VACB
Virginia Association of Community Banks
One Mission. Community Banks.®

Building an Effective Data Privacy Management Program

AMERICAN SECURITY & PRIVACY

Dr. Kevin F. Streff
605.270.4427
kevin.streff@americansecurityandprivacy.com

Agenda

- Understand what data privacy is and how it impacts FIs
- Distinguish between data security and data privacy
- Learn the sixteen privacy harms that can affect your FI
- Be able to explain the various roles and responsibilities of data privacy in a FI
- Learn what in Information Privacy Program looks like
- Next Steps – Getting started with data privacy management

Overview

Overview

Overview

Security vs. Privacy

- Data security protects information from unauthorized access, use, and disclosure. It also protects it from disruption, modification, or destruction.

- Data privacy is the right to control who gets to see your personal information like credit card numbers and account balances.

Data Privacy Principles

Privacy Principle	Definition
Collection Limitation	There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means
Data Quality	Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up to date
Purpose Specification	The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes
Use Limitation	Personal data should not be disclosed, made available or otherwise used for purposes other than those specified except with the consent of the data subject or by authority of the law
Security Safeguards	Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data
Openness	There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller
Individual Participation	An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed, or amended.
Accountability	A data controller should be accountable for complying with measures which give effect to the principles stated above

GDPR

- Similar to chip-and-pin, the United States will eventually follow Europe's lead
- Opt-in vs. Opt-out
- Crazy fines and enforcement
- Other countries are putting in equally restricting laws with difficult performance criteria
  - Brazil: 15 days to respond to a DSAR (United States is typically 45 days)

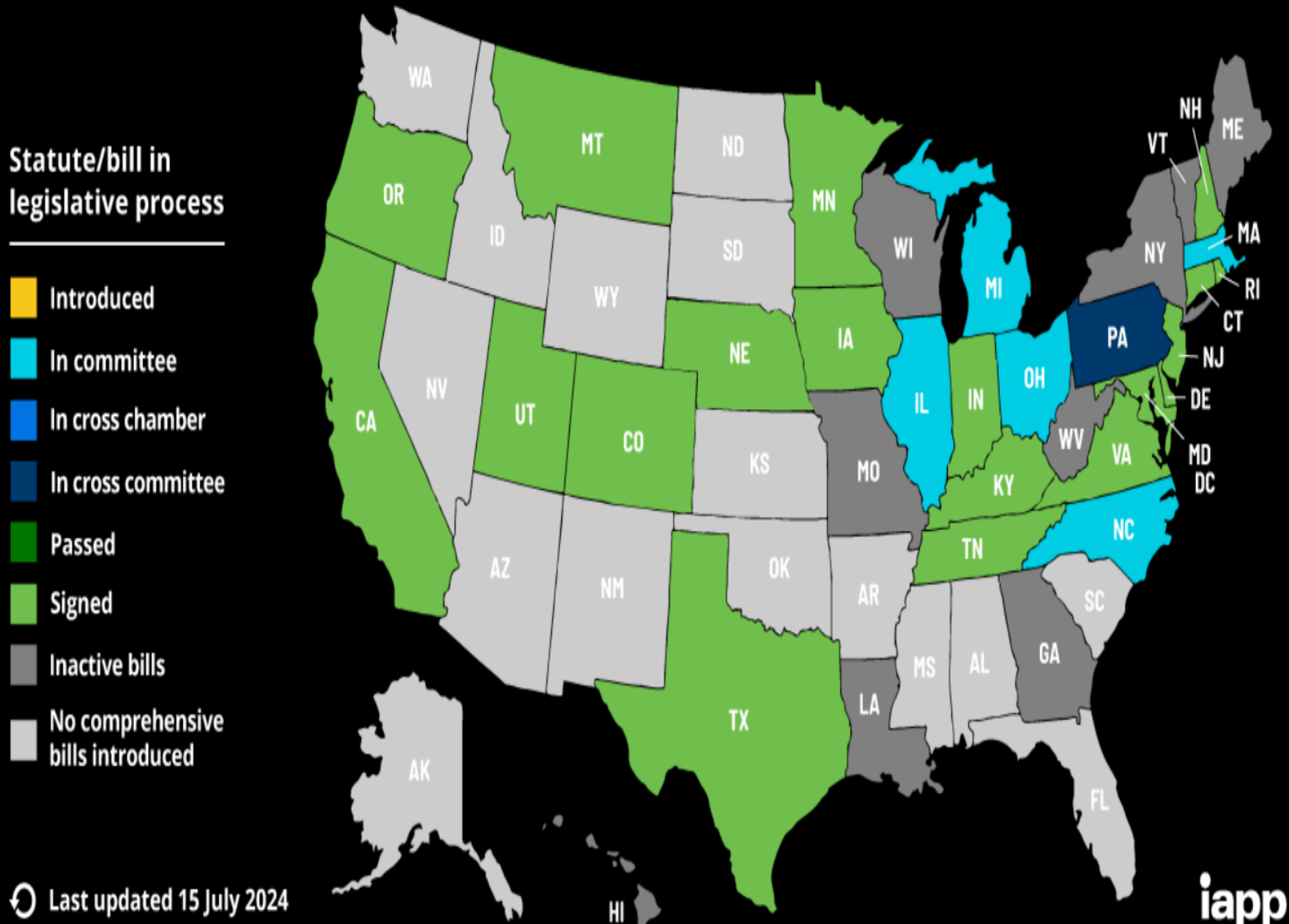
GLBA – Regulation P

- Focuses on consent
- Opt out
- Privacy notices
- Deals with an important but small slice of data privacy
- Consent vs. data stewardship
- Consent vs. accountability

U.S. Privacy Laws

- American Data Privacy and Protection Act (ADPPA) of 2022 – Failed in the House
- American Data Privacy Rights Act of 2024 - Failed

US State Privacy Legislation Tracker 2024



State Law – Virginia

- The right to know about the personal information a business collects about them and how it is used and shared;
- The right to delete personal information collected from them (with some exceptions);
- The right to opt-out of the sale or sharing of their personal information;
- The right to correct inaccurate personal information that a business has about them;
- The right to limit the use and disclosure of personal information collected about them.
- Code of Virginia Code - Chapter 53. Consumer Data Protection Act

Harm Defined

- Privacy Harm – which may also be called a violation or threat – are problematic actions that can result in a loss of privacy and adverse consequences for a person.
- Security has threats…privacy has harms

Privacy Harms

Group	Harm	Harm Definition
Information Collection	Surveillance	Watching, listening to, or recording of an individual's activities
	Interrogation	Questioning or probing individuals for personal information
Information Processing	Aggregation	Combining of various pieces of personal information
	Identification	Linking of information to an individual
	Insecurity	Carelessness in protecting information from leaks or improper access
	Secondary Use	Using personal information for a purpose other than for which it was collected
	Exclusion	Failing to let an individual know about the data that others have about them or participate in its handling or use
Information Dissemination	Breach of Confidentiality	Breaking a promise to keep an individual's information confidential
	Disclosure	Revealing truthful information about an individual that impacts their security or the way others judge their character
	Exposure	Revealing an individual's nudity, grief or bodily functions
	Increased Accessibility	Amplifying the accessibility of personal information
	Blackmail	Threatening to disclose personal information
	Appropriation	Using an individual's identity to serve the aims and interests of another
	Distortion	Disseminating false or misleading information about an individual
Invasion	Intrusion	Disturbing an individual's tranquility or solitude
	Decisional	Intruding into an individual's decision making regarding their private affairs

Data Privacy Management Benefits

- Meeting compliance requirements
- Avoiding fines and penalties
- Reduced risk of privacy breaches, which can result in fines, penalties, or civil lawsuits against the organization
- Reduced risk of data subjects being harmed from the organizations' privacy breaches
- Building and maintaining the brand value, accountholder loyalty, and the organization's reputation
- Supporting ethics and corporate responsibility
- Maintaining trust of investors, accountholders, and the general public
- Being able to support accountholder's wishes for how their data is handled
- Gaining a competitive advantage and differentiating from competitors

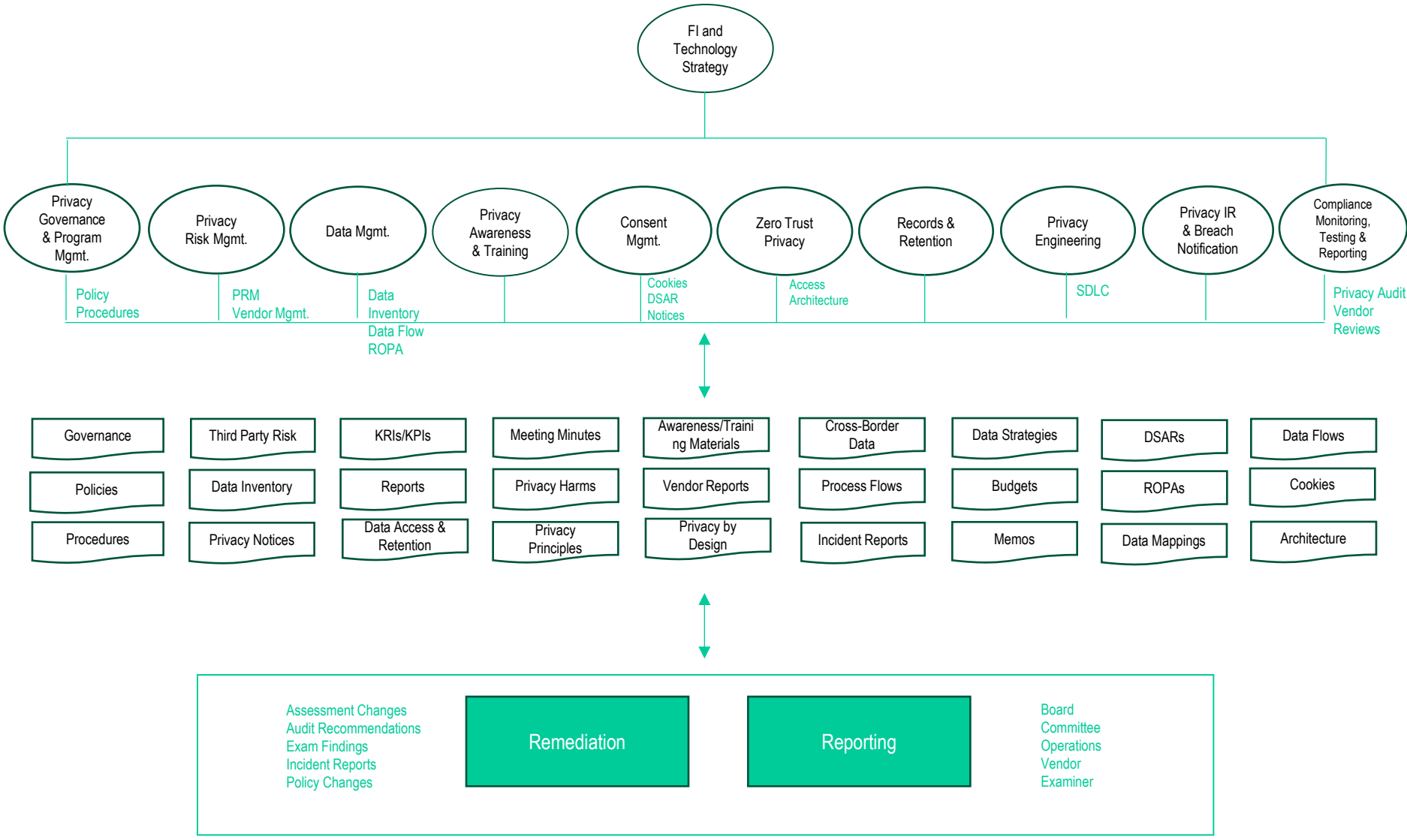
Privacy Roles and Responsibilities

- IPO/DIPO - NEW
- HR
- Marketing
- Finance
- Operations
- Information Technology
- Information Security
- Vendors
- Business Partners
- Employees
- Accountholders

Additional Foundations of an Information Privacy Program

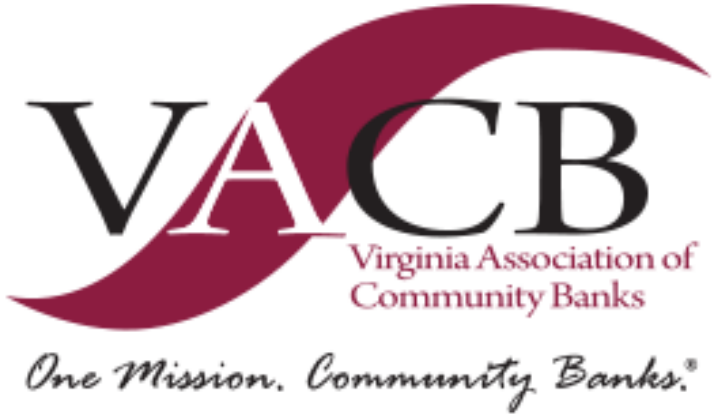
- Program Selection
- Policy Development
- Risk Management
- Vendor Management
- Incident Response
- Training and Awareness
- Auditing

Information Privacy Program Blueprint
American Security and Privacy, LLC



Five Affordable Next Steps

1. Name a Privacy Officer
2. Get the Privacy Officer some bank-specific data privacy training
3. Create a Data Privacy policy
4. Ensure your IT auditor is also assessing your data privacy program and practices
5. Perform a data privacy gap analysis to build a 3-year plan



Thank you VACB!

Questions

kevin.streff@americansecurityandprivacy.com