CCPA Readiness

Compliance Guide

Ext.prc.001.02 | 12.20.2019

Table Of Contents

- On 28th June 2018, the State of California enacted Bill AB-375, a sweeping new privacy bill known as the California Consumer Privacy Act (CCPA).

- **While amendments are expected, it comes into effect on January 1, 2020.**

- Organizations that have been focusing on building an accountable privacy program or on comprehensive GDPR compliance initiatives will be able to leverage that work for CCPA compliance initiatives.

- **Given the new individual rights within the law (right to request information; right of deletion; right to opt-out and obligations to inform), along with a private right of action, the risk of non-compliance is significant.**

CCPA
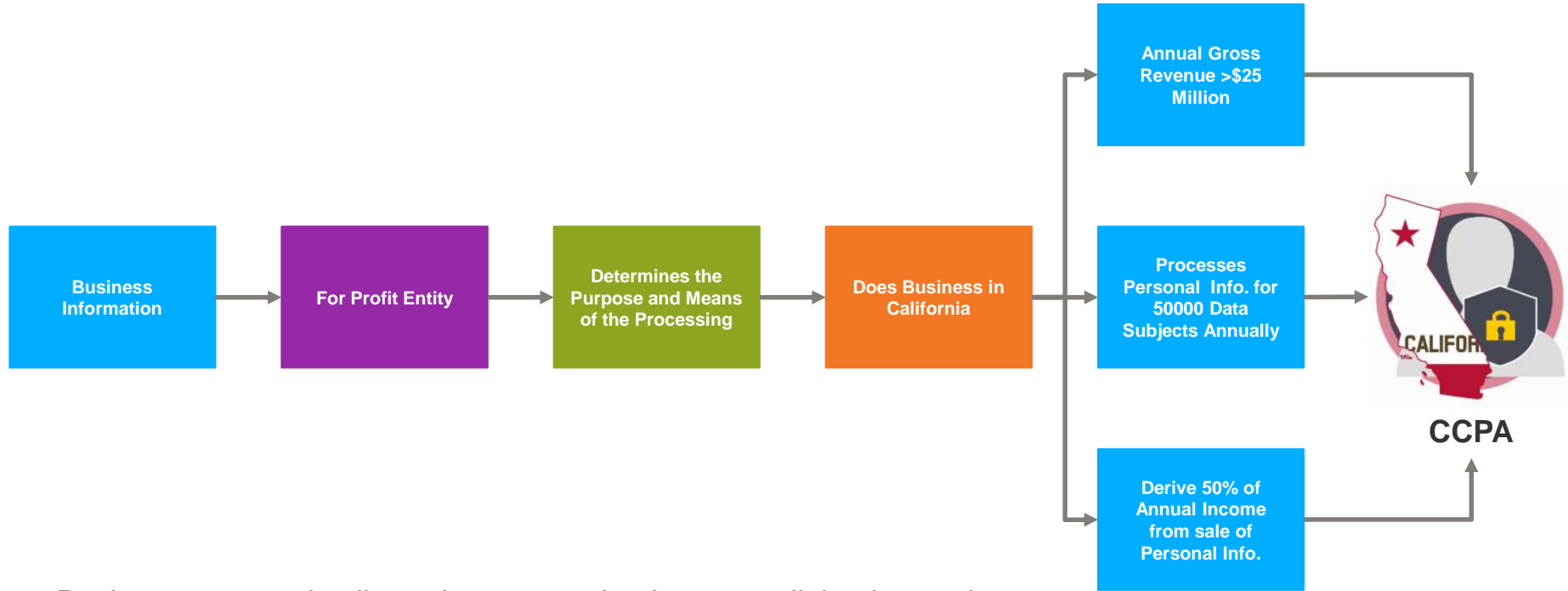
- Business contact details such as name, business email, business phone numbers, etc. are primarily processed and housed at ZINFI.
- ZINFI does business in California.
- ZINFI does not sell personal information.

ZINFI lets consumers

- **KNOW WHAT** personal information is collected from them.

- **KNOW WHETHER their** personal information is sold or disclosed to whom.

- **OPT OUT** of their processing of personal information.

CCPA Laws	CCPA Measures adopted by ZINFI
1798.100	Maintains procedures to respond to requests for access to personal data. Maintains a data privacy notice. Maintains procedures to respond to requests for data portability
1798.105	Maintains procedures to respond to requests to be forgotten or for erasure of data.
1798.110	Maintains procedures to respond to requests for information.
1798.115	Maintains procedures to respond to requests to opt- out of, restrict or object to processing.
1798.120	Maintains policies and procedures for collection and use of children and minors' personal data. Maintains policies and procedures for obtaining valid consent.
1798.125	Maintains policies and procedures for obtaining valid consent.
1798.130	Conducts privacy training reflecting job specific content.
1798.135	Maintains procedures to respond to requests to opt- out of, restrict or object to processing.
1798.145	Maintains procedures to respond to requests for information. Maintains procedures to respond to requests to be forgotten or for erasure of data.

PLANNED PHASES TO COMPLY

Assess	Design	Transform	Operate	Conform

ZINFI OPERATIONS

Assessments and Roadmap	Defined Implementation Path	Process Enhancements Completed	Operational Framework in Place	Ongoing Monitoring and Reporting

ZINFI DELIVERABLES

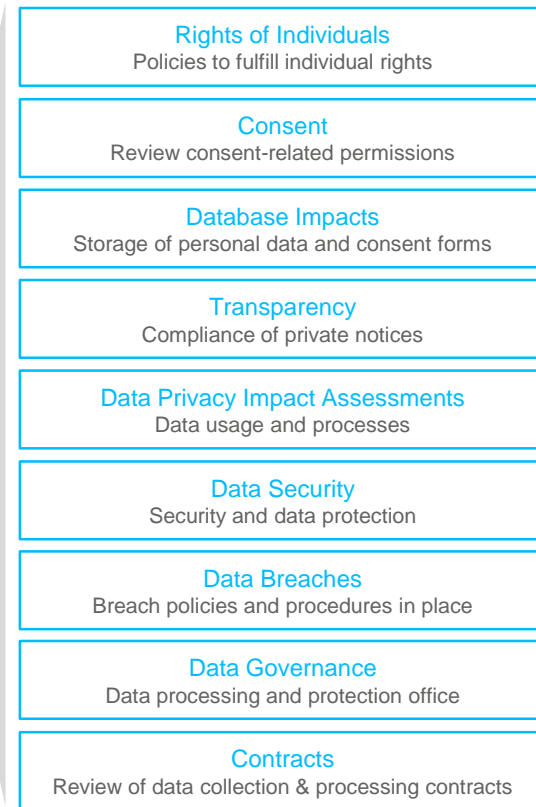| Privacy Impact Assessment	Design of Data Protection Controls	Data Protection Controls implemented	CCPA Integrated approach to Operations	Monitor and Deliver Compliance

1. What **personal data do we collect/store**?

2. Have we obtained it fairly? Do we **have the necessary consent**, and were the data subjects informed of the specific purpose for which we'll use their data? Were we clear and unambiguous about that purpose, and were the data subjects informed of their right to withdraw consent at any time?

3. Are we ensuring **we aren't holding data any longer than is necessary** and we are **keeping it up to date**?

4. Are we **keeping personal data safe and secure** using a level of security appropriate to the risk? Are we limiting access to ensure it is only being used for its intended purpose?

5. Are we collecting or processing any special categories of personal data, such as **sensitive personal data, children's data, biometric or genetic data**, etc.—and if so, are we meeting the standards to collect, process and store it?

6. Have we implemented a **policy of "data protection by design and default"** to ensure we're systematically considering the potential impact that a project or initiative might have on the privacy of individuals?

7. Do we have **procedures in place to handle requests from data subjects to modify, delete or access their personal data**? Do these procedures comply with the rules under the CCPA?

8. Do we have **security notification procedures** in place to ensure we meet our enhanced reporting obligations under the CCPA in case of a data breach in a timely manner?

9. Are our **staff trained in all areas of CCPA data privacy** to ensure they handle data in a compliant manner?

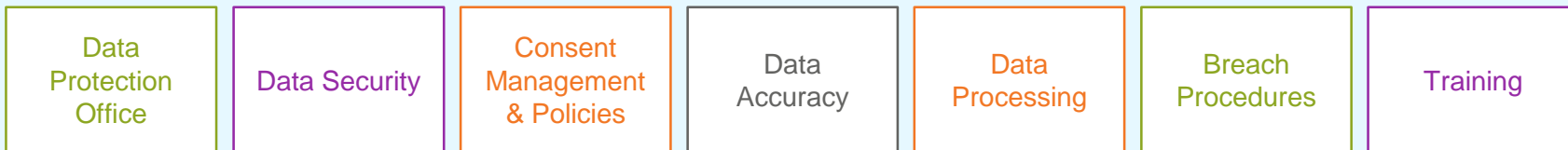10. Do we **review and audit the data** we hold on a regular basis?

CCPA - Compliance Road Map

1 Discover
Identify what personal data you have and where it resides

2 Control
Manage how personal data is used and accessed

3 Protect
Establish security controls to prevent, detect and respond to vulnerabilities and data breaches

4 Report
Act on data subject requests, consents and required documentation

5 Review
Analyze your data and systems, stay compliant and reduce risk

California Consumer Privacy Act

CCPA Ready

Rights of Individuals
Policies to fulfill individual rights

Consent
Review consent-related permissions

Database Impacts
Storage of personal data and consent forms

Transparency
Compliance of private notices

Data Privacy Impact Assessments
Data usage and processes

Data Security
Security and data protection

Data Breaches
Breach policies and procedures in place

Data Governance
Data processing and protection office

Contracts
Review of data collection & processing contracts

ZINFI's Seven-Factor CCPA Commitment

| Data Protection Office | Data Security | Consent Management & Policies | Data Accuracy | Data Processing | Breach Procedures | Training |

Operational Security
- Intrusion Detection
- Reducing Insider Risk
- Safe Employee Devices & Credentials
- Safe Software Development

User Identity & Storage
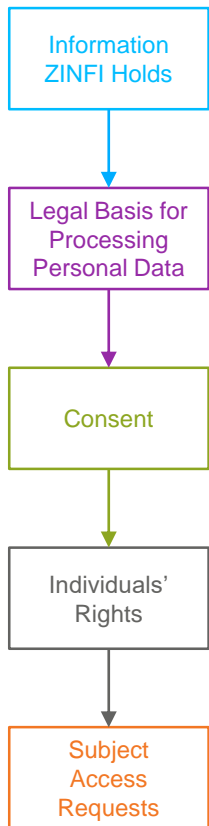- Authentication
- Login Abuse Protection
- Encryption

Internet Communication
- Network Security
- DoS Protection
- User Authentication

Service Deployment
- Access Management of End User Data
- Encryption of Inter-Service Communication
- Inter-Service Access Management
- Service Identity, Integrity, Isolation

Information ZINFI Holds

↓

Legal Basis for Processing Personal Data

↓

Consent

↓

**Individuals' Rights**

↓

Subject Access Requests

Consent Management

ZINFI establishes:
- Not only simple consent-obtaining procedures, but also demonstrates that the data subject has consented to processing of his/her data; records stored for fingertip access.
- Consent requests in the context of a written declaration are presented in an intelligible and easily accessible form, using clear and plain language. "Do Not Sell My Personal Information" Policy is presented transparently..
- Requests for consent conforms to the use of the service for which it is collected. The following are clearly defined and mailed to CA clients, prior to processing:
  - Why we collect the specific information
  - What we do with it
  - How long we keep it
  - How we destroy/retain it
  - How individuals can access the information you hold on them
  - Right to be forgotten information: data subject's right to withdraw consent at any time; the process for withdrawing consent should be just as easy as that for giving consent
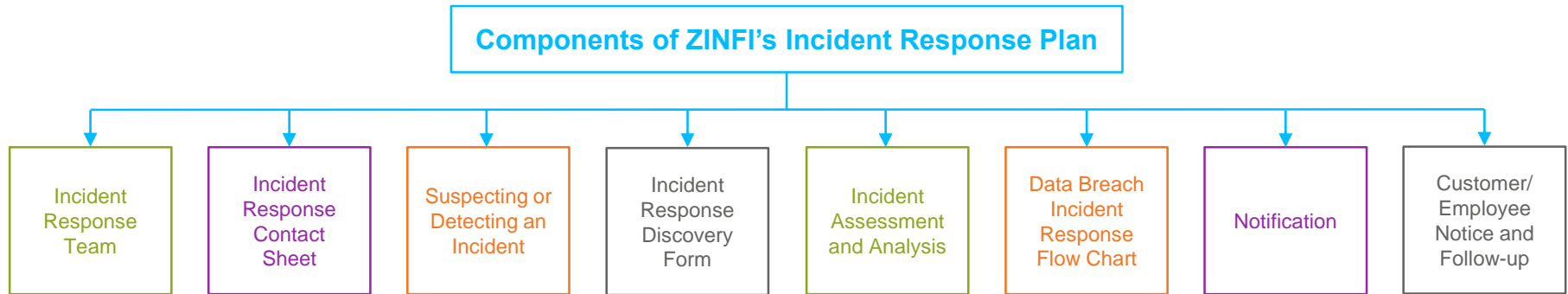
Implementing Procedures

- Privacy policies defined and revised for CCPA and undertaken by organization
- Marketing data protection policy (rulebook on filtering and sending customer offers)
- HR employee data protection policy (consent management of employees/associates for internal processing activities)
- Disagreement to consent policy (withdrawal management)
- Data retention policy/agreement
- Cookie usage and acceptance policy (defines data subject tracking consent, if any)

System Data Flow
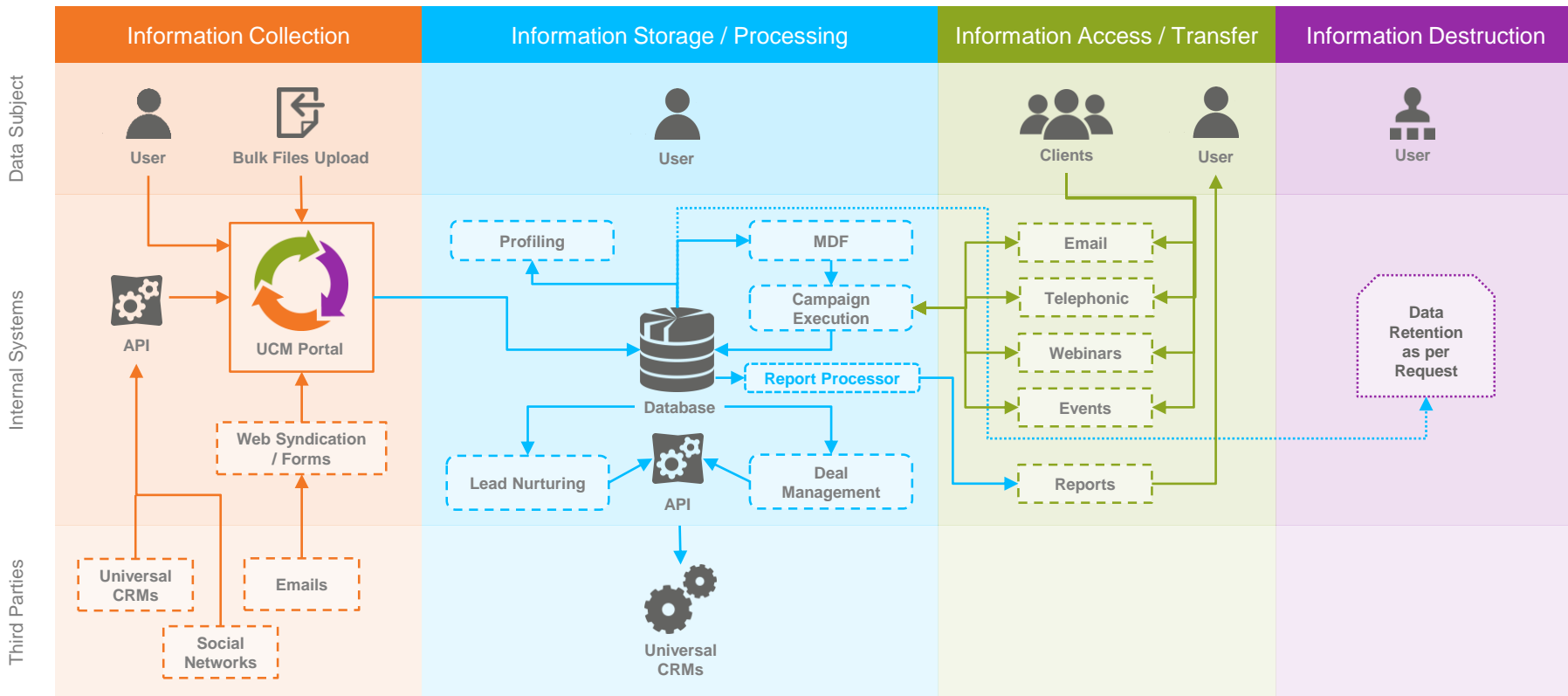
Maintenance of data breach incident response plan

1. Aims to reduce the exposure of organizations, customers/ employees and partners that arises from a data theft or data loss incident
2. Specifically includes policies and procedures to:
   - Assess the nature and scope of an incident, and identify what customer information systems and types of customer/employee information have been accessed or misused
   - Contain and control the incident to prevent further unauthorized access to, or misuse of, customer information, while preserving records and other evidence
   - Notify appropriate entities (data subjects, legal departments, etc.) about breach
   - Maintain or restore business continuity

Components of ZINFI's Incident Response Plan

| Incident Response Team | Incident Response Contact Sheet | Suspecting or Detecting an Incident | Incident Response Discovery Form | Incident Assessment and Analysis | Data Breach Incident Response Flow Chart | Notification | Customer/ Employee Notice and Follow-up |

The CCPA compliance parameters requires workforce privacy awareness training.

There are three types of training that are conducted by ZINFI:

- **General workforce privacy awareness training** – basic privacy awareness for the entire workforce.
- **Training about CCPA** – training that introduces select employee groups to CCPA (i.e., employees who need to know more about how CCPA works).
- **Role-based training** – training for specific roles in organizations, such as managing products and services for privacy or vendor management. Some individuals will require more specialized training about new responsibilities they will have under CCPA. We offer courses for specific, role-based privacy training.

Training deliverables:

Overview	Principles	Rights	Responsibilities
• What is data protection? • Who does CCPA apply to? • What does CCPA apply to? • Non-compliance and fines • Knowledge check	• Principles of CCPA • Lawfulness • Accountability • Policies • Data privacy	• Individual rights • Data subjects and rights • B2B/B2C rights • Reporting rights • Obligations of data controllers and processors	• CCPA compliance dos and don'ts • Breach notification • Roles of data security • Conclusion • Assessment

CCPA Conformance

Conducting Conformance Assessments and Registering:

Determine key metrics to measure privacy program
- Define conformation "success" for privacy program
- Determine metrics to assess privacy program and how they will be collected

→

Description of Data Flows
- Type of data
- Use of data
- Recorded in a flowchart
- Preparation of information asset register

→

Identifying Privacy Risks
- Apply the data protection principles
- Individual risks
- Compliance risks
- Preparation of risk register

→

Identification of Privacy Solutions
- Accept
- Reduce
- Eliminate
- Review Privacy Policies
- Maintain privacy inbox and respond to consumer requests

→

Registering outcomes
- Document status of each risk
- Identify risk objects
- Prepare final report
- Publish final report

Probable risks and ZINFI remedies:

Inability to meet CCPA requirements as part of regulatory audit	Reputation damage due to poor data policies	Data not properly safeguarded against loss, theft or unauthorized access	Non-adherence to the core principles of processing personal data	Data controllers / processors not aware of changes to obligations	Inappropriate use of a data subject's information
• ZINFI establishes data is held in a secure format; employee understanding of and compliance with CCPA obligations; evidence of data process control	• ZINFI ensures CCPA policies are kept up to date by scheduling automated reviews by appropriate personnel	• ZINFI employees understand the security requirements for how data should be stored and accessed; apply restrictions to data to control use	• ZINFI documents CCPA policies; captures electronic attestation; tracks compliance against deadlines; generates real-time compliance reports	• ZINFI employees have access to the latest version of procedures to CCPA policies; monitors employee understanding of their obligations	• ZINFI ensures that appropriate permissions are in place to allow data processors to use the data in the required fashion; ensures that data is current and valid

ZINFI Technologies, Inc.
6200 Stoneridge Mall Road, Suite 300
Pleasanton, CA 94588

sales@zinfitech.com