The Evergreen Privacy Program: How to Move Beyond the CCPA and GDPR Compliance Dates and Structure More Everlasting Programs

Privacy+ Security Forum

Speakers

TERESA TROESTER-FALK
Chief Global Privacy Strategist, Facilitator & Speaker
Nymity

RACHEL GLASSER
Chief Privacy Officer
Wunderman

BRITTANIE HALL
Senior Associate
Hogan Lovells, Privacy and CyberSecurity

Takeaways

- Identify the privacy initiatives that will lay the groundwork for ongoing compliance
- Leverage existing privacy law initiatives and project workstreams into sustainable business processes by finding a home for those workstreams in a privacy management accountability framework
- Learn how to effectively report on key compliance requirements so that you can communicate with key stakeholders and are “regulator-ready”

Agenda

- The state of the States
- What is an “evergreen” privacy program
- Panel Discussion
- Case Study – turning a privacy compliance initiative into a sustainable business process
- Questions

CCPA OVERVIEW

Main Individual Rights

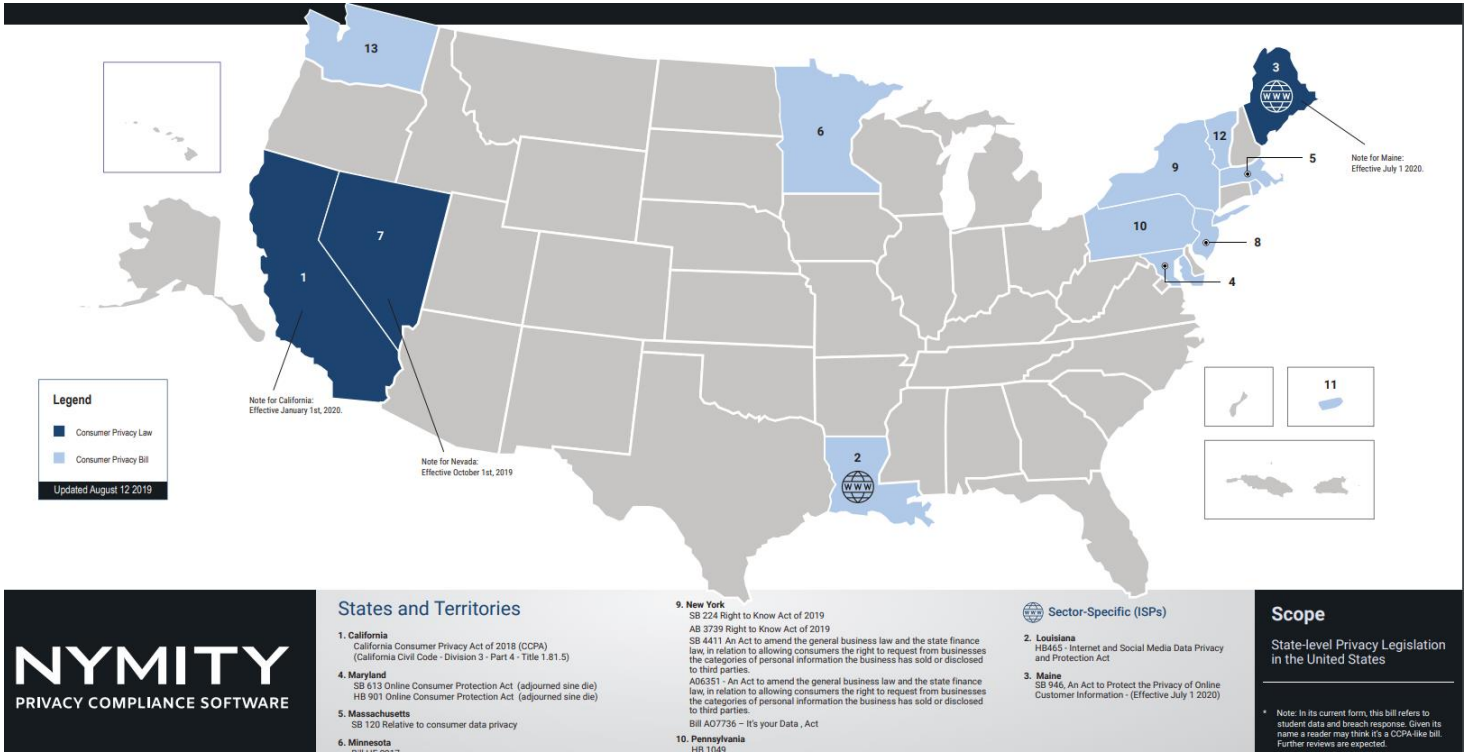
1. **RIGHT TO KNOW**
2. **RIGHT OF DELETION**
3. **RIGHT TO OPT-OUT FROM SALE**
4. **RIGHT TO NO DISCRIMINATION**
5. **PRIVATE RIGHT OF ACTION (breaches)**

Rights mainly apply to data collected in the 12 months preceding the request and can be exercised free of charge.

CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

- Applies in the **State of California** and to organizations doing business there
- Legislation focuses on **data subject rights**
- Rights only extended to **California residents**
- Will apply as of 1 January 2020

Thinking Ahead – California is Not the Only Law



The US Consumer Privacy Laws and Bills

Parallels

"DO NOT SELL" PERSONAL INFORMATION

- **Individual can request information about data sales**
- Individual has the right to opt-out of data sales
- **Organization has the obligation to display opt-out link or button**

GDPR AND CCPA-LIKE RIGHTS & OBLIGATIONS

- **Individual has the right of access to his/her data**
- Individual can request correction or deletion of data

STRONG ENFORCEMENT

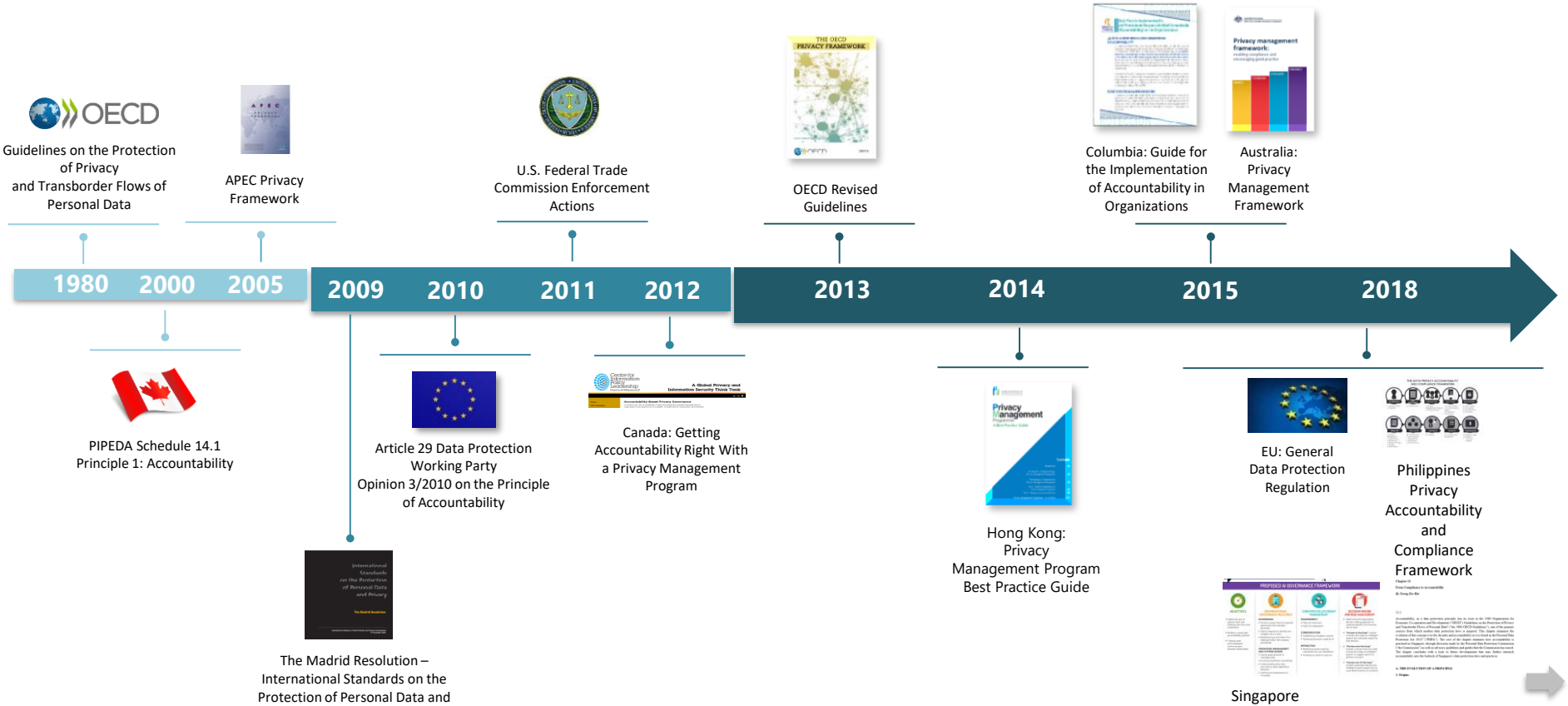
- **Attorneys-General in charge of enforcement**
- Possibility to impose penalties or hold organizations liable

EQUAL TREATMENT

- **Prohibition to discriminate** against consumers exercising their rights

ACCOUNTABILITY VS. COMPLIANCE

Development of Accountability as a Privacy and Data Protection Principle



Operationalizing Accountability

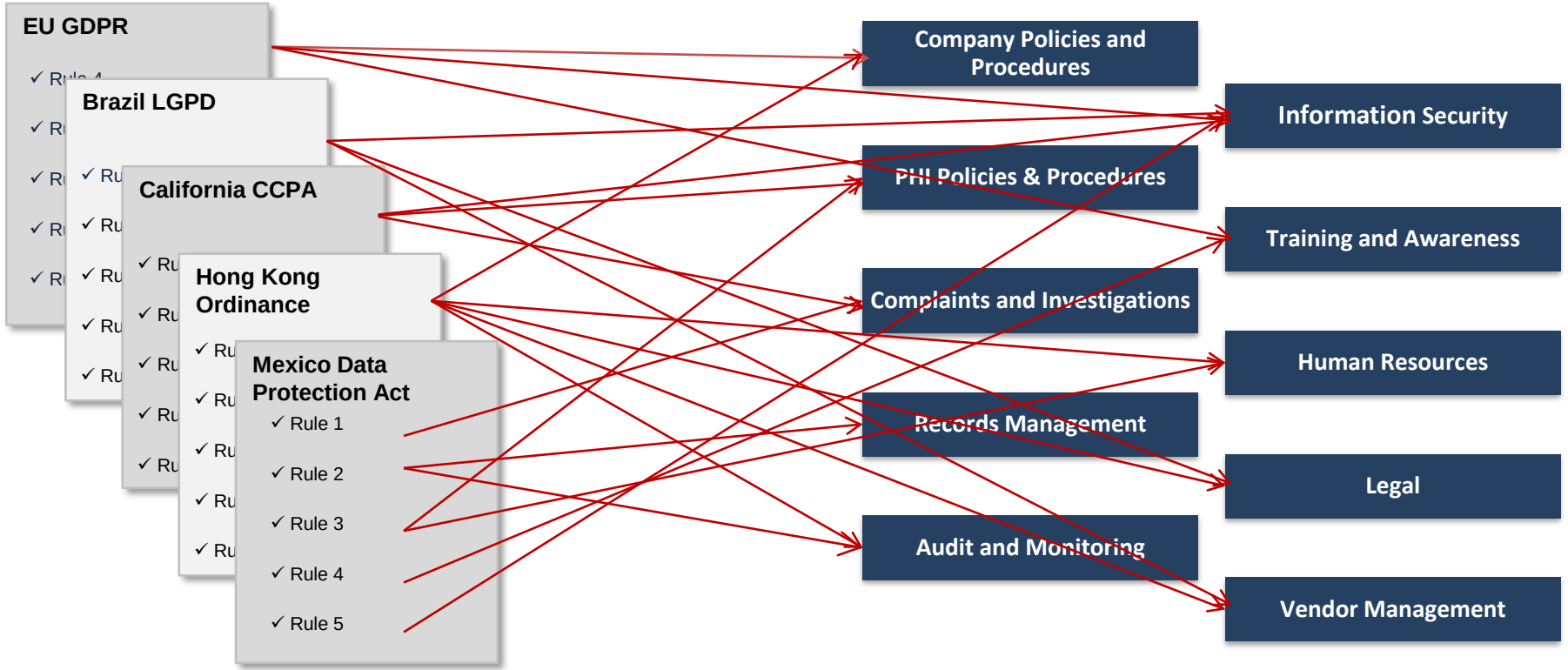
A proven method for putting in place appropriate technical and organisational measures and demonstrating compliance

Accountability is embedding ongoing technical and organisational measures throughout the organisation, resulting in the ability to demonstrate accountability and compliance with evidence.

RESPONSIBILITY	Appropriate Technical and organisational measures have been identified and are implemented and maintained on an ongoing basis
OWNERSHIP	An individual (or function or business unit) is answerable for the management and monitoring of technical and organizational measures
EVIDENCE	Documentation is produced as a result of implementing technical or organisational measure and that can be used as Evidence of accountability and compliance (board reporting, regulators)

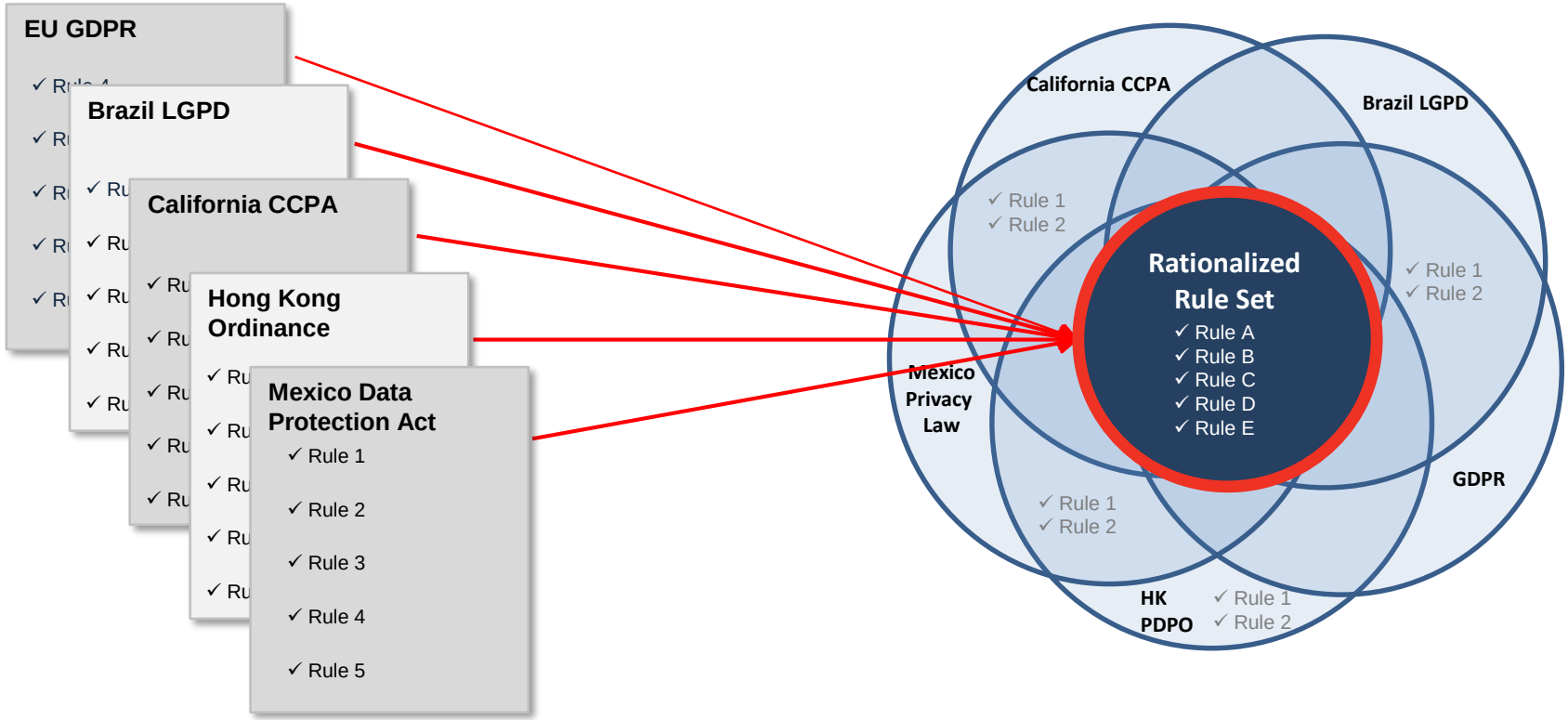
Traditional Compliance Assessment Approach

Many Regulatory Requirements → to → **Many** Privacy Programs & Activities



Traditional Compliance Assessment Approach

Many Regulatory Requirements → to → **Many** Privacy Programs & Activities



Accountability Based Approach

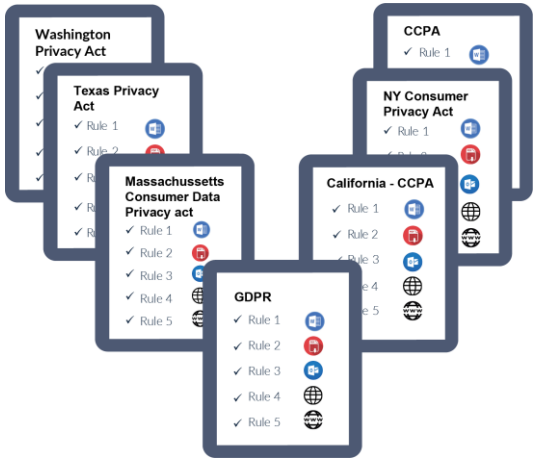
Leverage existing activities to comply with many laws and evidence of accountability to demonstrate compliance

ONE ACCOUNTABLE PRIVACY PROGRAM

Responsibility
Ownership
Evidence

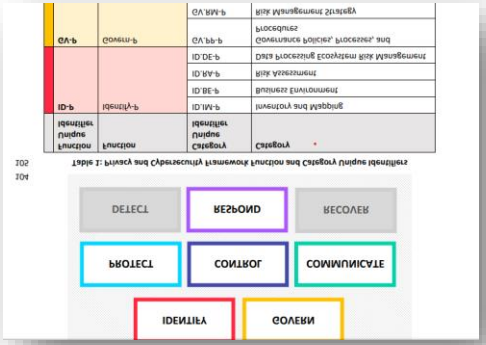
Evidence of accountability is mapped to requirements, allowing the organization to demonstrate compliance with laws and regulations on-demand, supported by evidence.

MANY REGULATORY REQUIREMENTS

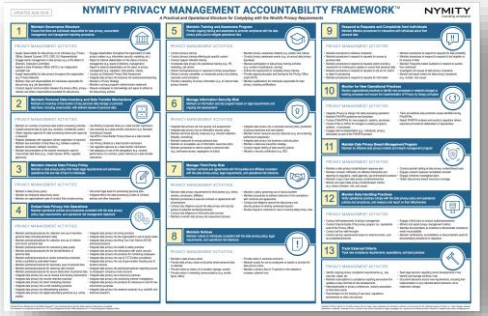


Responsible Measures (policies, procedures, processes)	GDPR	CCPA	Nevada
Maintain procedures to respond to requests for access to personal data	✓	✓	
Maintain procedures to respond opt-out of, restrict or object to processing	✓	✓	✓
Maintain procedures to respond to requests for data portability	✓	✓	
Maintain procedures to respond to requests to be forgotten or for erasure of data	✓	✓	
Provide data privacy notice at all point where personal data is collected	✓	✓	✓
Maintain technical security measures	✓		
Maintain a data privacy incident/response plan	✓		

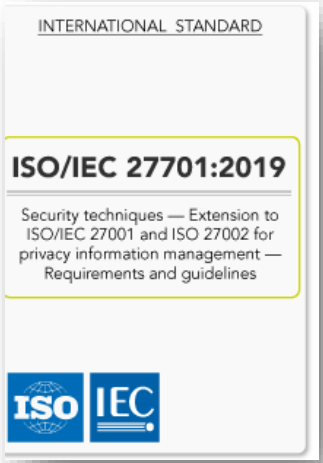
Privacy Frameworks



NIST Privacy Framework



Nymity Privacy Management Accountability Framework



ISO/IEC 27701: 2019

Extension to ISP 27001 for privacy information management

PANEL DISCUSSION

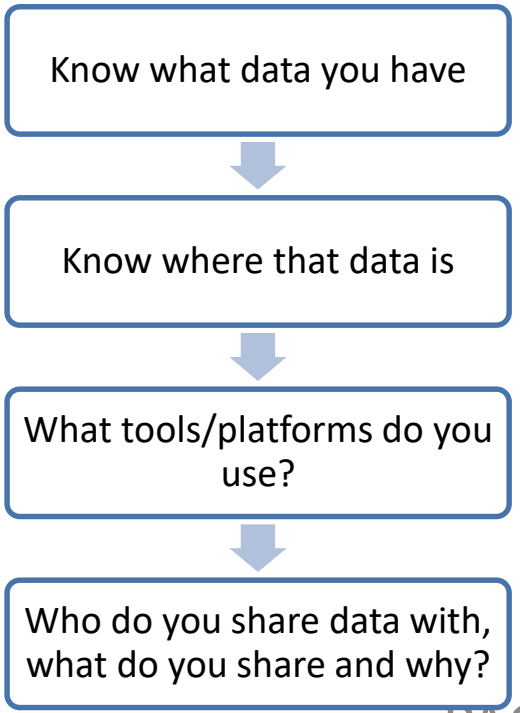
THE EVERGREEN PRIVACY PROGRAM

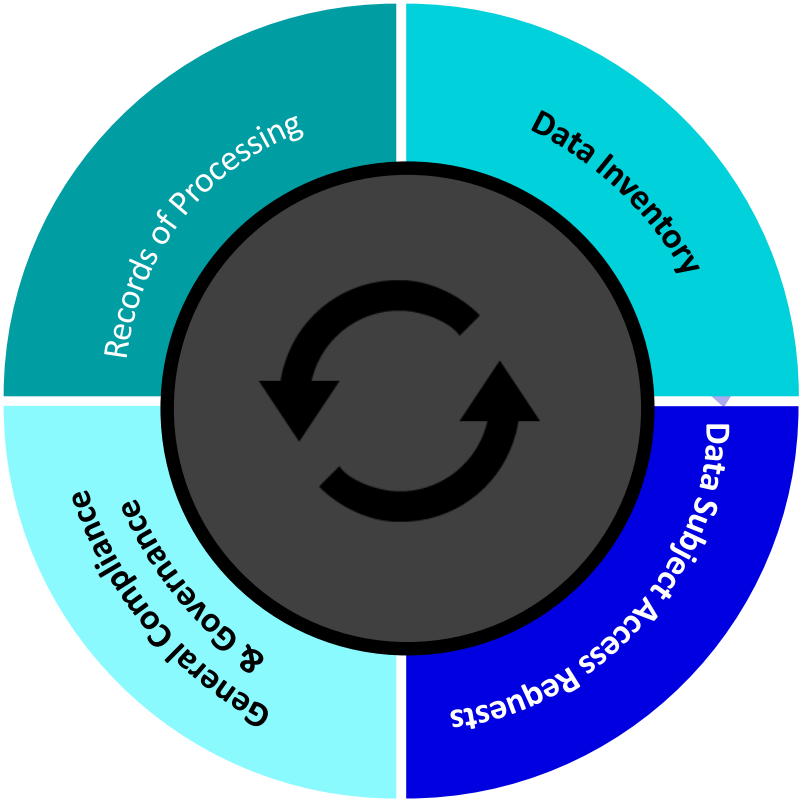

CarWash
ALL EMPLOYEES
TRAINED BY
MR MIYAGI

START WITH BEST PRACTICES

- Transparency
- Data quality
- Collection limitation
- Use limitation
- Accountability
- Individual participation

+ BUILD INTO EVERYDAY PROCESSES





The Evergreen Privacy Program

ABC Co.

Record of Personal Information and Required Categories

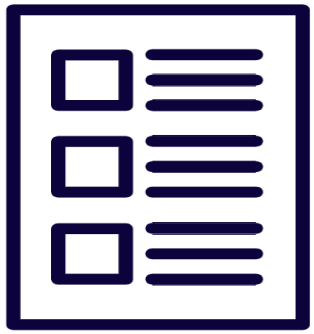
Business function	Purpose of processing	Categories of Consumers	Categories of personal information	Types of personal information collected e.g name, address, IP address, demographic data, age, gender,shopping preferences	Sensitive Data	Categories of sources from which personal information is collected	Categories of third parties to whom personal information was sold	Categories of third parties to whom information was disclosed for a business purpose	Retention schedule (if possible)	General description of technical and organisational security measures (if possible)
Human Resources	Personnel file	Employees	Contact details	name, address	N	employees	N/A	Service Providers	6 years post-employment	Encrypted storage
Human Resources	Personnel file	Employees	Pay details	account number	Y - Bank account details	employees	N/A	Service Providers	6 years post-employment	Encrypted storage, access controls
Human Resources	Recruitment	Successful candidates	Qualifications	name, address, email address	N	employees	N/A	Service Providers	6 years post-employment	Encrypted storage, access controls
Human Resources	Recruitment	Successful candidates	Employment history		N	employees	N/A	Service Providers	6 years	Encrypted storage, access controls
Sales	Direct marketing	Existing customers	Identifiers	name, address, email address, IP address, age,	N	Data Compiling companies Online and mobile websites and apps	Advertising/Marketing Companies, Apparel & Accessory Companies, Automotive Companies....	N/A	End of customer relationship	Encrypted storage and transfer
Sales	Direct marketing	Existing customers	Transactions Information	total annual purchase of women's apparel	N	Apparel and Accessory Companies, Consumer Survey Companies, Electronic Companies	N/A	N/A	End of customer relationship	Encrypted storage and transfer
Sales	Direct marketing	Potential customers	Demographic	age, gender, marital status	N	Data Compiling companies	N/A	N/A	1 year post-campaign	Encrypted storage and transfer
Sales	Direct marketing	Potential customers	Inferences	Marketing segments: high income earner, outdoor enthusiast, pets, hatchback cars, right-wing politics	Maybe - includes data elements race, ethnicity, political affiliation	Data Compling companies	Advertising/Marketing Companies, Apparel & Accessory Companies, Automotive Companies....	N/A	1 year post-campaign	Encrypted storage and transfer
Sales	Direct marketing	Potential customers	Internet or other electronic network activity information	browsing history, online interests	N	Online and mobile websites and apps	Advertising/Marketing Companies, Apparel & Accessory Companies, Automotive Companies	N/A		

Demonstrating Compliance – Regulator and Audit Ready

How will we demonstrate compliance?

Request No.	Date of Request	How the Request was Made	Identity of applicant verified	Status	Employee Assigned	Nature of the Request	Search for Records (where, when and by who)	Request was granted (how, date)	Request was denied (reasons, legal provision, date)	Data Subject Communication Sent	Statement outlining disagreement or complaint	Final Outcome

Electronic file for every request with the evidence



Upon request, write a formal report

Questions and Contact

TERESA TROESTER-FALK
Chief Global Privacy Strategist, Facilitator & Speaker
Nymity

RACHEL GLASSER
Chief Privacy Officer
Wunderman

BRITTANIE HALL
Senior Associate
Hogan Lovells, Privacy and CyberSecurity