



This is a sample of the final product and these pages are for your review and are protected by Janco's copyright.

<https://e-janco.com>

Privacy Compliance Policy



2024



Table of Contents

Privacy Compliance Policy – U.S. and EU Mandated Requirements.....	3
Overview.....	3
Right to Privacy.....	3
California Consumer Privacy Act of 2018.....	4
Consumer’s Right to Know Information that Has Been Captured.....	4
Consumer’s Right to Have Data Removed.....	5
Consumer’s Right to Know How Data is Used.....	6
Consumer’s Rights to Data That is Sold.....	7
Consumer’s Rights for Stopping the Sale of Data.....	8
Consumer’s Rights to Not be Discriminated Due to Opt Out.....	9
Enterprise Reporting Requirements.....	10
Enterprise Internet and WWW requirements.....	12
GDPR.....	13
Why Data is Captured.....	13
User Consent.....	14
Communication.....	15
Third Party Data.....	15
Profiling.....	16
Legacy data.....	16
PCI.....	17
HIPAA.....	20
Gramm-Leach-Bliley (Financial Services Modernization Act of 1999).....	21
Massachusetts 201 CMR 17.00 Data Protection Requirements.....	22
User/Customer Sensitive Information and Privacy Bill of Rights.....	23
Appendix.....	24
Forms.....	24
Privacy Compliance Policy Acceptance Agreement	
Job Descriptions.....	25
Chief Security Officer	
Data Protection Officer	
Manager Compliance	
Manager Security and Workstations	
Security Architect	
Privacy and Security Compliance Implementation Work Plan.....	26
What’s New.....	28



Privacy Compliance Policy US and EU Mandated Privacy Compliance

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

Overview

Mandated privacy requirements are designed to protect the individual's privacy from information in possession of an entity is personal information in the possession of procedures, and assigns responsibilities, for

This is a sample of the final product and these pages are for your review and are protected by Janco's copyright.

<https://e-janco.com>

activities at ENTERPRISE associated with This information includes but is not limited to 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:

- ✚ The right to know what personal information is being collected about them.
- ✚ The right to know whether their personal information is sold or disclosed and to whom.
- ✚ The right to say no to the sale of personal information.
- ✚ The right to access their personal information.
- ✚ The right to equal service and price, even if they exercise their privacy rights.

The definition of the specifics of the legislation and policies necessary to comply follows. All individuals capturing, viewing, or using consumer data need to follow the rules and guidelines to meet the Privacy Compliance Mandates.



Privacy Compliance Policy US and EU Mandated Privacy Compliance

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

**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>

the consumer with notice consistent with this section.

3. An Enterprise shall provide the information specified in subdivision (a) to a consumer only upon receipt of a verifiable consumer request.
4. An Enterprise that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, a readily useable format that allows the consumer to transmit this information to another entity without hindrance. An Enterprise may provide personal information to a consumer at any 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.

se that collects a consumer's personal
specific pieces of personal information the

on shall, at or before the point of collection,
tion to be collected and the purposes for which
terprise shall not collect additional categories
ed for additional purposes without providing



Privacy Compliance Policy US and EU Mandated Privacy Compliance

- 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.

	<i>Data Element</i>	<i>Storage Permitted</i>	<i>Protection Required</i>	<i>PCI DSS Requirement 3.4</i>
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name*	Yes	Yes*	No
	Service Code*	Yes	Yes*	No
	Expiration Date	Yes	Yes*	No
Sensitive Authentication Data**	Full Magnetic Stripe	No	N/A	N/A
	CVC2/CVV2/CID	No	N/A	N/A
	Pin / Pin Block	No	N/A	N/A

* These
consis
exampl
this da
DSS, h

** Ser

**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>

count Number). This protection must be
Additionally, other legislation (for
ity) may require specific protection of
being collected during the business. PCI



Privacy Compliance Policy US and EU Mandated Privacy Compliance

Appendix

Forms

Attached are forms that are in the subdirectory titled forms

Privacy Compliance Policy Acceptance Agreement

**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>



Privacy Compliance Policy US and EU Mandated Privacy Compliance

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

**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>



Privacy Compliance Policy

US and EU Mandated Privacy Compliance

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

This is a sample of the final product and these pages are for your review and are protected by Janco’s copyright.

<https://e-janco.com>

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.



Privacy Compliance Policy US and EU Mandated Privacy Compliance

What's New

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

**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>