# Privacy by Design for Web Developers

Building Trust through Responsible Development

January 24, 2024

**by Miguel Villegas**

iSecurePrivacy LLC

Mike.Villegas@isecureprivacy.com

213-453-6174

# Abstract

In today's digital landscape, the protection of user privacy has become a paramount concern. As web developers, it is our responsibility to ensure that the websites and applications we create not only deliver exceptional user experiences but also prioritize the privacy and security of user data. This lecture, "Privacy by Design for Web Developers," explores the foundational principles and practical strategies that empower web developers to integrate privacy into every facet of their work.

In this lecture, we will delve into the concept of Privacy by Design (PbD) and its significance in the context of web development. We will examine how PbD serves as a proactive approach to safeguarding user data, fostering trust, and complying with evolving privacy regulations such as the GDPR and CCPA/CPRA.


- ***Miguel (Mike) O. Villegas***

  *CISA, CISSP, CSX|F, CSX|A, CDPSE, CEH, ISO/IEC 27001 Lead Implementer*
- *vCISO for TRISTAR Insurance Group*
  *Long Beach, CA*
- *CTO for Xahive*
  *Toronto, Canada*
- *Mike.Villegas@isecureprivacy.com*
- *213.453.6174 (mobile)*

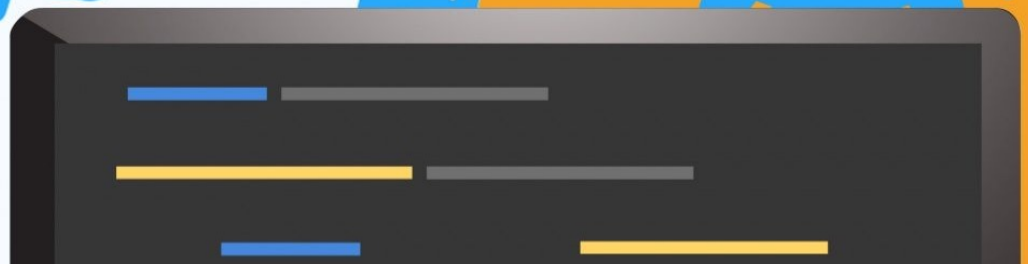
# Agenda

- Privacy by Design
- The 7 Foundational Principles of PbD
- US Privacy Laws
- Use CCPA/CPRA as Sample Privacy Rules
- Privacy Impact Assessment
- Privacy Policy
- Incorporate Privacy Into SDLC
- PCI Secure Software Framework
- Summary



CCPA Link: https://www.oag.ca.gov/privacy/ccpa

# Introduction



## 1 Definition of Privacy by Design (PbD)

Privacy by Design (PbD) is an approach to embedding privacy and data protection measures into the design and development of systems, processes, and technologies from the outset, rather than as an afterthought.

## 2 Importance of Privacy in Web Development

With the increasing focus on data privacy and security, integrating privacy features in web development is crucial to building user trust and compliance with regulations.

## 3 Agenda for the Presentation

This presentation will cover key concepts, principles, and best practices of Privacy by Design, aiming to equip web developers with the knowledge to build privacy-focused solutions.

# What is Privacy by Design (PbD)?

1

## Concept originated by Dr. Ann Cavoukian

Privacy by Design was conceptualized by Dr. Ann Cavoukian as an approach to proactively embedding privacy into the design and architecture of systems, promoting a privacy-respecting and data-protective mindset.

2

## Proactive approach to privacy

Privacy by Design advocates a proactive stance, emphasizing the importance of anticipating and preventing privacy breaches, rather than reacting to data protection issues after they have occurred.

3

## Embedding privacy into design

It emphasizes the integration of privacy into the design of systems, aiming to ensure that privacy considerations are core components of the architecture from the outset.

# The 7 Foundational Principles of PbD

1

**Proactive not Reactive**

Anticipate and prevent privacy breaches.

2

**Privacy as the Default Setting**

Ensure that privacy is the default setting for user data.

3

**Privacy Embedded into Design**

Integrate privacy into the system from the outset.

4

**Full Functionality – Positive-Sum, not Zero-Sum**

Seek to satisfy all legitimate interests and objectives in a win-win manner.

5

**End-to-End Security – Lifecycle Protection**

Ensure that all data is securely managed throughout its lifecycle.

6

**Visibility and Transparency**

Keep users informed about privacy practices and ensure transparency.

7

**Respect for User Privacy – Keep it User-Centric**

Empower user privacy through user-friendly options and controls.


# Legal and Regulatory Compliance

1 **Overview of relevant privacy laws**

Understanding and adhering to privacy laws such as GDPR and CCPA is essential for ensuring legal compliance and minimizing the risk of legal repercussions.

2 **Importance of aligning with legal requirements**

Aligning development practices with legal standards demonstrates a commitment to data privacy and protection, contributing to trust and credibility.

3 **Reducing legal risks through PbD**

Privacy by Design serves as a proactive strategy for reducing legal risks associated with data privacy non-compliance, safeguarding both users' rights and the organization's reputation.

# US Privacy Laws

- Currently, there is no single data protection legislation in the United States of America.
- However, California, Colorado, Connecticut, Utah, Virginia, and 10 other states (14) have each enacted comprehensive consumer data protection laws.
- In California, the California Consumer Privacy Act (CCPA) was signed into law in 2018 and came into force in January 2020.
- There are 21 states that do not have a statewide privacy law.
- The California Privacy Rights Act (CPRA) was passed in November 2020 and amended the CCPA.
- The provisions set forth under the CPRA came into force on January 1, 2023.



CCPA Link: https://www.oag.ca.gov/privacy/ccpa

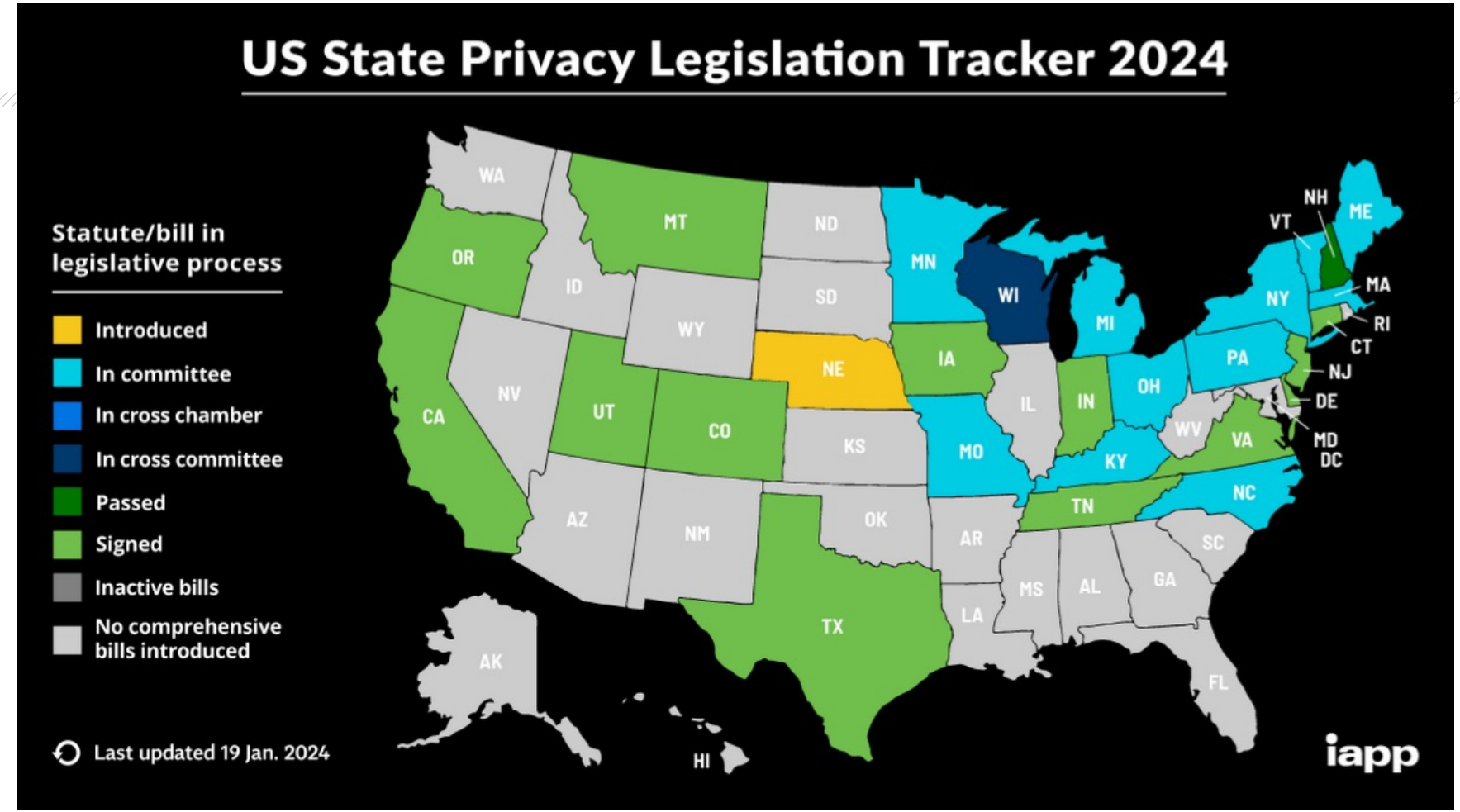
# US State Privacy Legislation Tracker 2024

## Comprehensive Consumer Privacy Bills

| State | Legislative process | Statute/bill | Common name | Consumer rights | | | | | | | | | Business obligations | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Right to access | Right to correct | Right to delete | Right to opt out of certain processing | Right to portability | Right to opt out of sales | Right to opt in for sensitive data processing | Right against automated decision-making | Private right of action | Opt-in default (requirement age) | Notice/transparency requirement | Risk assessments | Prohibition on discrimination (exercising rights) | Purpose/processing limitation |
| **LAWS SIGNED (TO DATE)** | | | | | | | | | | | | | | | | | |
| California | | CCPA | California Consumer Privacy Act (2018; effective 1 Jan. 2020) | X | | X | | X | X | | | L | 16 | X | | | X |
| | | CPRA | California Privacy Rights Act (2020; fully operative 1 Jan. 2023) | X | X | X | S | X | X | | X | L | 16 | X | X | X | X |



https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf

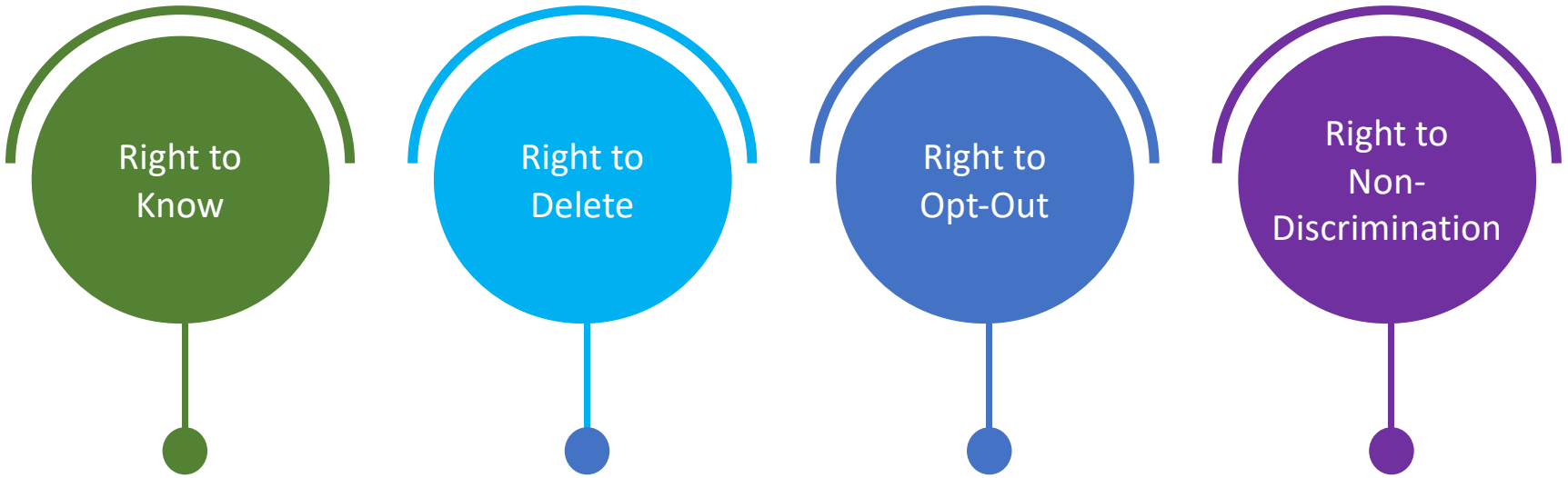





https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

# CCPA

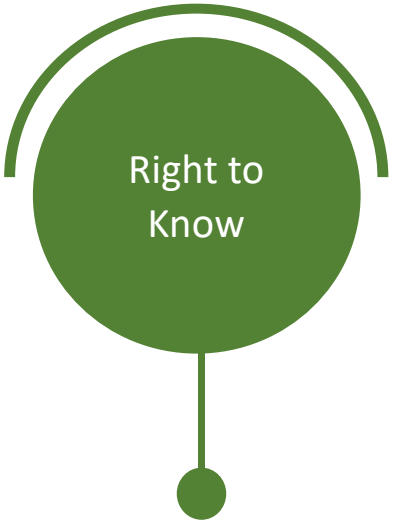
The **California Consumer Privacy Act** (**CCPA**) of 2018 is a state statute intended to enhance privacy rights and consumer protection for residents of California, United States.






CCPA Link: https://www.oag.ca.gov/privacy/ccpa

# CCPA



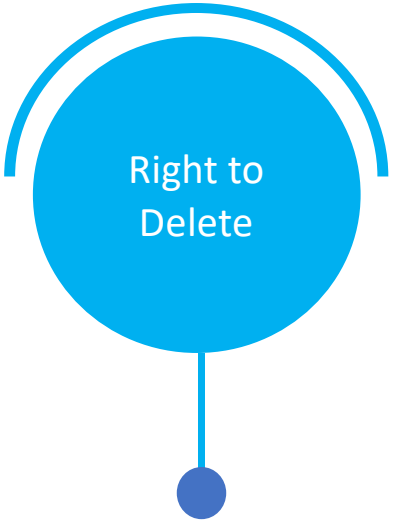

The right to know – you can request businesses to disclose

- PII that is collected about you
- Sources where PII is collected
- Purpose the business uses PII
- With whom the business discloses PII
- What PII the business sells or discloses to third-parties



CCPA Link: https://www.oag.ca.gov/privacy/ccpa

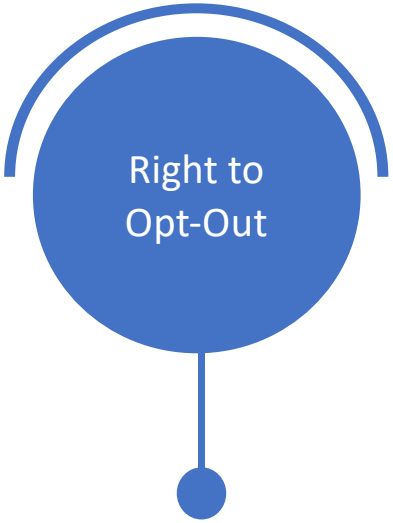
# CCPA




The right to delete – You can request that businesses delete personal information

- That the business collects from you
- The business tells service providers to do the same
- This right to delete is subject to certain exceptions (such as if the business is legally required to keep the information).

# CCPA




The right to opt-out – you may request that businesses

- Stop selling or sharing your personal information (“opt-out”)
- Including via a user-enabled global privacy control.
- Businesses cannot sell or share your personal information after they receive your opt-out request unless you later authorize them to do so again.



CCPA Link: https://www.oag.ca.gov/privacy/ccpa

# CCPA


The right to non-discrimination for exercising their CCPA rights– you may request that businesses

- Cannot deny goods or services,
- Charge you a different price, or
- Provide a different level or quality of goods or services just because you exercised your rights under the CCPA.

# CCPA – Additional Business Obligations

- **Provide notice** to consumers at or before data collection.
- **Create procedures to respond to requests** from consumers to opt-out, know, and delete.
  - For requests to opt-out, businesses must provide a "Do Not Sell My Info" link on their website or mobile app.
- **Respond to requests from consumers** to know, delete, and opt-out within specific timeframes.
  - **As proposed by the draft regulations,** businesses must treat user-enabled privacy settings that signal a consumer's choice to opt-out as a validly submitted opt-out request.
- **Verify the identity of consumers** who make requests to know and to delete, whether or not the consumer maintains a password-protected account with the business.



CCPA Link: https://www.oag.ca.gov/privacy/ccpa

# CCPA – Additional Proposed Business Obligations

- **Disclose financial incentives** offered in exchange for the retention or sale of a consumer's personal information
  - **Explain how they calculate the value of the personal information**.
- **Businesses must maintain records of requests** and how they responded for 24 months in order to demonstrate their compliance.
  - Businesses that collect, buy, or sell the personal information **of more than 4 million consumers have additional record-keeping and training obligations.**



CCPA Link: https://www.oag.ca.gov/privacy/ccpa

# Privacy Impact Assessment (PIA)

1

## Definition of PIA

Privacy Impact Assessment (PIA) is a process used to identify, assess, and mitigate the privacy risks of a proposed project, system, or technology, ensuring that privacy considerations are integrated at the early stages of development.

2

## Conducting a PIA for web development projects

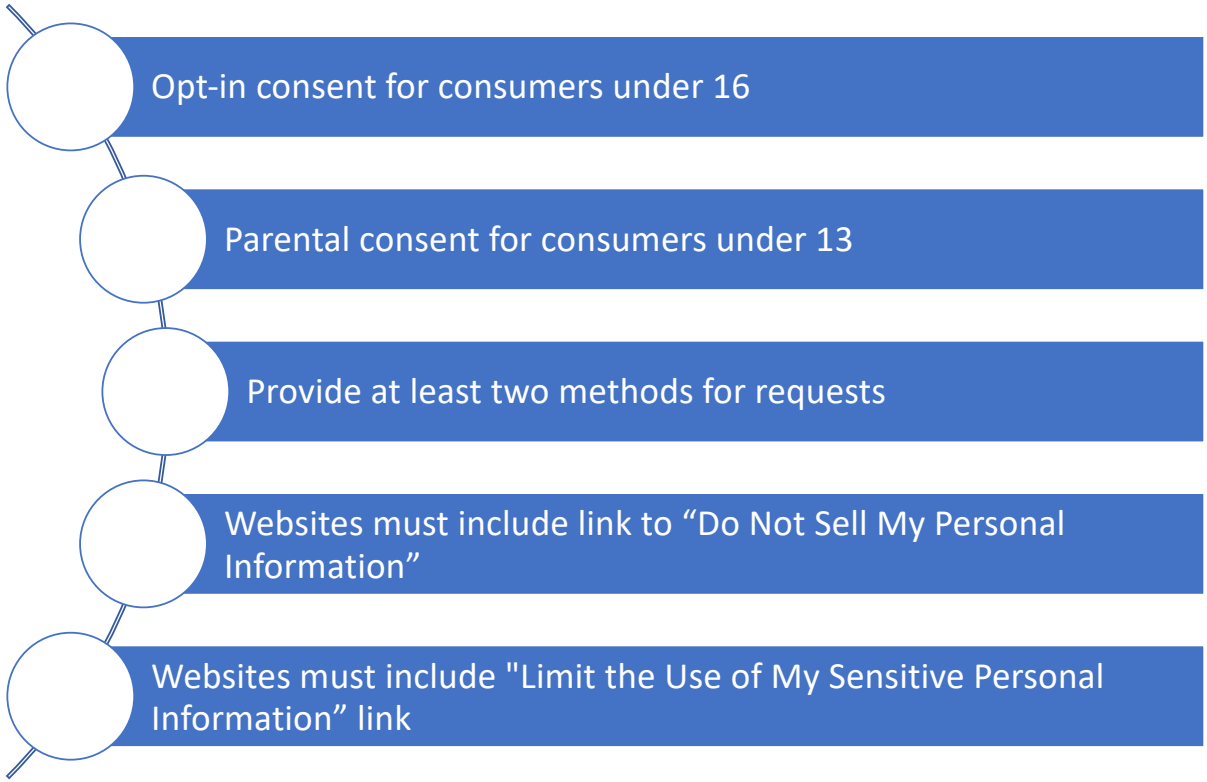
Developers can leverage PIA to systematically evaluate the potential privacy impacts of web development projects, addressing privacy risks and enhancing overall compliance.

3

## Identifying and mitigating privacy risks

PIA facilitates the identification of potential privacy risks and the implementation of measures to mitigate these risks, reinforcing privacy-by-design practices.

# CCPA/CPRA Opt-Out




**A business does not need to provide a notice of right to opt-out if:**

1) It does not sell personal information; and
2) It states in its privacy policy that it does not sell personal information



https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-add-adm.pdf

# COOKIES

When you visit some web pages, you are given the option to set a cookie when you click another link. The cookie contains information about how the cookie works.

There are several types of cookies:

- Session Cookies
- Persistent Cookies
  - Authentication Cookies
  - Tracking Cookies
- First-Party Cookies
- Third-Party Cookies


- Zombie Cookies
- Essential Cookies

# CPPA Proposes Requiring Browsers to Offer Opt-Out Signals

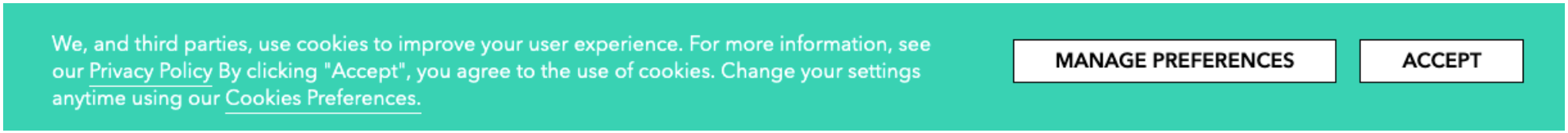
The California Privacy Protection Agency Board voted 5-0 at its December 8, 2023, meeting to advance a legislative proposal to require browser vendors to include a feature that allows users to exercise their California privacy rights through opt-out preference signals.

- CPPA Board voted 5-0 to advance proposal
- Would require browser vendors to include opt-out preference signals
- Signals allow consumers to easily opt-out of data sale/sharing
- Only 10% of browsers currently support signals
- Proposal aims to make it easier for consumers to exercise privacy rights
- CA would be first state to mandate if passed into law



https://cppa.ca.gov/announcements/2023/20231211.html

# SAMPLE




Your choice regarding cookies on this website:

We, and third parties, use cookies and other electronic tools to enhance your experience, analyze site usage, and deliver advertisements tailored to your interests. For more information, please read our Privacy Policy By clicking "Accept", you will save your cookie settings and agree to the use of these tools.

**Required**

These cookies are required to enable core site functionality.

Adobe Experience Platform Launch
Google Tag Manager

**Performance** **Off**

These cookies allow us to analyze site usage so we can measure and improve performance. They collect information in a way that does not directly identify individuals.

- ☐ Google Analytics and Optimize
- ☐ Adobe Analytics

**Advertising** **Off**

We and our advertising partners use electronic technologies to collect certain types of personal information through our digital properties in order to provide you with relevant advertisements. Personal information may include your IP address, digital identifiers, and your interactions with digital properties.

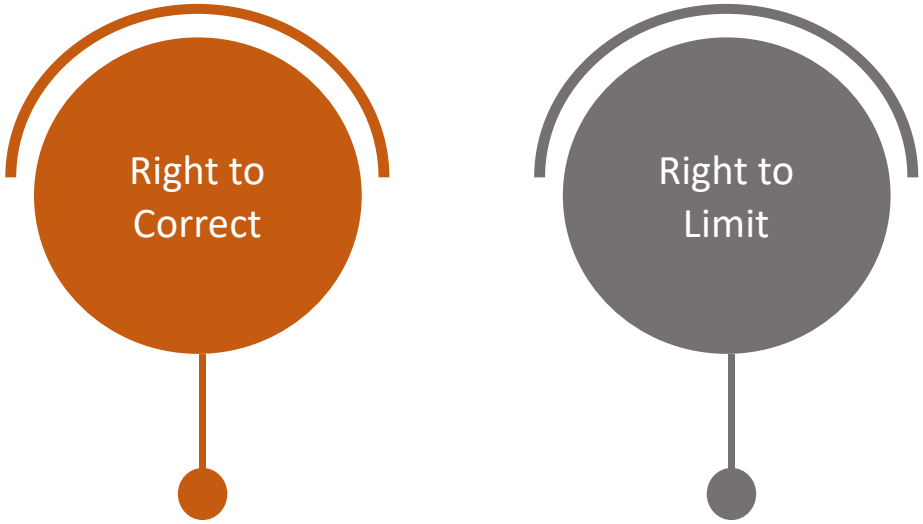
- ☐ SalesWings
- ☐ StackAdapt
- ☐ Bing Ads & Remarketing
- ☐ DoubleClick and Google Audiences
- ☐ Twitter Tracking and Advertising
- ☐ Google Ads
- ☐ LinkedIn Marketing Solutions
- ☐ LinkedIn Ads
- ☐ Facebook Custom Audience

ACCEPT REJECT

By clicking "Accept", you are saving your cookie settings and agreeing to the use of these tools. You can change your settings at anytime using the Cookies Preferences link in the footer of this website.

# CPRA

In November of 2020, California voters approved Proposition 24, the CPRA, which amended the CCPA and added new additional privacy protections that began on January 1, 2023. As of January 1, 2023, consumers have new rights in addition to those above, such as:





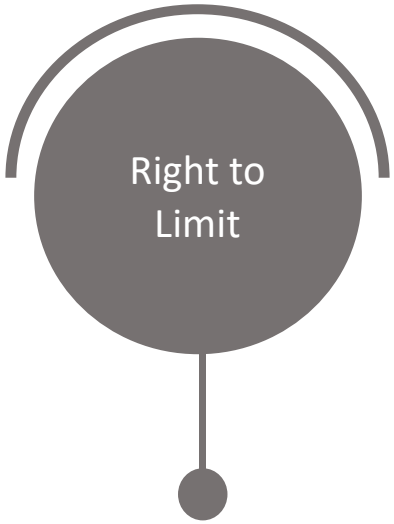

CCPA Link: https://www.oag.ca.gov/privacy/ccpa

# CPRA


The right to correct – You may ask businesses to correct inaccurate information that they have about you.

The California Privacy Protection Agency is currently engaged in a formal rulemaking process and has proposed CCPA regulations pertaining to the right to correct, but these are not currently final or effective.

# CPRA




The right to limit the use and disclosure of sensitive personal information collected about them. You can direct businesses to

- Only use your sensitive personal information for limited purposes
- For example, your social security number, financial account information, your precise geolocation data, or your genetic data for limited purposes, such as providing you with the services you requested.



CCPA Link: https://www.oag.ca.gov/privacy/ccpa

# Privacy Impact Assessment (PIA)

## Categories

- Employee Data
- Customer Data
- Patient Data
- Suppliers/Vendors
- Company Information

## Personal Information

- Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
- Characteristics of protected classifications under California or federal law.
- Biometric information.
- Professional or employment-related information.

- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website application, or advertisement.

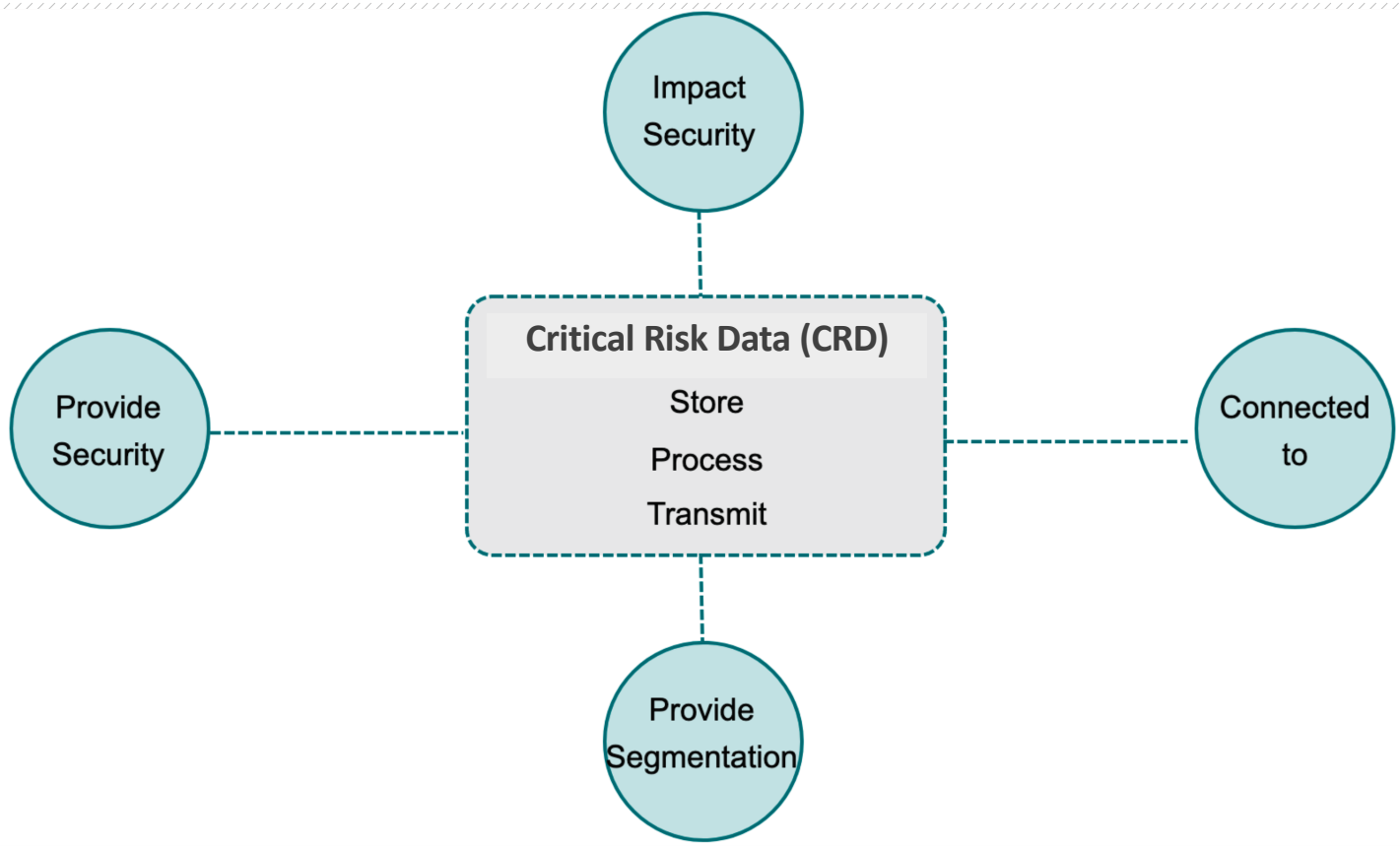
- Geolocation data.
- Audio, electronic, visual, thermal, olfactory, or similar information.
- Education information, defined as information that is not publicly available
- Inferences drawn from any of the information identified to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
- Sensitive personal information."

# Privacy Impact Assessment (PIA)

## Data Inventory

- Data – describe the data
- Source – where does it come from or generated
- Location/Where Stored
- Were has data been sent?
- Technology Used (Is the data located on:
  - (1) database (e.g., MS SQL, Oracle, MySQL, Postgres, etc)
  - (2) server (e.g., Windows, Linux, HP/UX)
  - (3) file share (Sharepoint, Windows, Google Docs, Box,etc),
  - (4) mobile device (e.g., laptops, smartphones, tablets),
  - (5) applications (e.g., Excel, MS Access),
  - (6) cloud services (e.g., AWS, Azure, Google Apps, Office 365)
- Data Purpose
- Consent of Data Subjects?
- Retention Requirements
- Parties with Access to Data
- Security Measures to Protect Data
- Destruction – how is it destroyed?
- Contact information of the Data Controller, Data Processor, and Data Protection Officer
- Classification / Sensitivity
- Business Criticality
- Comments

# SCOPE OF DATA



# Using the PIA

**PIA is a valuable tool for organizations to implement PbD principles.**

- Typically, the PIA is done by the Privacy Officer, CISO, or Internal Audit
- PIA is sent to each critical business unit and backoffice group in the enterprise
- An aggregated PIA is consolidated to see where critical data resides
- Provide input on the PIA process.
- Use the PIA to determine where critical data resides
- Perform an inventory of your own for data that you will be using in your development process
- If it is critical risk data (CRD), provide your list to the CPO, CISO, or Audit to ensure it is included in the updated Annual PIA.

# Sensitive Data

All sensitive data stored, processed, or transmitted by the software is identified.

- all payment data (PII, ePHI, PCI, critical risk data)
- authentication credentials (passwords, tokens, certificates, DEKs, KEKs)
- cryptographic keys and related data (such as IVs and seed data for random number generators);
- system configuration data such as:
  - registry entries,
  - platform environment variables,
  - prompts for plaintext data in software allowing for the entry of PIN data, or configuration scripts.
- Where is it stored
  - Temporary storage (volatile memory)
  - Semi-permanent storage (RAM)
  - Non-volatile storage (flash drives and flash storage media)
- How is it protected
  - Cryptography • ACL. • Protected memory. • HSM

# Web Software Components and Services

Modern software is rarely created entirely in-house and is typically composed of various bespoke code segments that are integrated with numerous components. The following software components need to be identified, verified, and tested for vulnerabilities:

- All proprietary software libraries, packages, modules, and/or code packaged in a manner that enables them to be tracked as a freestanding unit of software.
- All third-party and open-source frameworks, libraries, and code embedded in or used by the software during operation.
- All third-party software dependencies, APIs, and services called by the software during operation.

NIST refers to “provenance data” as information of the above components and services, versions, and any third-party code that may be embedded in these components.

## The software does not disclose sensitive data through unintended channels.

- Error messages, error logs, or memory dumps.
- Execution environments that may be vulnerable to remote side-channel attacks to expose sensitive data
- Automatic storage or exposure of sensitive data by the underlying execution environment, such as through swap-files, system error logging, keyboard spelling, and auto-correct features
- Sensors or services provided by the execution environment that may be used to extract or leak sensitive data such as through use of an accelerometer to capture input of a passphrase to be used as a seed for a cryptographic key, or through capture of sensitive data through use of cameras, near-field communication (NFC) interfaces

# Data Minimization and Purpose Limitation

## Collecting only necessary data

Developers should limit the collection of personal data to what is strictly necessary for the intended purpose, reducing the volume of collected data, and minimizing privacy risks.

## Defining the purpose of data processed

A clear definition of the purpose of data processing enables transparent and lawful data handling, aligning with the principle of purpose limitation within Privacy by Design.

## Limiting data collection

Emphasizing data minimization supports the principle of Privacy by Design, ensuring that only essential data is collected, processed, and retained, thereby enhancing user privacy and trust.

**IF YOU DO NOT NEED IT**
**DO NOT STORE IT**

# CCPA/CPRA Cybersecurity Audit

**§ 7123. Scope of Cybersecurity Audits.**

- Title of qualified individuals responsible for business's cybersecurity program
- Date the cybersecurity program evaluation presented to BOD
- Safeguards
  - Authentication such as MFA, strong unique passwords or passphrases
  - Strong encryption of PII at rest and in transit
  - Zero trust architecture
  - Account management and access controls (RBAC)
    - Employee, contractor, other personnel
    - Service provider restricted access
    - Privileges to third parties to whom the business sells or shares PII
  - Restrict number of privileged accounts
  - Inventory of PII, hardware, software, and approval process
  - Patching and change management
  - Secure hardware and software configuration standards
  - Vulnerability management (scans, pen tests, network monitoring)
  - AV/Anti-Malware
  - Segmentation controls
  - Cybersecurity awareness, education, and training
  - Secure development and secure coding
  - Oversight of service providers/vendors
  - Retention requirements
  - Incident Response



https://cppa.ca.gov/meetings/materials/20230908.html

# California Governor Approves "Delete Act" to Strengthen Data Privacy

- Governor Newsom signed "California Delete Act" (SB 362) into law
- Gives CPPA authority over state's data broker registry
- Requires accessible deletion system for consumers by January 1, 2026
- Allows consumers to direct data brokers to delete info in one step
- Prohibits data brokers from selling/sharing deleted info
- Expands CCPA's definition of sensitive personal information
- Strengthens protections for reproductive privacy
- Goes into effect January 1, 2024
- By January 1, 2028, data brokers required to have independent compliance audit
- Penalty of $200 administrative fine per day for non-compliance



https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202120220SB362


# User Consent and Control

1

## Importance of obtaining informed consent

Ensuring that users provide informed consent for data collection and processing activities, respecting their autonomy and privacy preferences as fundamental components of Privacy by Design.

2

## Providing users with control

Empowering users with control over their personal data, including the ability to access, review, and manage their data, fostering trust and transparency within Privacy by Design.

3

## Clear and user-friendly consent mechanisms

Implementing transparent and easily accessible consent mechanisms allows users to make informed choices, honoring the user-centric principle of Privacy by Design.

# Privacy-Focused Development Tools and Frameworks

### Overview of tools and frameworks

Existing development tools and frameworks prioritize privacy elements, offering developers the resources to integrate privacy-enhancing features into their solutions.

### Incorporating privacy features

Integrating privacy-focused tools and frameworks into development environments facilitates the cultivation of privacy-aware applications and systems.

### Examples

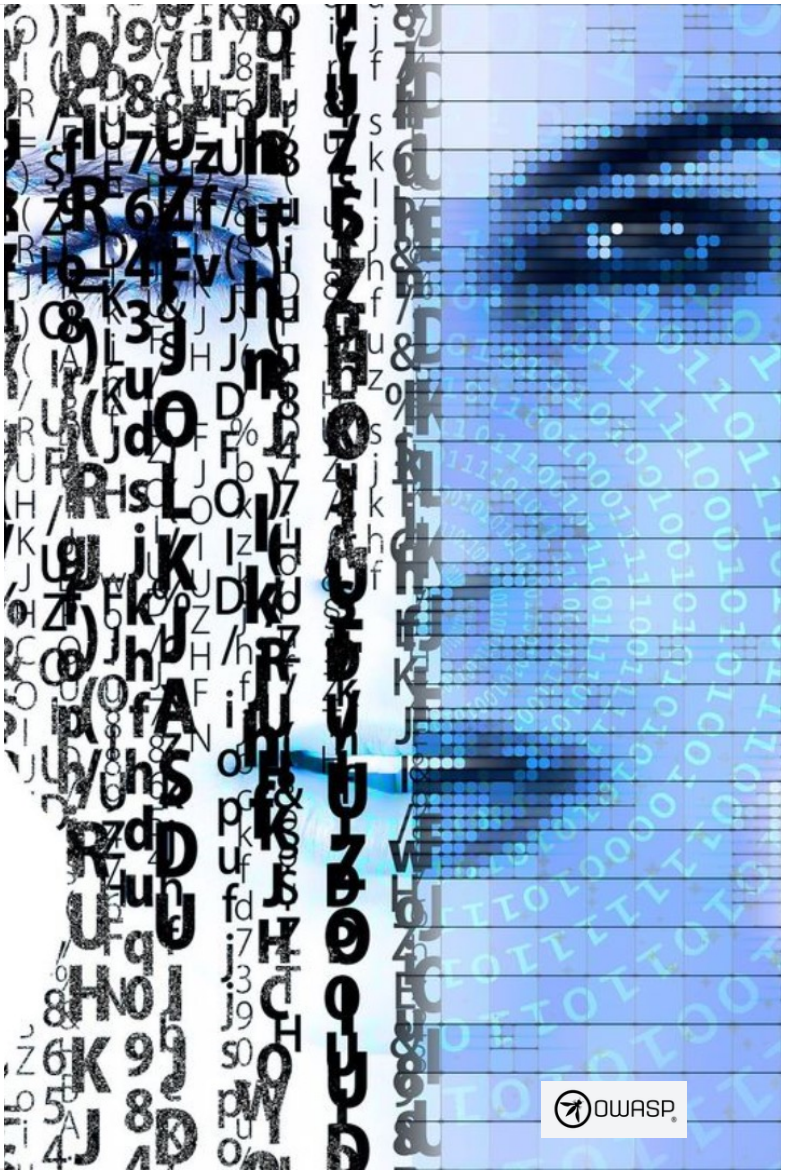
Privacy-preserving libraries and secure coding practices exemplify the initiative to incorporate privacy-centric developments into web development processes.

# Privacy Training for Developers

| | |
|---|---|
| **Importance of privacy awareness** | Inducting developers with a comprehensive understanding of privacy principles and best practices enriches their ability to design and develop privacy-respecting solutions. |
| **Incorporating privacy training** | Integrating privacy education into developer onboarding processes illuminates the significance of privacy by design in the organization's ethos and operational standards. |
| **Continuous education and updates** | Maintaining ongoing education and updates on privacy best practices ensures that developers remain adept at evolving privacy requirements and industry standards. |

# Privacy Testing and Auditing

- Integration into the development lifecycle
- Regular privacy audits
- Tools and methodologies



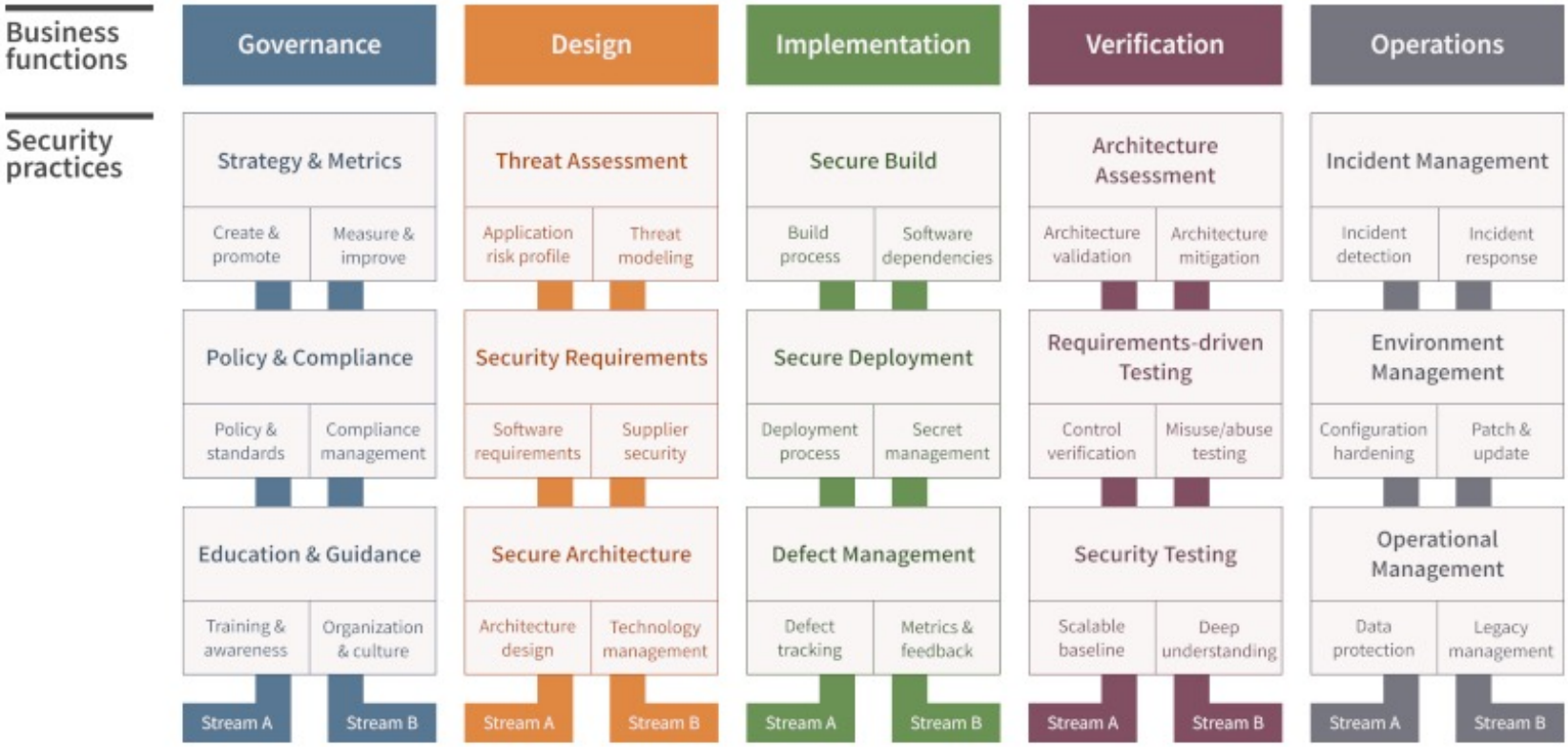
TRISTAR

TABLE OF CONTENTS



TRISTAR

# OWASP SAMM v2.0




iSecurePrivacy LLC

The Software Assurance Maturity Model (SAMM) is an open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization.

OWASP

# Software Development Life Cycle (SDLC)

**If you have 1 hour to chop down a tree, you should spend 45 minutes sharpening your ax**

**Privacy and Cybersecurity**

# Incorporate Privacy into SDLC

| | |
|---|---|
| **Requirements Analysis** | Identify privacy requirements for the application, considering factors such as data collection, storage, processing, data traversal, sharing, and destruction |
| **Design** | Develop application designs that prioritize privacy, incorporating featuers such as data minimization, encryption, access controls, and secure data storage. Use industry-accepted encryption algorithms. |
| **Implementation** | Ensure that privacy-enhancing technologies and best practices are employed during the development process, including secure coding techniques, privacy-preserving algorithms, and secure data transmission protocols. |
| **Testing** | Conduct thorough privacy testing, including vulnerability assessments, fuzzy testing, penetration testing, static and dynamic code analysis scans, OWASP Top 10, CWE |
| **Deployment** | Implement privacy controls and monitoring systems to ensure that the applicaion maintains compliance with data protection regulations and adheres to privacy best practices throughout its lifecycle. |
| **Maintenance and Updates** | Regularly review and update the application to address emerging privacy risks and regulatory changes, ensuring that privacy remains a core consideration throughout the application's lifecycle. |

# PCI Secure Software Framework (SSF)

| Secure SLC Control Objectives | Secure Software Control Objectives |
|---|---|
| CO1: Security Responsibilities and Resources | CO1: Critical Asset Identification |
| CO2: Software Security Policy & Strategy | CO2: Secure Defaults |
| CO3: Threat Identification & Mitigation | CO3: Sensitive Data Retention |
| CO4: Vulnerability Detection & Mitigation | CO4: Critical Asset Protection |
| CO5: Change Management | CO5: Authentication & Access Control |
| CO6: Software Integrity Protection | CO6: Sensitive Data Protection |
| CO7: Sensitive Data Protection | CO7: Use of Cryptography |
| CO8: Vendor Security Guidance | CO8: Activity Tracking |
| CO9: Stakeholder Communications | CO9: Attack Detection |
| CO10: Software Update Information | CO10: Threat & Vulnerability Management |
| | CO11: Secure Software Updates |
| | CO12: Software Vendor Implementation Guidance |

PCI Security Standards Council

## Module C – Web Software Requirements

| Module Name | Overview | Control Objectives |
|---|---|---|
| **Module C: Web Software Requirements** | Additional security requirements for payment software that uses Internet technologies, protocols, and languages to initiate or support electronic payment transactions. | **C.1**: Web Software Components & Services<br>**C.2**: Web Software Access Controls<br>**C.3:** Web Software Attack Mitigation<br>**C.4**: Web Software Communications |

https://docs-prv.pcisecuritystandards.org/Software%20Security/Supporting%20Document/PCI-Secure-Software-Program-Guide-v1_2.pdf

# PCI Account Data

| Account Data | |
|---|---|
| Cardholder Data includes: | Sensitive Authentication Data includes: |
| • Primary Account Number (PAN) | • Full track data (magnetic-stripe data or equivalent on a chip) |
| • Cardholder Name | • CAV2/CVC2/CVV2/CID |
| • Expiration Date | • PINs/PIN blocks |
| • Service Code | |

| PAN Obfuscation | |
|---|---|
| • Encryption | Implies it can be decrypted |
| • Truncation | 1234-56**-****-7890 (first 6; last 4) |
| • Hashing | One way hashing with salt; need strong algorithm not subject to rainbow |
| • Tokenization | Data replaced by surrogate, proxy values or tokens |
| • Masking | Data displayed in viewing or entering (first 6; last 4) |

# The 7 Foundational Principles of PbD

1

**Proactive not Reactive**

Anticipate and prevent privacy breaches.

2

**Privacy as the Default Setting**

Ensure that privacy is the default setting for user data.

3

**Privacy Embedded into Design**

Integrate privacy into the system from the outset.

4

**Full Functionality – Positive-Sum, not Zero-Sum**

Seek to satisfy all legitimate interests and objectives in a win-win manner.

5

**End-to-End Security – Lifecycle Protection**

Ensure that all data is securely managed throughout its lifecycle.

6

**Visibility and Transparency**

Keep users informed about privacy practices and ensure transparency.

7

**Respect for User Privacy – Keep it User-Centric**

Empower user privacy through user-friendly options and controls.

# THANK YOU!