SCCE™
Society of Corporate Compliance and Ethics

Privacy Trends in the US and Implications for US and Global Organizations

September 15, 18th Annual CEI
National Harbor, MD

1

Speaker

TERESA TROESTER-FALK

President/Founder, BlueSky Privacy
Chief Global Privacy Strategist, Nymity

Disclaimer: The handouts for this presentation were prepared and used to accompany this session. Neither the information contained herein or the accompanying comments of the presenter should be construed as the provision of legal advice. Views expressed are those of the specific presenter.

2

Outline

01
Baselining: What is Privacy?

02
Update on the State of US Consumer Privacy Laws and Bills

03
Understanding Trends and Themes

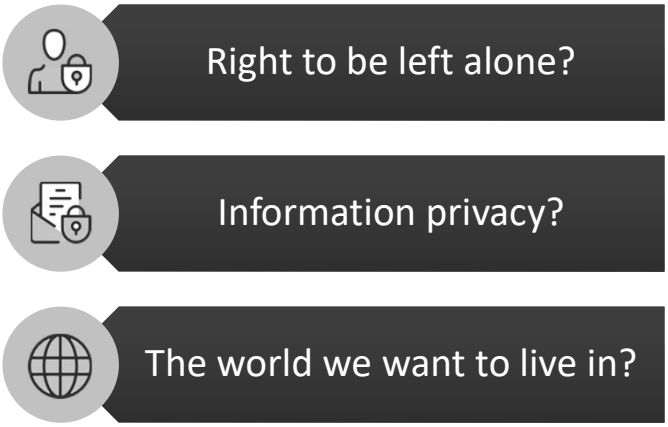
04
How to "Future-Proof" Your Privacy Compliance Initiatives

3

What is Privacy?

4

Baselining: How Do We Define Privacy?



5

Compliance, Privacy and Security

Compliance	Data (Information) Privacy	Data Security
A systematic approach to governance designed to ensure that an organization meets its obligations under applicable laws, regulations, best practices, contracts, and internal policies.	Generally focused on the use and governance of PII. Organizations must implement policies to ensure that personal information is being collected, shared, and used in appropriate ways.	Focuses on protecting data (PII, confidential information, etc.) from impermissible access, including intentional malicious attacks. Organizations maintain the privacy of their data by having security protocols in place to prevent against external threats and data breaches.

6

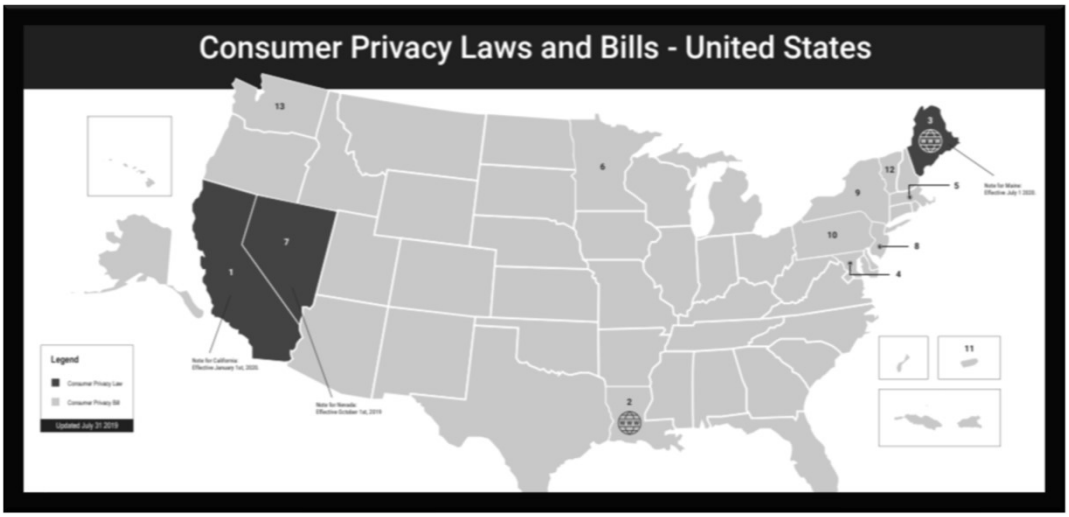
The US Consumer Privacy Laws and Bills

Overview of existing and pending legislation and requirements

7

The US Consumer Privacy Laws and Bills

Pending and Adopted Legislation



8

California Consumer Privacy Act - Overview

- Stated to go into effect January 1, 2020
- Set to be one of the toughest privacy laws in the US
  - New states already passing similar bills
- Broadly expands the rights of consumers
  - Requires in scope businesses to be more transparent about collection, use, disclosure and sale of personal information
- May be a motivating event for businesses to enhance data privacy management practices
- For companies subject to GDPR, ability to leverage GDPR initiatives to address operational needs

Who must comply?

- Any business worldwide doing business in California;
- exceeding thresholds of:
  A. annual gross revenues of $25 million;
  B. personal information of 50,000 or more California residents, households, or devices annually; or
  C. 50% or more annual revenue from selling California residents' personal information.
- Parent companies and subsidiaries sharing the same branding, even if they themselves do not exceed the applicable thresholds

Who must comply? Key Definitions

Personal Information

- Any information associated with, relating to, or capable of being associated with, or that could reasonably be linked, directly or indirectly, with a particular consumer or household.
- *See § 1798.140(o).*

Consumer

- A natural person who is a California resident.
- *See § 1798.140(g).*

Sale

- Selling, renting, releasing, disclosing, transferring, making available, or otherwise communicating a consumer's personal information to another business or a third party for monetary or other valuable consideration.
- *See § 1798.140(t).*

11

Who Must Comply? Key Definitions

Business

- Any for-profit entity that collects personal information, determines the purposes and means of processing that information, does business in California, and meets at least one threshold related to revenue or volume of personal information collection; and
- Any entity that controls, or is controlled by, a qualifying business if it shares common branding.
- *See § 1798.140(c).*

Service Provider

- Any for-profit entity that: (1) processes personal information on behalf of a business (2) pursuant to a written contract that prohibits the service provider from retaining, using, and disclosing personal information other than for the specific purpose of performing the service specified in the contract or as CCPA otherwise allows.
- *See § 1798.140(v).*

Third Party

- Defined in the negative to include any person other than: (1) the business that collects consumer personal information; or (2) a person who receives personal information from a business pursuant to certain contractual limitations (similar to restrictions imposed on service providers).
- *See § 1798.140(w).*

12

Main Individual Rights

1. **RIGHT OF ACCESS**
2. **RIGHT OF DELETION**
3. **RIGHT TO DATA PORTIBILITY**
4. **RIGHT TO INFORMATION ON DATA SELLING**
5. **RIGHT TO OPT-OUT OF DATA SELLING**
   6. **DO NOT SELL BUTTON/LINK**
7. **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; changes to the body of law still possible

How to comply?

Update Privacy Policies:

- Provide at or before collection: categories of personal information (PI) to be collected and underlying purposes (information may be provided elsewhere)
- Separate lists of categories of PI collected, sold or disclosed for a business purpose in the preceding 12 months (explicitly state if not sold or disclosed)
- Categories of sources of PI collected
- Business/commercial purposes for collecting or selling PI

How to comply?

Update Privacy Policies to Include:

- Categories of third parties receiving PI
- Description of the rights to access, deletion, to obtain information about disclosures, to opt out of sales, and not to be discriminated against
- If PI is sold: Fact that PI collected may be sold and clear and conspicuous link, titled "Do Not Sell My Personal Information", to webpage that enables opt-out
- Method(s) for submitting requests including, at a minimum, toll-free telephone number and, where maintained by the business, website address

15

How to comply?

A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:

a) Denying goods or services to the consumer.
b) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.
c) Providing a different level or quality of goods or services to the consumer, if the consumer exercises the consumer's rights under this title.
d) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

16

How to comply?

Access, Deletion rights: Implement processes and policies to

- verify the identity of individuals making requests
- timely provide portable copies
- delete personal information or claim statutory exception

(1)Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.
(2)Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.
(3)Debug to identify and repair errors that impair existing intended functionality.
(4)Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law.
(5)Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.
(6)Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.
(7)To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.
(8) Comply with a legal obligation.
(9)Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

- obtain assistance of service providers

17

Bill	Summary	Subject	Latest Bill Version	Lead Authors	Status	Last History Action
AB-25	Excludes employment information from definition of "consumer."	California Consumer Privacy Act of 2018.	Amended Senate 6/28/2019.	Chau	Senate: In committee process - Appropriations.	7/10/2019 – From committee: Amend, and do pass as amended and re-refer to Committee on Appropriations. (Ayes 8. Noes 0.) (July 9).
AB-846	Clarifies nondiscrimination provision as it applies to loyalty programs.	Customer loyalty programs.	Amended Assembly 5/20/2019.	Burke, Low, Mullin	Senate: In committee process - Appropriations.	6/6/2019 - Referred to Committee on Judiciary.
AB-873	Amends the definition of "deidentified"; removes "household" from definition of "personal information" and revises to mean "reasonably linkable" to a consumer.	California Consumer Privacy Act of 2018.	Amended Assembly 5/02/2019.	Irwin	Senate: In committee process – Judiciary.	7/9/2019 - In committee: Set, first hearing. Failed passage. Reconsideration granted.
AB-874	Excludes "publicly available information" from the definition of "personal information," and clarifies that deidentified or aggregate information is "not personal information."	California Consumer Privacy Act of 2018.	Amended Assembly 3/25/2019.	Irwin	Senate: In committee process – Appropriations.	7/10/2019 - From committee: Do pass and re-refer to Committee on Appropriations with recommendation: To Consent Calendar. (Ayes 8. Noes 0.) (July 9). Re-referred to Committee on Appropriations.
AB-1138	Requires verifiable parental consent that complies with Children's Online Privacy Protection Act to create a social media or app account.	Social media: the Parent's Accountability and Child Protection Act.	Amended Assembly 5/13/2019.	Gallagher	Senate: In committee process - Appropriations.	7/10/2019 - From committee: Amend, and do pass as amended. (Ayes 8. Noes 0.) (July 9).
AB-1146	Exempts vehicle and ownership data for purpose of vehicle repair relating to a warranty or recall.	California Consumer Privacy Act of 2018: exemptions – vehicle information.	Amended Senate 6/28/2019.	Berman	Senate: In committee process - Appropriations.	7/10/2019 - From committee: Do pass and re-refer to Committee on Appropriations. (Ayes 8. Noes 0.) (July 9). Re-referred to Committee on Appropriations.

18

Bill	Summary	Subject	Latest Bill Version	Lead Authors	Status	Last History Action
AB-1202	Creates "data broker" registry with the California attorney general.	Privacy: data brokers.	Amended Senate 6/28/2019.	Chau	Senate: In committee process - Appropriations.	7/5/2019 - Read second time and amended. Re-referred to Committee on Appropriations.
AB-1281	Require a business in California to disclose use of facial-recognition technology in a physical sign that is clear and conspicuous at the entrance of every location.	Privacy: facial-recognition technology – disclosure.	Amended Senate 7/5/2019.	Chau	Senate: In committee process - Appropriations.	7/5/2019 - Read second time and amended. Re-referred to Committee on Appropriations.
AB-1355	Allows for differential treatment of a consumer reasonably related to the value of the consumer's information to the business, and requires a business make disclosures regarding a consumer's rights.	Personal information.	Amended Assembly 4/12/2019.	Chau	Senate: In committee process - Appropriations.	7/10/2019 - From committee: Do pass and re-refer to Committee on Appropriations with recommendation: To Consent Calendar. (Ayes 8. Noes 0.) (July 9). Re-referred to Committee on Appropriations.
AB-1564	Modifies the methods that a business make available to consumers to submit requests.	Consumer privacy: consumer request for disclosure methods.	Amended Senate 6/14/2019.	Berman	Senate: In committee process - Appropriations.	5/22/2019 - From committee: Amend, and do pass as amended and re-refer to Committee on Appropriations (Ayes 8. Noes 0.) (July 9).

19

Nevada

Main Individual Rights

1. **RIGHT TO OPT-OUT OF DATA SELLING**
2. **DO NOT SELL BUTTON/LINK**

Amends an existing online privacy notice law and is significantly narrower than the CCPA.

Sale of data more narrowly defined: exchanging personal information specifically for monetary consideration and for onward licensing or sale.

ACT RELATING TO INTERNET PRIVACY

- Applies to "operators" ($\neq business$)
- Defines consumer in more limited way
- Does not extend to household information
- Legislation focuses on **sale of data**
- Rights only extended to **Nevada residents**
- Will apply as of 1 October 2019

20

The US Consumer Privacy Laws and Bills

Pending and Adopted Legislation

- California
- Louisiana
- Maine
- Maryland
- Massachusetts
- Minnesota
- Nevada
- New Jersey
- New York
- Pennsylvania
- Puerto Rico
- Vermont
- Washington

21

Understanding Trends and Themes

22

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

23

The US Consumer Privacy Laws and Bills

Differences

SCOPE OF APPLICATION

- **Significant differences between jurisdictions**
- Depending on annual gross revenue, number of consumers, etc.
- **Covered data: e.g. employee data, healthcare data not consistently covered**

PRIVATE RIGHT OF ACTION

- **Only included in some of the bills, unlike CCPA or GDPR**
- Notable examples are Louisiana, Maryland, Massachusetts, New York, Pennsylvania, Puerto Rico and Washington

ACCOUNTABILITY

- **Significant differences between jurisdictions on requirements to be able to demonstrate compliance**

24

The US Consumer Privacy Laws and Bills

Outliers

Maine

Maine - SB946 (law)
(Providers of broadband Internet access services)

Louisiana

Louisiana - HB465 (bill)
(Providers of broadband Internet access services)

Puerto Rico

Puerto Rico bill assigns the responsibility for enforcement to the Secretary of Consumer Affairs.

Washington

State of Washington bill includes limits to the use of facial recognition: meaningful human review, consent, court order needed when surveilling specific individuals.

It follows the more extensive structure of the GDPR and includes definitions of sensitive data, controller and data subjects and requires transparency.

Unlikely to be discussed before 2020.

25

Federal Law

?

26

How to Future-Proof Your Privacy Compliance Initiatives: Is It Time to Invest in a Privacy Program?

27

The Need for a Privacy Program

Main Reasons

HIGHER VOLUME & CONTINUOUSLY CHANGING LEGAL REQUIREMENTS

INCREASED PUBLIC AWARENESS

INCREASED ENFORCEMENT

ACCOUNTABILITY

28

29

Accountability

- Globally recognized as a key building block for privacy and data protection regulation
- Gives effect to legal requirements and data privacy laws
- Delivers corporate digital responsibility for the 21st century and modern, data-driven economies

30

What must organizations do to be "accountable"?

Accountability requires organizations to:

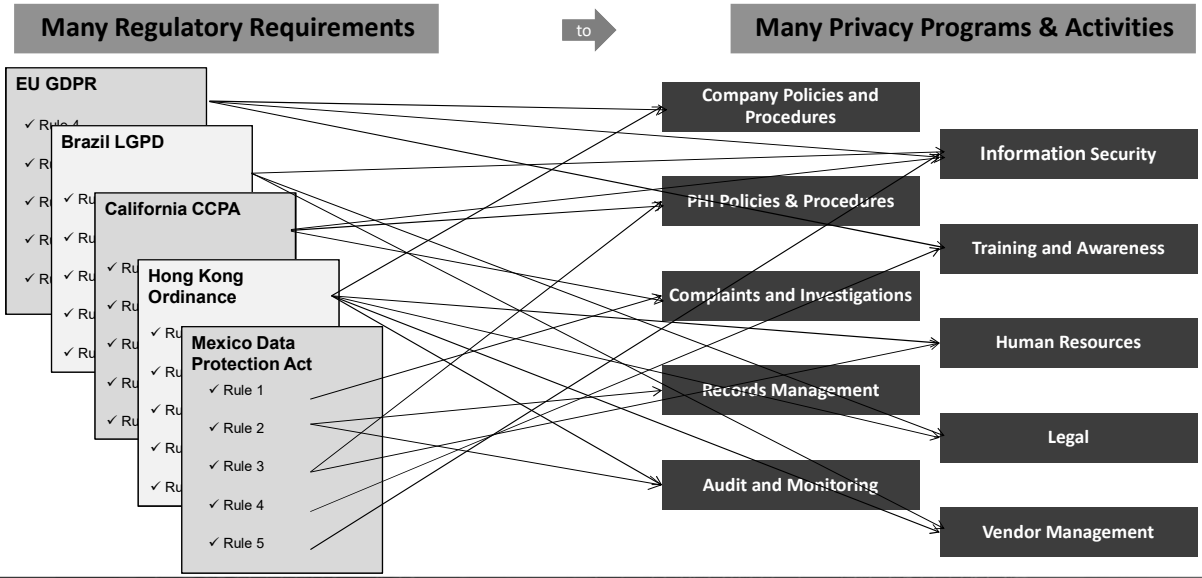
- Implement within the company a comprehensive privacy program covering all core elements of accountability that enables compliance with applicable laws, regulations or industry standards
- Verify the effectiveness and delivery of such a privacy program and ensure continuous improvement
- Be able to demonstrate the existence and effectiveness of such a program internally (to Board and senior level management) and externally on request (to regulators, business partners and individuals)

31

Core Components

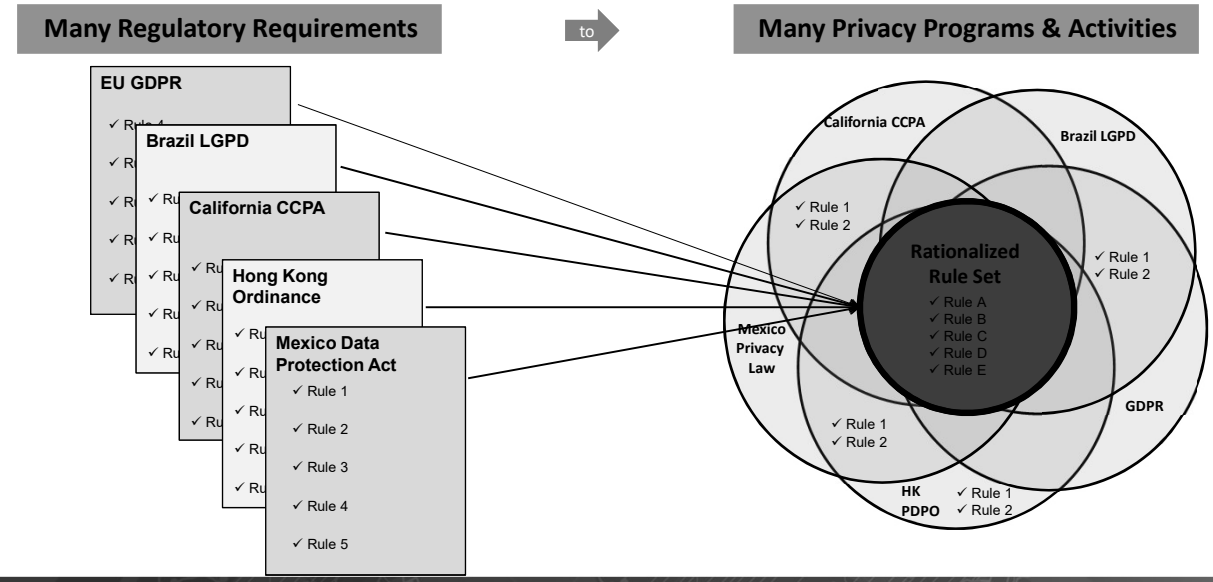
32

Traditional Compliance Assessment Approach



33

Traditional Compliance Assessment Approach



34

Accountability Based Approach

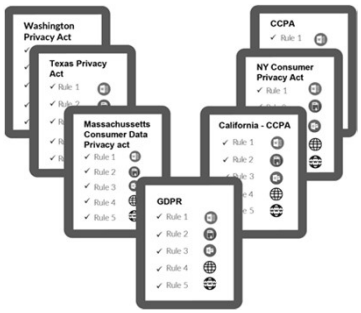
Leverage existing activities to comply with many laws and evidence of accountability to demonstrate compliance

ONE ACCOUNTABLE PRIVACY PROGRAM

Evidence of Privacy Management Activities exists throughout the organization (within the privacy program as well as operations). Evidence is collected in centralized repository, structured in a line with the Privacy Management "categories."

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



35

Accountability Approach to Compliance with Multiple Laws

ACCOUNTABILITY

Privacy Programme
Infrastructure

- ✓ Responsibility
- ✓ Ownership
- ✓ Evidence

How does the organization comply?

CAPACITY TO COMPLY

Privacy Programme
Outcomes

- ✓ Laws and regulations (LGPD, GDPR, California CCPA and 800 other privacy laws and regulations!)
- ✓ Regulator Guidance
- ✓ Enforcement Actions
- ✓ Codes

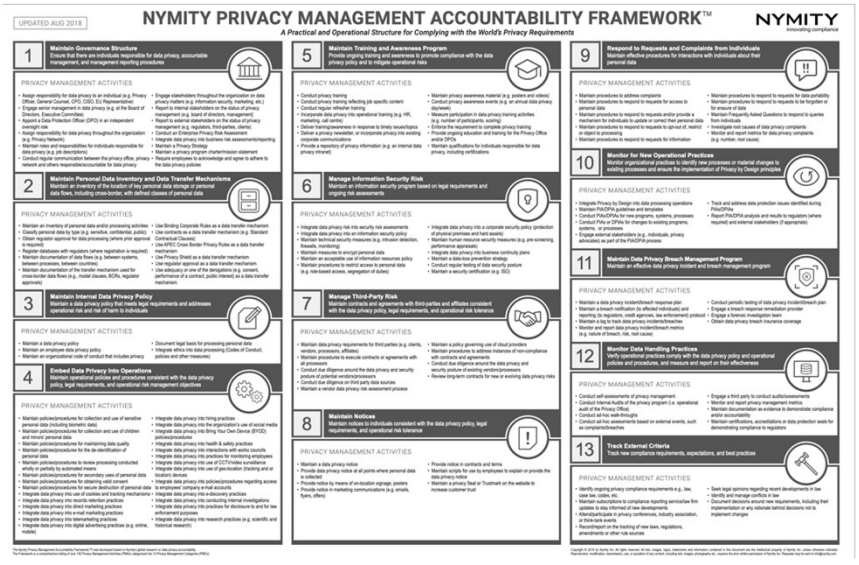
Can the organization demonstrate a capacity to comply?

36

Privacy Frameworks

37

Nymity Privacy Management Accountability Framework



NYMITY PRIVACY MANAGEMENT ACCOUNTABILITY FRAMEWORK™

NYMITY

A Practical and Operational Structure for Complying with the World's Privacy Requirements

UPDATED AUG 2018

1 Maintain Governance Structure
Ensure that there are individuals responsible for data privacy, accountable management, and management reporting procedures

PRIVACY MANAGEMENT ACTIVITIES

- Assign responsibility for data privacy to an individual (e.g. Privacy Officer, General Counsel, CPO, CSO, EU Representative)
- Engage senior management in data privacy (e.g. at the Board of Directors, Executive Committee)
- Appoint a Data Protection Officer (DPO) in an independent oversight role
- Assign responsibility for data privacy throughout the organization (e.g. Privacy Network)
- Maintain roles and responsibilities for individuals responsible for data privacy (e.g. job descriptions)
- Conduct regular communication between the privacy office, privacy network and others responsible/accountable for data privacy
- Engage stakeholders throughout the organization on data privacy matters (e.g. information security, marketing, etc.)
- Report to internal stakeholders on the status of privacy management (e.g. board of directors, management)
- Report to external stakeholders on the status of privacy management (e.g. regulators, third-parties, clients)
- Conduct an Enterprise Privacy Risk Assessment
- Integrate data privacy into business risk assessments/reporting
- Maintain a Privacy Strategy
- Maintain a privacy program charter/mission statement
- Require employees to acknowledge and agree to adhere to the data privacy policies

2 Maintain Personal Data Inventory and Data Transfer Mechanisms
Maintain an inventory of the location of key personal data storage or personal data flows, including cross-border, with defined classes of personal data

PRIVACY MANAGEMENT ACTIVITIES

- Maintain an inventory of personal data and/or processing activities
- Classify personal data by type (e.g. sensitive, confidential, public)
- Obtain regulator approval for data processing (where prior approval is required)
- Register databases with regulators (where registration is required)
- Maintain documentation of data flows (e.g. between systems, between processes, between countries)
- Maintain documentation of the transfer mechanism used for cross-border data flows (e.g., model clauses, BCRs, regulator approvals)
- Use Binding Corporate Rules as a data transfer mechanism
- Use contracts as a data transfer mechanism (e.g. Standard Contractual Clauses)
- Use APEC Cross Border Privacy Rules as a data transfer mechanism
- Use Privacy Shield as a data transfer mechanism
- Use regulator approval as a data transfer mechanism
- Use adequacy or one of the derogations (e.g. consent, performance of a contract, public interest) as a data transfer mechanism

3 Maintain Internal Data Privacy Policy
Maintain a data privacy policy that meets legal requirements and addresses operational risk and risk of harm to individuals

PRIVACY MANAGEMENT ACTIVITIES

- Maintain a data privacy policy
- Maintain an employee data privacy policy
- Maintain an organizational code of conduct that includes privacy
- Document legal basis for processing personal data
- Integrate ethics into data processing (Codes of Conduct, policies and other measures)

4 Embed Data Privacy Into Operations
Maintain operational policies and procedures consistent with the data privacy policy, legal requirements, and operational risk management objectives

PRIVACY MANAGEMENT ACTIVITIES

- Maintain policies/procedures for collection and use of sensitive personal data (including biometric data)
- Maintain policies/procedures for collection and use of children and minors' personal data
- Maintain policies/procedures for maintaining data quality
- Maintain policies/procedures for the de-identification of personal data
- Maintain policies/procedures to review processing conducted wholly or partially by automated means
- Maintain policies/procedures for secondary uses of personal data
- Maintain policies/procedures for obtaining valid consent
- Maintain policies/procedures for secure destruction of personal data
- Integrate data privacy into use of cookies and tracking mechanisms
- Integrate data privacy into direct marketing practices
- Integrate data privacy into e-mail marketing practices
- Integrate data privacy into telemarketing practices
- Integrate data privacy into digital advertising practices (e.g. online, mobile)
- Integrate data privacy into hiring practices
- Integrate data privacy into the organization's use of social media
- Integrate data privacy into Bring Your Own Device (BYOD) policies/procedures
- Integrate data privacy into health & safety practices
- Integrate data privacy into interactions with works councils
- Integrate data privacy into practices for monitoring employees
- Integrate data privacy into use of CCTV/video surveillance
- Integrate data privacy into use of geo-location (tracking and or location) devices
- Integrate data privacy into policies/procedures regarding access to employees' company e-mail accounts
- Integrate data privacy into e-discovery practices
- Integrate data privacy into conducting internal investigations
- Integrate data privacy into practices for disclosure to and for law enforcement purposes
- Integrate data privacy into research practices (e.g. scientific and historical research)

5 Maintain Training and Awareness Program
Provide ongoing training and awareness to promote compliance with the data privacy policy and to mitigate operational risks

PRIVACY MANAGEMENT ACTIVITIES

- Conduct privacy training
- Conduct privacy training reflecting job specific content
- Conduct regular refresher training
- Incorporate data privacy into operational training (e.g. HR, marketing, call centre)
- Deliver training/awareness in response to timely issues/topics
- Deliver a privacy newsletter, or incorporate privacy into existing corporate communications
- Provide a repository of privacy information (e.g. an internal data privacy intranet)
- Maintain privacy awareness material (e.g. posters and videos)
- Conduct privacy awareness events (e.g. an annual data privacy day/week)
- Measure participation in data privacy training activities (e.g. number of participants, scoring)
- Enforce the requirement to complete privacy training
- Provide ongoing education and training for the Privacy Office and/or DPOs
- Maintain qualifications for individuals responsible for data privacy, including certifications

6 Manage Information Security Risk
Maintain an information security program based on legal requirements and ongoing risk assessments

PRIVACY MANAGEMENT ACTIVITIES

- Integrate data privacy risk into security risk assessments
- Integrate data privacy into an information security policy
- Maintain technical security measures (e.g. intrusion detection, firewalls, monitoring)
- Maintain measures to encrypt personal data
- Maintain an acceptable use of information resources policy
- Maintain procedures to restrict access to personal data (e.g. role-based access, segregation of duties)
- Integrate data privacy into a corporate security policy (protection of physical premises and hard assets)
- Maintain human resource security measures (e.g. pre-screening, performance appraisals)
- Integrate data privacy into business continuity plans
- Maintain a data-loss prevention strategy
- Conduct regular testing of data security posture
- Maintain a security certification (e.g. ISO)

7 Manage Third-Party Risk
Maintain contracts and agreements with third-parties and affiliates consistent with the data privacy policy, legal requirements, and operational risk tolerance

PRIVACY MANAGEMENT ACTIVITIES

- Maintain data privacy requirements for third parties (e.g. clients, vendors, processors, affiliates)
- Maintain procedures to execute contracts or agreements with all processors
- Conduct due diligence around the data privacy and security posture of potential vendors/processors
- Conduct due diligence on third party data sources
- Maintain a vendor data privacy risk assessment process
- Maintain a policy governing use of cloud providers
- Maintain procedures to address instances of non-compliance with contracts and agreements
- Conduct due diligence around the data privacy and security posture of existing vendors/processors
- Review long-term contracts for new or evolving data privacy risks

8 Maintain Notices
Maintain notices to individuals consistent with the data privacy policy, legal requirements, and operational risk tolerance

PRIVACY MANAGEMENT ACTIVITIES

- Maintain a data privacy notice
- Provide data privacy notice at all points where personal data is collected
- Provide notice by means of on-location signage, posters
- Provide notice in marketing communications (e.g. emails, flyers, offers)
- Provide notice in contracts and terms
- Maintain scripts for use by employees to explain or provide the data privacy notice
- Maintain a privacy Seal or Trustmark on the website to increase customer trust

9 Respond to Requests and Complaints from Individuals
Maintain effective processes for interactions with individuals about their personal data

PRIVACY MANAGEMENT ACTIVITIES

- Maintain procedures to address complaints
- Maintain procedures to respond to requests for access to personal data
- Maintain procedures to respond to requests and/or provide a mechanism for individuals to update or correct their personal data
- Maintain procedures to respond to requests to opt-out of, restrict or object to processing
- Maintain procedures to respond to requests for information
- Maintain procedures to respond to requests for data portability
- Maintain procedures to respond to requests to be forgotten or for erasure of data
- Maintain Frequently Asked Questions to respond to queries from individuals
- Investigate root causes of data privacy complaints
- Monitor and report metrics for data privacy complaints

10 Monitor for New Operational Practices
Monitor organizational practices to identify new processes or material changes to existing processes and ensure the implementation of Privacy by Design principles

PRIVACY MANAGEMENT ACTIVITIES

- Integrate Privacy by Design into data processing operations
- Maintain PIA/DPIA guidelines and templates
- Conduct PIAs/DPIAs for new programs, systems, processes
- Conduct PIAs or DPIAs for changes to existing programs, systems, or processes
- Engage with stakeholders (e.g., individuals, privacy advocates) as part of the PIA/DPIA process
- Track and address data protection issues identified during PIAs/DPIAs
- Report PIA/DPIA analysis and results to regulators (where required) and external stakeholders (if appropriate)

11 Maintain Data Privacy Breach Management Program
Maintain an effective data privacy incident and breach management program

PRIVACY MANAGEMENT ACTIVITIES

- Maintain a data privacy incident/breach response plan
- Maintain a breach notification (to affected individuals) and reporting (to regulators, credit agencies, law enforcement) protocol
- Maintain a log to track data privacy incidents/breaches
- Monitor and report data privacy incident/breach metrics (e.g. nature of breach, risk, root cause)
- Conduct periodic testing of data privacy incident/breach plan
- Engage a breach response remediation provider
- Engage a forensic investigation team
- Obtain data privacy breach insurance coverage

12 Monitor Data Handling Practices
Verify operational practices comply with the data privacy policy and operational policies and procedures, and measure and report on their effectiveness

PRIVACY MANAGEMENT ACTIVITIES

- Conduct self-assessments of privacy management
- Conduct Internal Audits of the privacy program (i.e. operational audit of the Privacy Office)
- Conduct ad-hoc walk-throughs
- Conduct ad-hoc assessments based on external events, such as complaints/breaches
- Engage a third party to conduct audit/assessments
- Monitor and report privacy management metrics
- Maintain documentation as evidence to demonstrate compliance and/or accountability
- Maintain certifications, accreditations or data protection seals for demonstrating compliance to regulators

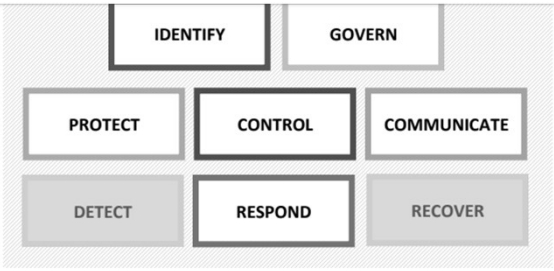
13 Track External Criteria
Track new compliance requirements, expectations, and best practices

PRIVACY MANAGEMENT ACTIVITIES

- Identify ongoing privacy compliance requirements e.g., law, case law, codes, etc.
- Maintain subscriptions to compliance reporting services/law firm updates to stay informed of new developments
- Attend conferences, privacy conferences, industry association, or think-tank events
- Record/report on the tracking of new laws, regulations, amendments or other rule sources
- Seek legal opinions regarding recent developments in law
- Identify and manage conflicts in law
- Document decisions around new requirements, including their implementation or any rationale behind decisions not to implement changes

38

NIST Privacy Framework



104

105 **Table 1: Privacy and Cybersecurity Framework Function and Category Unique Identifiers**

Function Unique Identifier	Function	Category Unique Identifier	Category
ID-P	Identify-P	ID.IM-P	Inventory and Mapping
		ID.BE-P	Business Environment
		ID.RA-P	Risk Assessment
		ID.DE-P	Data Processing Ecosystem Risk Management
GV-P	Govern-P	GV.PP-P	Governance Policies, Processes, and Procedures
		GV.RM-P	Risk Management Strategy

39

ISO 27701 (Formerly 27552)
Enhancement to ISO/IEC 27001 for Privacy Management

- To enhance the existing Information Security Management System (ISMS) with additional requirements in order to establish, implement, maintain, and continually improve a Privacy Information Management System (PIMS)
- Outlines a framework for Personally Identifiable Information (PII) Controllers and PII Processors to manage privacy controls to reduce the risk to the privacy rights of individuals
- Intended to be a certifiable extension to ISO/IEC 27001 certifications

40

41

42