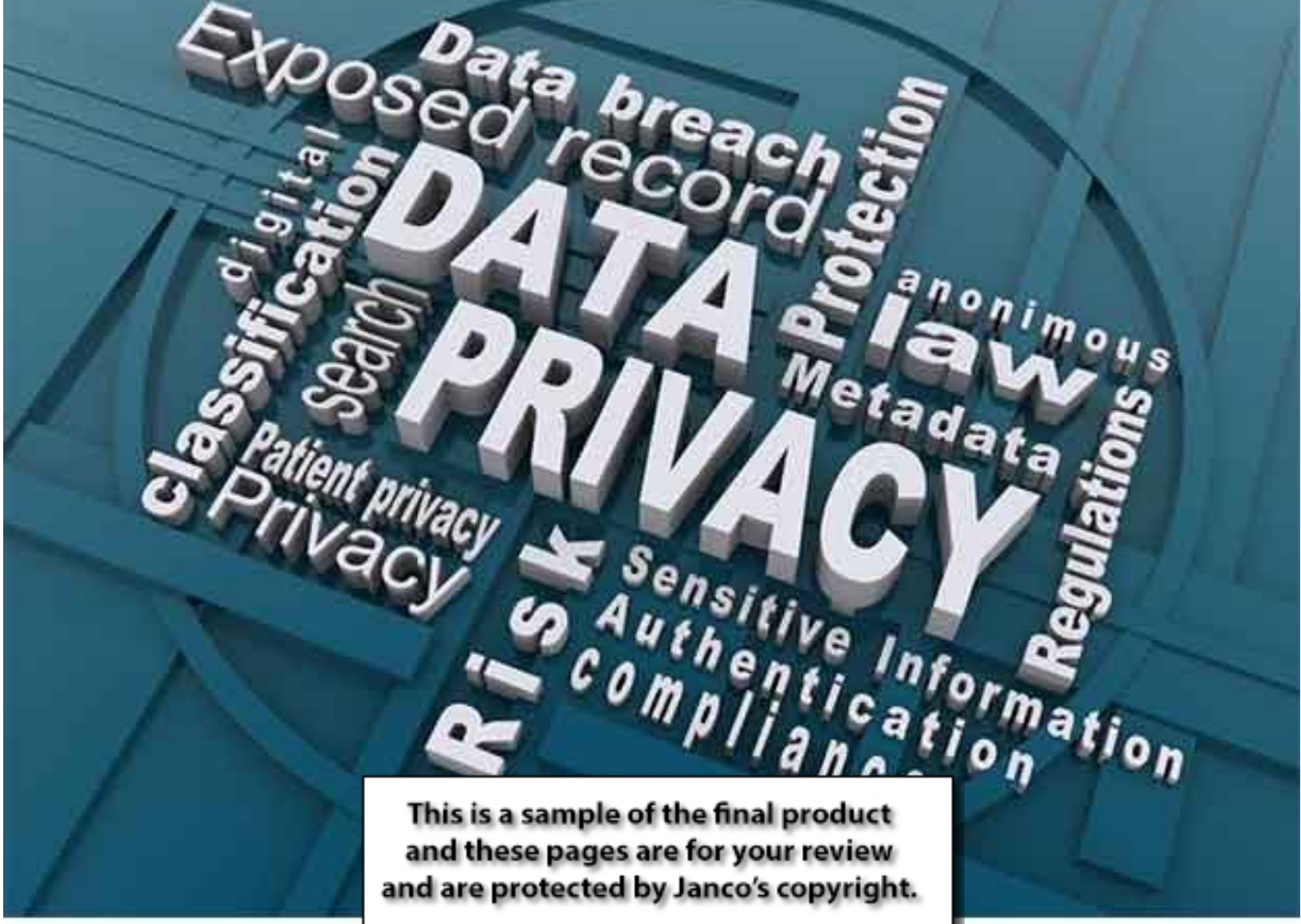

Privacy Compliance Policy

Janco Associates

2025

Table of Contents

Privacy Compliance Policy – U.S. and EU-Mandated Requirements

Overview

Mandated privacy requirements are designed to protect the individual's privacy from unwarranted invasion, to make sure that personal information in possession of an entity is properly used, and to prevent any potential misuse of personal information in the possession of that entity. This policy establishes the processes and procedures, and assigns responsibilities, for fulfilling mandated privacy requirements.

The Chief Security Officer or delegate must approve all processing activities at ENTERPRISE associated with information (data) that falls within mandated privacy requirements. This information includes but is not limited to customer identification data, contact information, email addresses, social security numbers, credit card numbers, credit card expiration dates, security codes, passwords, customer names, customer numbers, ENTERPRISE proprietary data, and any other data (i.e. California Personal ID number).

This policy applies to the entire enterprise, its vendors, its suppliers (including outsourcers), and co-location providers and facilities regardless of the methods used to store and retrieve this information (e.g. online processing, outsourced to a third party, Internet, Intranet, or swipe terminals).

All processing, storage, and retrieval activities for this information must maintain strict access control standards and the Chief Security Officer mandates these specific policies be followed.

Right to Privacy

The right to privacy has been defined in two major pieces of legislation – one for the EU (GDPR) and the other in the California Privacy Act:

bout them.

isclosed and to whom.

ivacy rights.

The definition of the sp l individuals capturing, viewing, or using consumer data need to follow the rules and guidelines to meet the Privacy Compliance Mandates.

California Consumer Privacy Act

Under the California Consumer Privacy Act, the following set of privacy requirements are mandated: and policies are to be followed.

Consumer's Right to Know Information that Has Been Captured

1. A consumer shall have the right to request that an Enterprise that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.
2. An Enterprise that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. An Enterprise shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.
3. An Enterpr umer only upon receipt of a verifiable
4. An Enterpr ccess personal informatio he consumer, the personal in d by mail or electronically, and if prov extent technically feasible, a readily us o another entity without hindrance. y time but shall not be required to provide personal information to a consumer more than twice in 12 months.
5. This section shall not require An Enterprise to retain any personal information collected for a single, one-time transaction if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.
   (1) Retain any personal information collected for a single, one-time transaction, if the information is not sold or retained by the business.
   (2) Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

Consumer's Right to Have Data Removed

1. A consumer shall have the right to request that An Enterprise delete any personal information about the consumer that the business has collected from the consumer.
2. An Enterprise that collects personal information about consumers shall disclose the consumer's rights to request the deletion of the consumer's personal information.
3. An Enterprise that receives a verifiable request from a consumer to delete the consumer's personal information according to subdivision (a) of this section shall delete the consumer's personal information
onsumer's personal information from their

ply with a consumer's request to delete
usiness or service provider to maintain the

on was collected, provide a good or service
in the context of An Enterprise's ongoing
orm 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.

(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.

- If there are no standard PCI DSS processes in place and each store is responsible for its processes, then the sample size must be larger to ensure that each store understands and implements PCI DSS requirements appropriately.

	Data Element	Storage Permitted	Protection Required	PCI DSS Requirement 3.4
Cardholder Data	Primary Account Number	Yes	Yes	Yes
Sensitive Authentication Data**				

* These data elements must be protected if stored in conjunction with the PAN (Primary Account Number). This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data or proper disclosure of a company's practices if consumer-related personal data is being collected during the business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

** Sensitive authentication data must not be stored after authorization (even if encrypted).

Appendix

Forms

Attached are forms that are in the subdirectory titled forms

Privacy Compliance Policy Acceptance Agreement

Job Descriptions

Attached are job descriptions which are in the subdirectory titled Job Descriptions

- Chief Security Officer
- Data Protection Officer
- Manager Compliance
- Manager Security and Workstations
- Security Architect

Privacy and Security Compliance Implementation Work Plan

The privacy and security compliance process to meet the EU's GDPR and California's CCPA is a multi-step process involving both the IT function and the enterprise's operations movement. The focus is on the two prongs of GDPR and CCPA compliance mandates – privacy and security.

Define where the enterprise is and the issues it faces.

Define privacy requirements

1. Review existing privacy policies and statements and document how they compare with GDPR and
2. rect, delete, and transfer personal data
3. d systems

[illegible]

1. tify gaps, benchmark maturity, and establish conformance roadmaps
2. Identify potential vulnerabilities, supporting security and privacy by design
3. Discover and classify personal data assets and affected systems in preparation for designing security controls

Define what must be done

Document privacy requirements

1. Create a work plan that details your GDPR and CCPR remediation and implementation activities
2. Design the policies, business processes, and supporting technologies you'll need to implement your plans
3. Create a GDPR and CCPR reference architecture
4. Evaluate compliance governance processes

Document security requirements

1. Develop a security remediation and implementation plan
2. Define a security reference architecture
3. Define technical and Key Performance Indicators (KPIs) to reduce risk, including encryption, pseudonymization, access control, and monitoring.

What's New

2025

- Reviewed and updated mandated compliance requirements.
- Updated all the attached electronic forms to meet the most current version.
- Updated all the attached job descriptions to meet the latest requirements.

2024

- Reviewed and updated mandated compliance requirements.
- Updated all the attached electronic forms to meet the most current version.
- Updated all the attached job descriptions to meet the latest requirements.

2023

- Updated the User Bill of Rights
- Updated all the attached electronic forms to meet the most current version.
- Updated all the attached job descriptions to meet the latest requirements.

2022

- Updated the User Bill of Rights
- Updated all the attached electronic forms to meet the most current version
- Updated all the attached job descriptions to meet the latest requirements

2021

- Updated to meet the latest compliance requirements
- Updated all the attached electronic forms to meet the most current version
- Updated all the attached job descriptions to meet the latest requirements

2020

- Updated to meet the latest compliance requirements
- Updated all the attached electronic forms to meet the most current version
- Updated all the attached job descriptions to meet the latest requirements