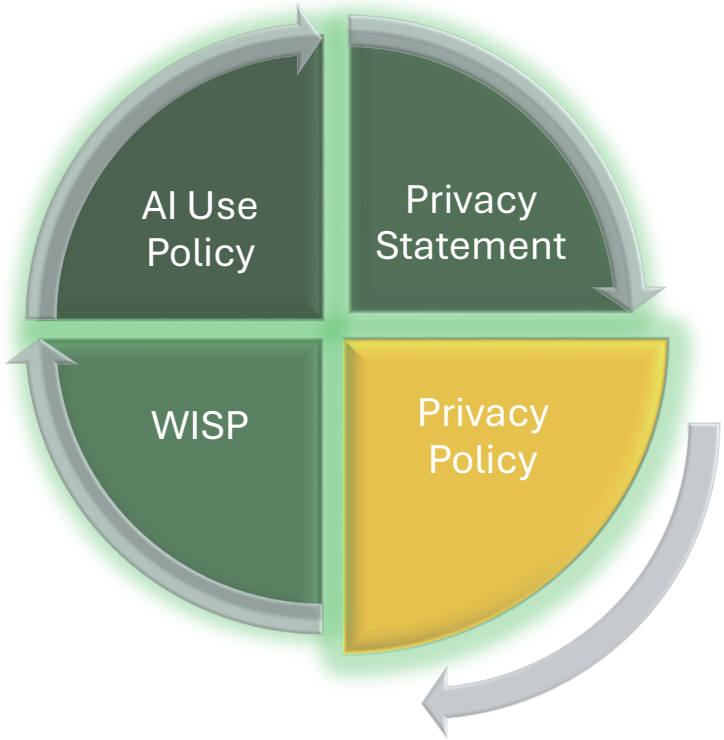
Translates privacy obligations into day-to-day internal conduct and activites

Privacy Policy: the Elements



- Scope & Applicability
- Roles & Responsibilities
- Data Lifecycle Rules
- Legal Bases / Permitted Uses
- Data Subject / Consumer Rights Handling
- Data Minimization & Purpose Limitation
- Vendor / Third-Party Management
- Cross-Border Transfers
- Retention & Deletion
- Incident Response Interface
- Training & Awareness
- Monitoring & Auditing

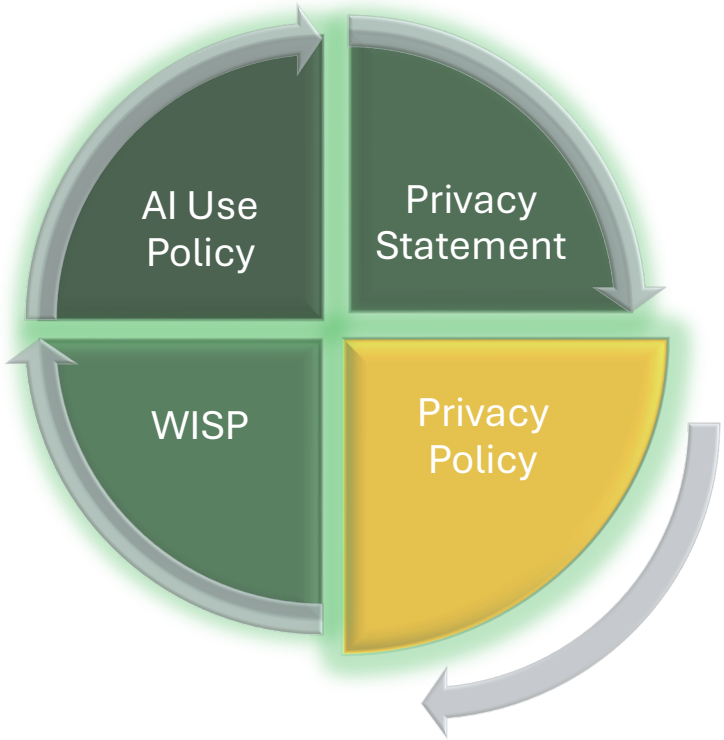
Privacy Policy: the drafting goal…



Operational Clarity

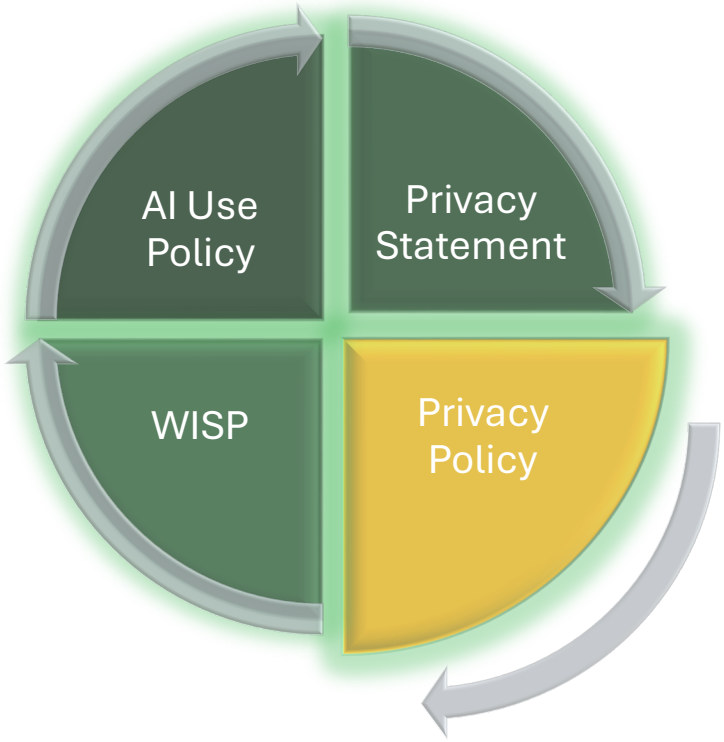
- Erase the gray wherever possible
- Standardize employee behavior
- Create a defensible internal control environment, especially across varied business sectors

Privacy Policy: location in the framework



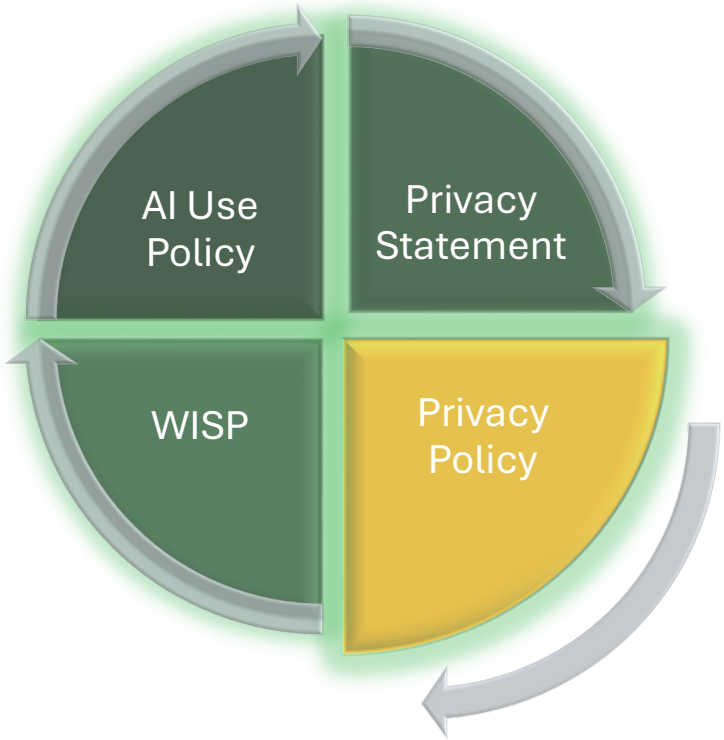
- Lives above SOPS and instructions but below & among enterprise principles (*e.g.* Code of Conduct)
- Bridges legal obligations to operational controls
- Cross reference incident responses, records administration, vendor management and trainings

Privacy Policy: a Risk Mitigator



Risk Type	How it mitigates
Regulatory	Demonstrates accountability and governance structure
Litigation	Shows “reasonable” compliance posture
Reputational	Prevents misalignment between promises and practices
Operational	Reduces inconsistent data handling across business units

Privacy Policy: for next level compliance



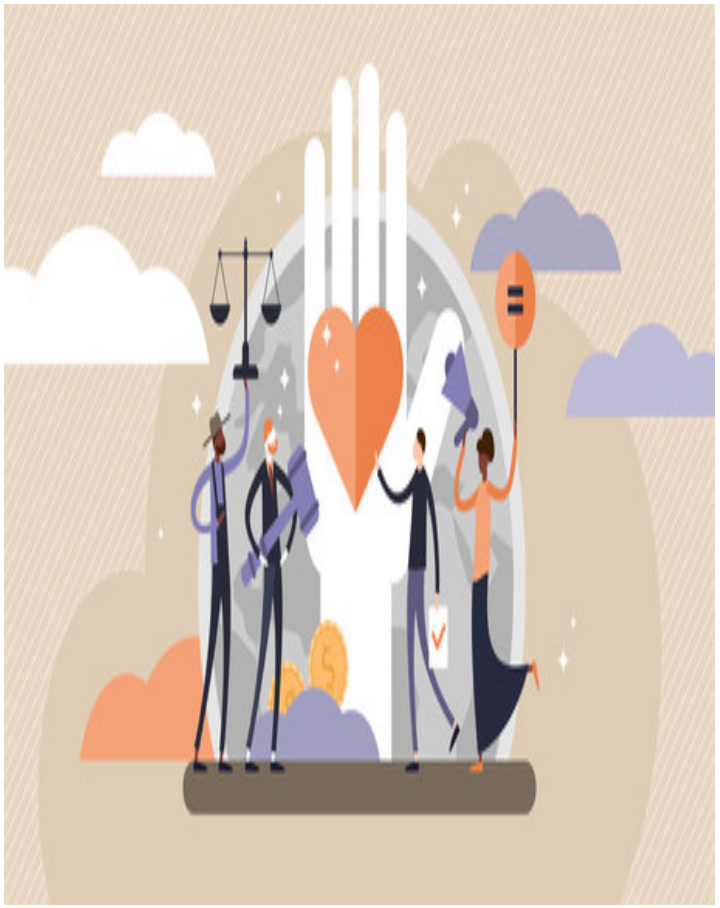
Clear Data Classification framework

Defined Risk Tiers
(by type of processing; by data type)

Link to:

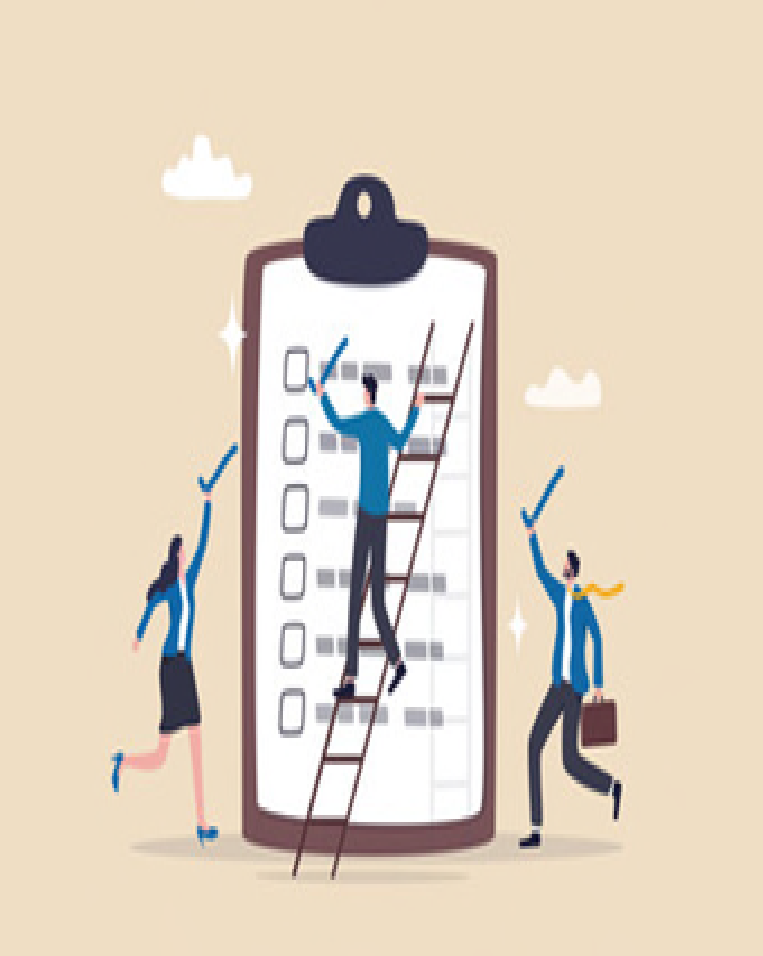
AI Governance
Vendor Risk Management
Automated Workflows, e.g. CRMs, CMPs

Consumer Rights (the most common)



- Access
- Correct
- Delete
- Portability
- Against Automated Decision Making
- Opt Out of certain processing (e.g. sale, profiling, sensitive data)
- To Opt In to Sensitive Data Processing

Business Obligations (the most common)

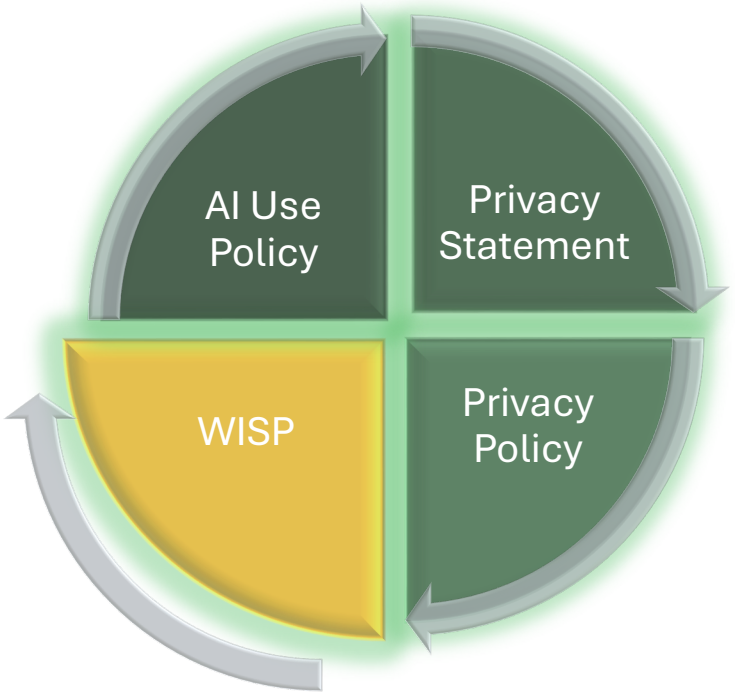


- Notice
- Transparency
- Data Processing Agreements
- Age-related limitations
- No discrimination for exercising data rights
- Processing limited to purpose
- Data Protection (Impact) Assessments

So…what are we to do?

- External Statement
- Internal Privacy OS

WISP: how you actually secure the data



Function:

Data Security Playbook (the Security Governance program, in writing)

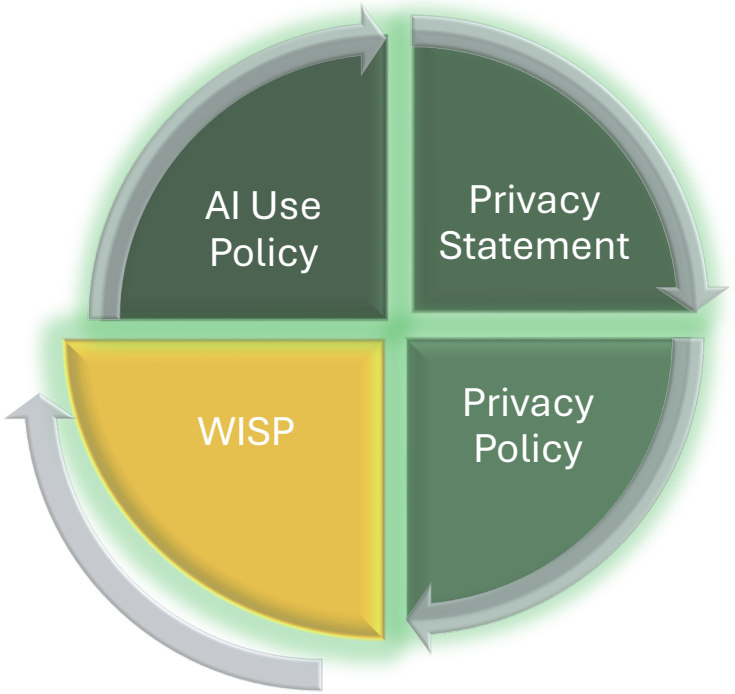
Audience:

- IT; Security; InfoSec
- Legal; Compliance
- Executive Management

How it fits into Governance:

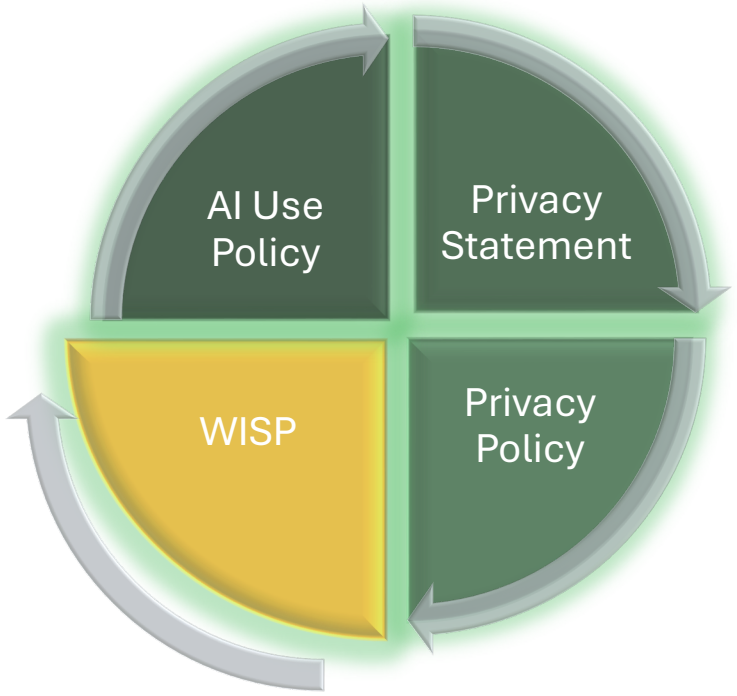
Documented administrative, technical and physical safeguards and monitoring

WISP: the Elements



- Governance & Ownership
- Risk Assessment
- Access Controls
- Data Classification
- Encryption
- Network Security
- Vendor Security
- Incident Response
- Training
- Monitoring & Testing
- Data Retention & Disposal

WISP: how & where it's used



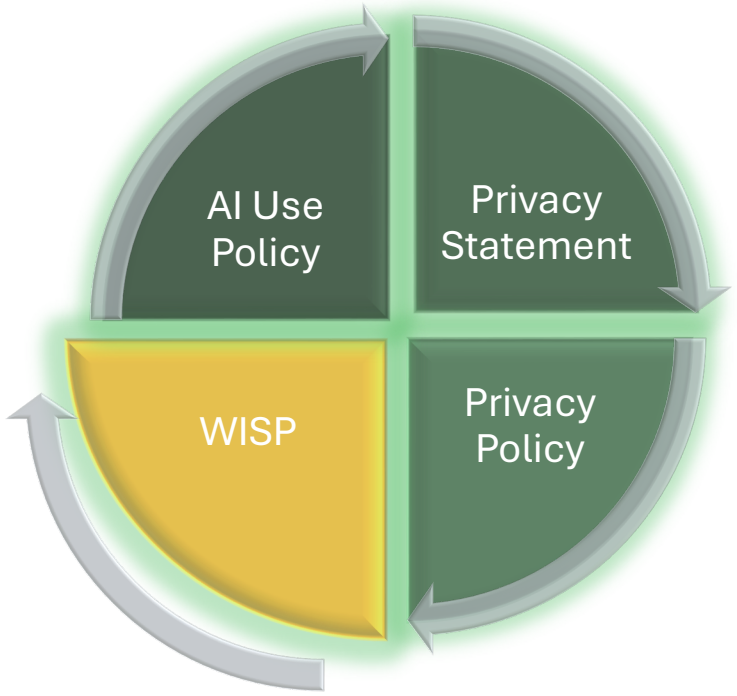
For business operations, it will drive:

- Security practices
- Vendor vetting and onboarding
- Incident response
- Data breach procedure
- Cyberinsurance underwriting
- Regulatory Audits

It will appear in:

- Regulatory/enforcement inquiries
- Client/partner audits
- DPAs

WISP: it needs to be:



REAL

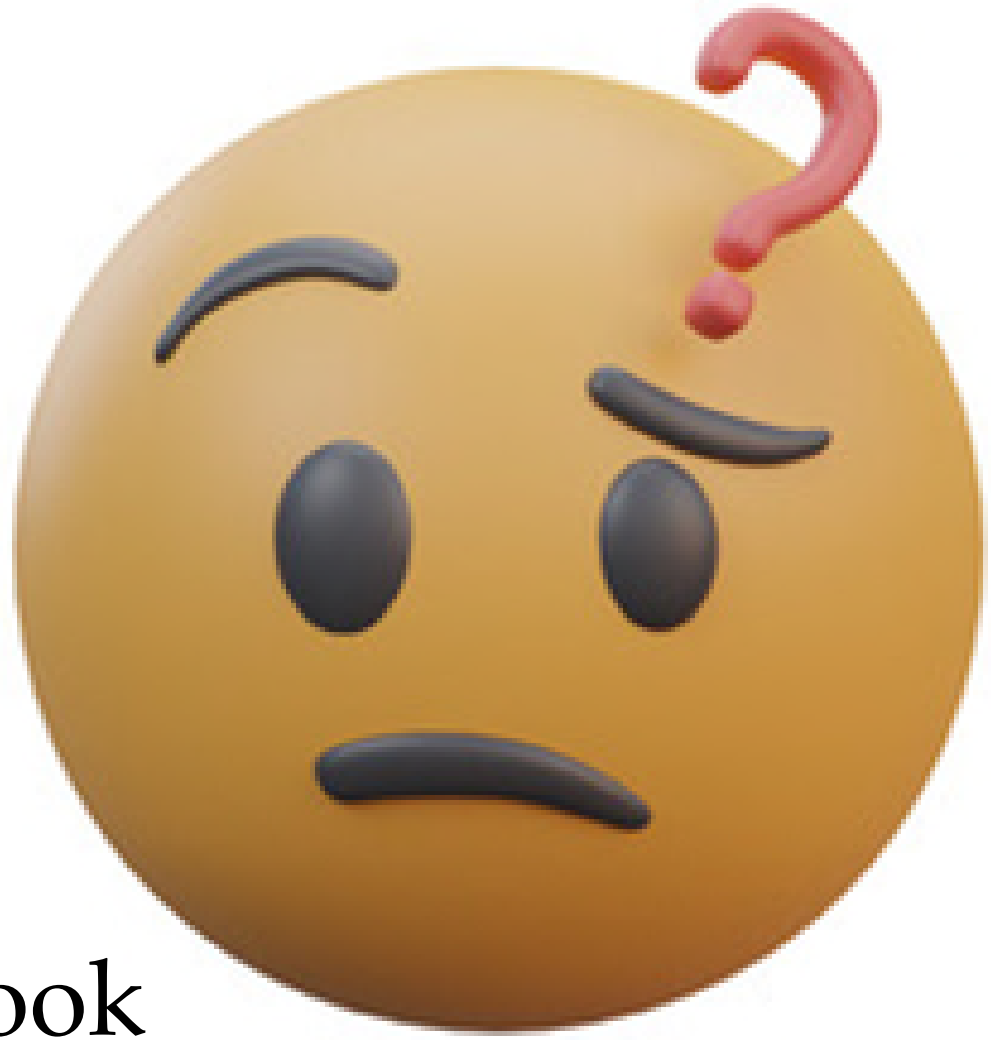
PRACTICAL

SPECIFIC

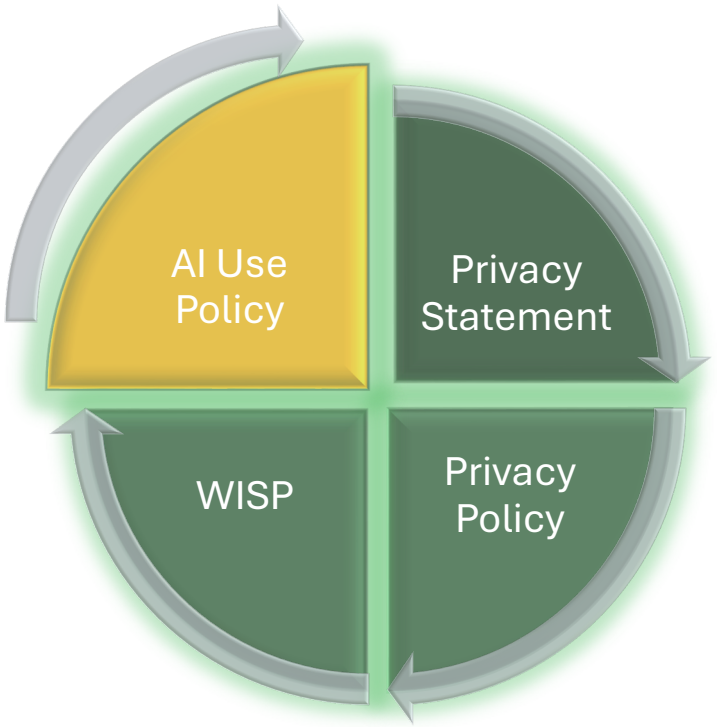
RIGHT-SIZED

So…what are we to do?

- External Statement
- Internal Privacy OS
- Data Security Playbook



AI Use Policy: governing emerging AI



Function:

Rules for permissible use of AI and similarly dynamic technologies

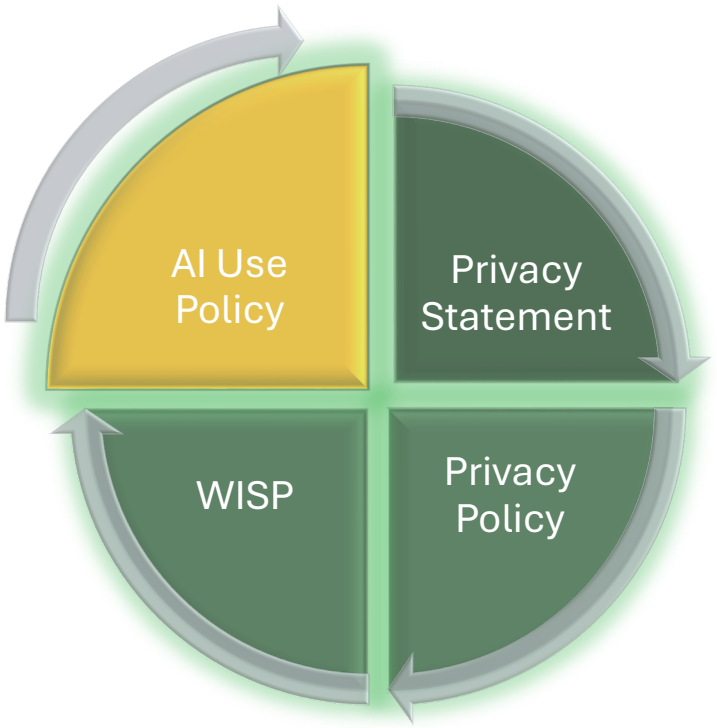
Audience:

- Employees
- Vendors / Service Providers
- Targeted business units with legitimate use cases

How it fits into Governance:

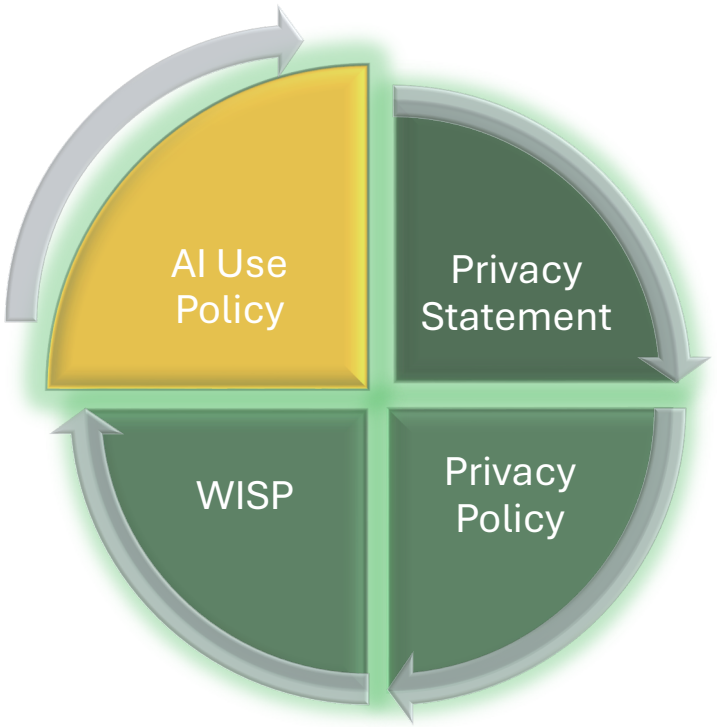
Regulates AI and solution adoption, data leakage, misuse, bias and solidifies accountability

AI Use Policy: the Elements



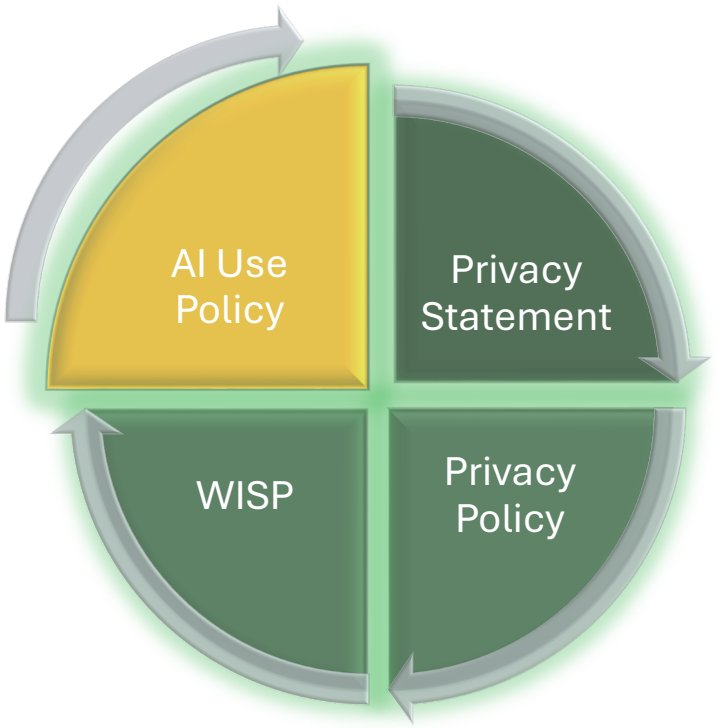
- Scope & Applicability
- Permitted Uses
- Prohibited Uses
- Data Input Restrictions
- Output Validation
- AI Risk Classification
- Vendor / Tool Approval
- Transparency Requirements
- Monitoring & Auditing
- Training

AI Use Policy: location in the framework



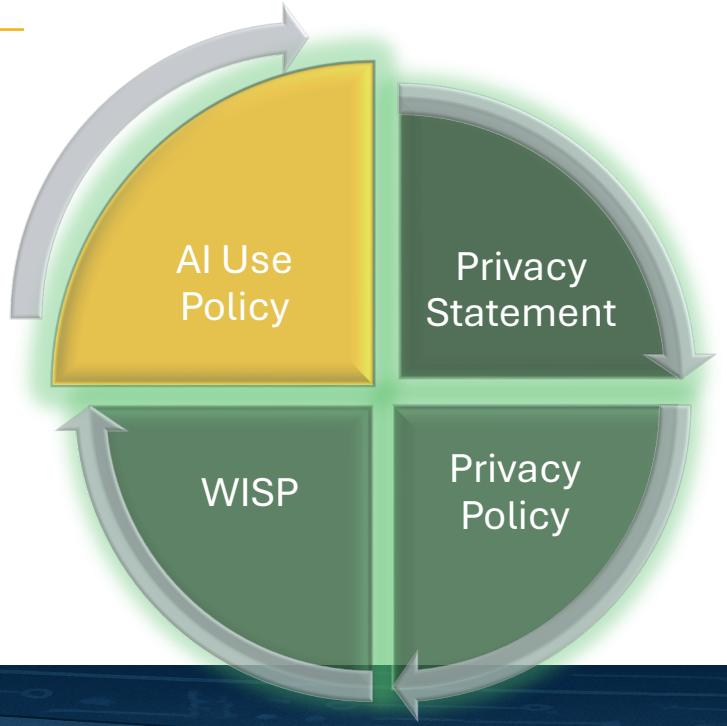
- Lives along side core enterprise policies as a top-tier goveance document
- Operationalize by way of standards, controls and procedures to align with privacy, cybersecurity and risk management architectures

AI Use Policy: the Business Enabler



- Facilitates safe adoption of AI tools and solutions
- Supports innovations without increasing regulatory exposure
- Provides clear rules for employees and vendors
- Accelerates AI deployment by establishing guardrails

AI Use Policy: mitigate growings risks



Hallucinations

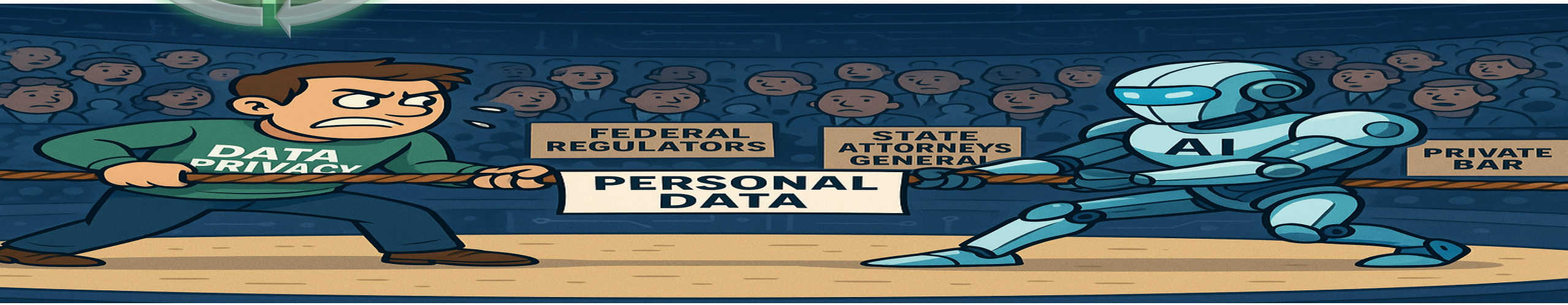
- Inaccuracy incorporated into decision making

Data Leakage

- Confidential, personal information into accessible LLMs

Bias / Discrimination

- Outputs unfair impact on individuals



Before deploying any ADMTs or similar tools:

ASSESS if using ADMT for significant decisions (of consequence)

ANALYZE current privacy processes to determine when & how info processing will be subject to ADMT regulations

MAP out how pre-use notices and individual rights will be addressed

Unified Data Privacy Governance enables…

Global cross-sectoral data sets with accessibility and type controls to manage risk profile

Simplify integration and M&A obligations

Privacy as accelerator of efficiencies, trust and brand equity

Rising consumer and regulator expectations and scrutiny

Unified vendor vetting and employee standards across operating companies

Big Picture

Thoughtful data governance
can protect the privacy of personal data and increase security
to reduce the likelihood of misuse, breach and liability

DO WHAT YOU SAY (concerning data privacy)

SAY WHAT YOU DO (with personal data)

What to look out for:

- Outward facing statements
- Align your representations to your practices
- Vendor, Marketing and Sales Relationships
- Contract Management
- Cross Border Data Flows
- Artificial Intelligence

Questions & Contacts

Scan to Learn More About Porzio's Data Privacy Practice

Alfred R. Brunetti, Esq. CIPP/US, CIPM

Chair - Data Privacy Practice Group