CPRA (formerly CCPA) Readiness report for AssistNow Inc

Generated on 11 February 2025

Report summary

This report provides a summary of AssistNow Inc's readiness posture for CPRA (formerly CCPA) compliance as of 11th February 2025. Sprinto continuously monitors the security and readiness posture of AssistNow Inc to ensure you have a transparent view into how they have setup Sprinto to meet industry standards. Below is a list of controls implemented by the organization to meet the compliance requirements. Sprinto achieves this by connecting to the systems, tools and policies of the company, and running continuous checks to determine the health of the controls.

Legend

- Check is healthy
- Check is work in progress

7002

Restrictions on the Collection and Use of Personal Information.

7002(a)

In accordance with Civil Code section 1798.100, subdivision (c), aA business’s collection, use, retention, and/or sharing of a consumer’s personal information shall be reasonably necessary and proportionate to achieve:

INTERNAL CONTROLS AND CHECKS

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically ✓

Control **SDC 72**

Entity has a documented policy and procedures to provide guidelines for Data Protection which includes staff members' responsibilities with handling personal data as per the company's regulatory requirements

Monitored via 1 check

Data Protection Policy ✓

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7002(a)(1)

In accordance with Civil Code section 1798.100, subdivision (c), a business's collection, use, retention, and/or sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve: (1) The purpose(s) for which the personal information was collected or processed, which shall comply with the requirements set forth in subsection (b).

INTERNAL CONTROLS AND CHECKS

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 72**

Entity has a documented policy and procedures to provide guidelines for Data Protection which includes staff members' responsibilities with handling personal data as per the company's regulatory

requirements

Monitored via 1 check

Data Protection Policy

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

7002(a)(2)

In accordance with Civil Code section 1798.100, subdivision (c), a business's collection, use, retention, and/or sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve: (2) Another disclosed purpose that is compatible with the context in which the personal information was collected, which shall comply with the requirements set forth in subsection (c).

INTERNAL CONTROLS AND CHECKS

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 72**

Entity has a documented policy and procedures to provide guidelines for Data Protection which includes staff members' responsibilities with handling personal data as per the company's regulatory requirements

Monitored via 1 check

Data Protection Policy ✓

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map ✓

7002(b)

The purpose(s) for which the personal information was collected or processed shall be consistent with the reasonable expectations of the consumer(s) whose personal information is collected or processed. The consumer's reasonable expectations concerning the purpose for which their personal information will be collected or processed shall be based on the following

INTERNAL CONTROLS AND CHECKS

Control **SDC 19**

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

Monitored via 1 check

Risk assessment should be conducted periodically ✓

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 24**

Entity's Senior Management reviews and approves all company policies annually.

Monitored via 1 check

Policies should be reviewed by senior management	✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 44**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.

Monitored via 5 checks

Staff devices should have antivirus running
Endpoint Security Policy
Asset Management Policy
Physical and Environmental Security Procedure
Asset Management Procedure

Control **SDC 46**

Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.

Monitored via 5 checks

Staff devices should have OS updated
Endpoint Security Policy
Asset Management Policy
Physical and Environmental Security Procedure
Asset Management Procedure

Control **SDC 47**

Entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.

Monitored via 3 checks

Staff devices health should be monitored regularly
Staff devices should have screen lock enabled
Endpoint Security Policy

Control **SDC 48**

Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.

Monitored via 1 check

Media Disposal Policy ✓

Control **SDC 49**

Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.

Monitored via 3 checks

Asset Management Policy ✓
Asset Management Procedure ✓
Encryption Policy ✓

Control **SDC 50**

Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.

Monitored via 3 checks

Asset Management Policy ✓
Network Security Procedure ✓
Asset Management Procedure ✓

Control **SDC 64**

Entity has documented policies and procedures to manage changes to its operating environment.

Monitored via 4 checks

Operation Security Policy	✓
SDLC Procedure	✓
Operations Security Procedure	✓
System Acquisition and Development Lifecycle Policy	✓

Control **SDC 65**

Entity has procedures to govern changes to its operating environment.

Monitored via 3 checks

Operation Security Policy	✓
SDLC Procedure	✓
Operations Security Procedure	✓

Control **SDC 66**

Entity has established procedures for approval when implementing changes to the operating environment.

Monitored via 3 checks

Operation Security Policy	✓
SDLC Procedure	✓
Operations Security Procedure	✓

Control **SDC 67**

Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's

service commitments and system requirements

Monitored via 1 check

Risk Assessment & Management Policy

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

Monitored via 2 checks

Risk assessment should be conducted periodically

Risk Assessment & Management Policy

Control **SDC 72**

Entity has a documented policy and procedures to provide guidelines for Data Protection which includes staff members' responsibilities with handling personal data as per the company's regulatory requirements

Monitored via 1 check

Data Protection Policy

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically ✓

Control **SDC 100**

Entity ensures that customer data used in non-Production environments requires the same level of protection as the production environment.

Monitored via 2 checks

Asset Management Policy ✓

Asset Management Procedure ✓

Control **SDC 104**

Entity has documented policies and procedures for endpoint security and related controls.

Monitored via 3 checks

Endpoint Security Policy ✓

Asset Management Policy ✓

Asset Management Procedure ✓

Control **SDC 108**

Entity uses Sprinto, a continuous monitoring system, to alert the security team to update the access levels of team members whose roles have changed.

Monitored via 3 checks

Access to critical systems should be reviewed

Access Control Procedure

Access Control Policy

Control **SDC 113**

Entity conducts risk assessment of suspected data breaches and any significant data breaches are notified to all affected parties without unreasonable delay.

Monitored via 3 checks

Incidents should be investigated based on severity

Incident Management Procedure

Incident Management Policy

Control **SDC 135**

Entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.

Monitored via 3 checks

Access Control Procedure

Acceptable Usage Policy

Access Control Policy

Control **SDC 393**

Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.

Monitored via 2 checks

Business Continuity Plan ✓

Business Continuity & Disaster Recovery Policy ✓

Control **SDC 392**

Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident

Monitored via 2 checks

Business Continuity Plan ✓

Business Continuity & Disaster Recovery Policy ✓

Control **SDC 58**

Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal

Monitored via 2 checks

Operation Security Policy ✓

Operations Security Procedure ✓

7002(b)(1)

The purpose(s) for which the personal information was collected or processed shall be consistent with the reasonable expectations of the consumer(s) whose personal information is collected or processed. The consumer's reasonable expectations concerning the purpose for which their personal information will be collected or processed shall be based on the following: (1) The relationship between the consumer(s) and the business. For example, if the consumer is intentionally interacting with the business on its website to purchase a good or service, the consumer likely expects that the purpose for collecting or processing the personal information is to provide that good or service. By

contrast, for example, the consumer of a business's mobile flashlight application would not expect the business to collect the consumer's geolocation information to provide the flashlight service.

INTERNAL CONTROLS AND CHECKS

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map 

7002(b)(2)

The purpose(s) for which the personal information was collected or processed shall be consistent with the reasonable expectations of the consumer(s) whose personal information is collected or processed. The consumer's reasonable expectations concerning the purpose for which their personal information will be collected or processed shall be based on the following: (2) The type, nature, and amount of personal information that the business seeks to collect or process. For example, if a business's mobile communication application requests access to the consumer's contact list in order to call a specific individual, the consumer who is providing their contact list likely expects that the purpose of the business's use of that contact list will be to connect the consumer with the specific contact they selected. Similarly, if a business collects the consumer's fingerprint in connection with setting up the security feature of unlocking the device using the fingerprint, the consumer likely expects that the business's use of the consumer's fingerprint is only for the purpose of unlocking their mobile device.

INTERNAL CONTROLS AND CHECKS

Control **SDC 70**

Entity performs physical and/or logical labeling of information systems as per the guidelines documented policy defined for data classification

Monitored via 1 check

Data Classification Policy

Control **SDC 71**

Entity has a documented policy outlining guidelines for the disposal and retention of information.

Monitored via 1 check

Data Retention Policy

Control **SDC 72**

Entity has a documented policy and procedures to provide guidelines for Data Protection which includes staff members' responsibilities with handling personal data as per the company's regulatory requirements

Monitored via 1 check

Data Protection Policy

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

7002(b)(3)

The purpose(s) for which the personal information was collected or processed shall be consistent with the reasonable expectations of the consumer(s) whose personal information is collected or

processed. The consumer’s reasonable expectations concerning the purpose for which their personal information will be collected or processed shall be based on the following: (3) The source of the personal information and the business’s method for collecting or processing it. For example, if the consumer is providing their personal information directly to the business while using the business’s product or service, the consumer likely expects that the business will use the personal information to provide that product or service. However, the consumer may not expect that the business will use that same personal information for a different product or service offered by the business or the business’s subsidiary

INTERNAL CONTROLS AND CHECKS

Control **SDC 70**

Entity performs physical and/or logical labeling of information systems as per the guidelines documented policy defined for data classification

Monitored via 1 check

Data Classification Policy ✓

Control **SDC 71**

Entity has a documented policy outlining guidelines for the disposal and retention of information.

Monitored via 1 check

Data Retention Policy ✓

Control **SDC 72**

Entity has a documented policy and procedures to provide guidelines for Data Protection which includes staff members' responsibilities with handling personal data as per the company's regulatory requirements

Monitored via 1 check

Data Protection Policy ✓

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

7002(b)(4)

The purpose(s) for which the personal information was collected or processed shall be consistent with the reasonable expectations of the consumer(s) whose personal information is collected or processed. The consumer's reasonable expectations concerning the purpose for which their personal information will be collected or processed shall be based on the following: (4) The specificity, explicitness, prominence, and clarity of disclosures to the consumer(s) about the purpose for collecting or processing their personal information, such as in the Notice at Collection and in the marketing materials to the consumer(s) about the business's good or service. For example, the consumer that receives a pop-up notice that the business wants to collect the consumer's phone number to verify their identity when they log in likely expects that the business will use their phone number for the purpose of verifying the consumer's identity and not for marketing purposes. Similarly, the consumer may expect that a mobile application that markets itself as a service that finds cheap gas close to the consumer will collect and use the consumer's geolocation information for that specific purpose when they are using the service.

INTERNAL CONTROLS AND CHECKS

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

7002(b)(5)

The purpose(s) for which the personal information was collected or processed shall be consistent with the reasonable expectations of the consumer(s) whose personal information is collected or processed. The consumer's reasonable expectations concerning the purpose for which their personal information will be collected or processed shall be based on the following: (5) The degree to which the involvement of service providers, contractors, third parties, or other entities in the collecting or processing of personal information is apparent to the consumer(s). For example, the consumer likely expects an online retailer's disclosure of the consumer's name and address to a delivery service provider in order for that service provider to deliver a purchased product, because that service provider's involvement is apparent to the consumer. By contrast, the consumer may not expect the disclosure of personal information to a service provider if the consumer is not directly interacting with the service provider or the service provider's role in the processing is not apparent to the consumer

INTERNAL CONTROLS AND CHECKS

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7002(c)(1)

Whether another disclosed purpose is compatible with the context in which the personal information was collected shall be based on the following: (1) At the time of collection of the personal information, the reasonable expectations of the consumer(s) whose personal information is collected or processed concerning the purpose for which their personal information will be collected or processed, based on the factors set forth in subsection (b)

INTERNAL CONTROLS AND CHECKS

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7002(c)(2)

Whether another disclosed purpose is compatible with the context in which the personal information was collected shall be based on the following: (2) The other disclosed purpose for which the business seeks to further collect or process the consumer’s personal information, including whether it is a Business Purpose listed in Civil Code section 1798.140, subdivisions (e)(1) through (e)(8)

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

7002(c)(3)

Whether another disclosed purpose is compatible with the context in which the personal information was collected shall be based on the following: (3) The strength of the link between subsection (c)(1) and subsection (c)(2). For example, a strong link exists between the consumer's expectations that the personal information will be used to provide them with a requested service at the time of collection, and the use of the information to repair errors that impair the intended functionality of that requested service. This would weigh in favor of compatibility. By contrast, for example, a weak link exists between the consumer's reasonable expectations that the personal information will be collected to provide a requested cloud storage service at the time of collection, and the use of the information to research and develop an unrelated facial recognition service

INTERNAL CONTROLS AND CHECKS

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7002(d)

For each purpose identified in subsection (a)(1) or (a)(2), the collection, use, retention, and/or sharing of a consumer's personal information to achieve that purpose shall be reasonably necessary and proportionate. The business's collection, use, retention, and/or sharing of a consumer's personal information shall also be reasonably necessary and proportionate to achieve any purpose for which the business obtains the consumer's consent in compliance with subsection (e). Whether a business's collection, use, retention, and/or sharing of a consumer's personal information is reasonably necessary and proportionate to achieve the purpose identified in subsection (a)(1) or (a)(2), or any purpose for which the business obtains consent, shall be based on the following:

INTERNAL CONTROLS AND CHECKS

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map ✓

7002(d)(1)

(1) The minimum personal information that is necessary to achieve the purpose identified in subsection (a)(1) or (a)(2), or any purpose for which the business obtains consent. For example, to complete an online purchase and send an email confirmation of the purchase to the consumer, an online retailer may need the consumer's order information, payment and shipping information, and email address.

INTERNAL CONTROLS AND CHECKS

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

7002(d)(2)

(2) The possible negative impacts on consumers posed by the business's collection or processing of the personal information. For example, a possible negative impact of collecting precise geolocation information is that it may reveal other sensitive personal information about the consumer, such as health information based on visits to healthcare providers.

INTERNAL CONTROLS AND CHECKS

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

7002(d)(3)

The existence of additional safeguards for the personal information to specifically address the possible negative impacts on consumers considered by the business in subsection (d)(2). For example, a business may consider encryption or automatic deletion of personal information within a specific window of time as potential safeguards.

INTERNAL CONTROLS AND CHECKS

Control **SDC 11**

Entity systems generate information that is reviewed and evaluated to determine impacts on the functioning of internal controls.

Monitored via 2 checks

Asset Management Policy	✓
Asset Management Procedure	✓

Control **SDC 19**

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

Monitored via 1 check

Risk assessment should be conducted periodically	✓

Control **SDC 20**

Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.

Monitored via 1 check

Risk assessment should be conducted periodically	✓

Control **SDC 22**

Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.

Monitored via 1 check

Information security officer should be assigned

Control **SDC 23**

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

Monitored via 1 check

Internal Audit

Control **SDC 24**

Entity's Senior Management reviews and approves all company policies annually.

Monitored via 1 check

Policies should be reviewed by senior management

Control **SDC 25**

Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

Monitored via 3 checks

Management Review of Internal Audit

Senior management should be assigned

Compliance Policy

Control **SDC 26**

Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.

Monitored via 3 checks

- Organization chart should be reviewed by senior management ✓
- HR Security Procedure ✓
- HR Security Policy ✓

Control **SDC 27**

Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.

Monitored via 2 checks

- Risk assessment should be reviewed by senior management ✓
- Risk Assessment & Management Policy ✓

Control **SDC 28**

Entity's Infosec officer reviews and approves the list of people with access to production console annually

Monitored via 1 check

- Access to critical systems should be reviewed ✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

- Vendor risk assessment should be reviewed by senior management ✓
- Vendor Management Policy ✓
- Vendor Management Procedure ✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 31**

Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.

Monitored via 1 check

Org policy should be defined	✓

Control **SDC 32**

Entity's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers.

Monitored via 4 checks

Org chart should be maintained	✓
Compliance Policy	✓
Compliance Procedure	✓
Information Security Policy	✓

Control **SDC 44**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.

Monitored via 5 checks

Staff devices should have antivirus running	✓
Endpoint Security Policy	✓
Asset Management Policy	✓
Physical and Environmental Security Procedure	✓
Asset Management Procedure	✓

Control **SDC 45**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.

Monitored via 2 checks

Staff devices should have disk encryption enabled	✓
Endpoint Security Policy	✓

Control **SDC 46**

Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.

Monitored via 5 checks

Staff devices should have OS updated	✓
Endpoint Security Policy	✓
Asset Management Policy	✓

Physical and Environmental Security Procedure

Asset Management Procedure

Control **SDC 47**

Entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.

Monitored via 3 checks

Staff devices health should be monitored regularly

Staff devices should have screen lock enabled

Endpoint Security Policy

Control **SDC 48**

Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.

Monitored via 1 check

Media Disposal Policy

Control **SDC 49**

Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.

Monitored via 3 checks

Asset Management Policy

Asset Management Procedure

Encryption Policy

Control **SDC 50**

Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.

Monitored via 3 checks

Asset Management Policy	✓
Network Security Procedure	✓
Asset Management Procedure	✓

Control **SDC 51**

Entity has set up processes to utilize standard encryption methods, including HTTPS with the TLS algorithm, to keep transmitted data confidential.

Monitored via 1 check

Production systems should be secured with HTTPS	✓

Control **SDC 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

Monitored via 2 checks

Incident Management Procedure	✓
Incident Management Policy	✓

Control **SDC 54**

Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.

Monitored via 1 check

Incidents should be investigated based on severity

Control **SDC 59**

Entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives and verifies the integrity of these backups.

Monitored via 3 checks

Operation Security Policy

Business Continuity Plan

Operations Security Procedure

Control **SDC 64**

Entity has documented policies and procedures to manage changes to its operating environment.

Monitored via 4 checks

Operation Security Policy

SDLC Procedure

Operations Security Procedure

System Acquisition and Development Lifecycle Policy

Control **SDC 65**

Entity has procedures to govern changes to its operating environment.

Monitored via 3 checks

Operation Security Policy

SDLC Procedure

Operations Security Procedure

Control **SDC 66**

Entity has established procedures for approval when implementing changes to the operating environment.

Monitored via 3 checks

Operation Security Policy

SDLC Procedure

Operations Security Procedure

Control **SDC 67**

Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements

Monitored via 1 check

Risk Assessment & Management Policy

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

Monitored via 2 checks

Risk assessment should be conducted periodically

Risk Assessment & Management Policy

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map	✓

Control **SDC 100**

Entity ensures that customer data used in non-Production environments requires the same level of protection as the production environment.

Monitored via 2 checks

Asset Management Policy	✓
Asset Management Procedure	✓

Control **SDC 104**

Entity has documented policies and procedures for endpoint security and related controls.

Monitored via 3 checks

Endpoint Security Policy	✓
Asset Management Policy	✓
Asset Management Procedure	✓

Control **SDC 108**

Entity uses Sprinto, a continuous monitoring system, to alert the security team to update the access levels of team members whose roles have changed.

Monitored via 3 checks

Access to critical systems should be reviewed	✓
Access Control Procedure	✓
Access Control Policy	✓

Control **SDC 113**

Entity conducts risk assessment of suspected data breaches and any significant data breaches are notified to all affected parties without unreasonable delay.

Monitored via 3 checks

Incidents should be investigated based on severity	✓
Incident Management Procedure	✓
Incident Management Policy	✓

Control **SDC 135**

Entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.

Monitored via 3 checks

Access Control Procedure	✓
Acceptable Usage Policy	✓
Access Control Policy	✓

Control **SDC 141**

Entity requires that all critical endpoints are encrypted to protect them from unauthorized access.

Monitored via 7 checks

Staff devices should have disk encryption enabled
Staff devices health should be monitored regularly
Endpoint Security Policy
Asset Management Policy
Physical and Environmental Security Procedure
Asset Management Procedure
Acceptable Usage Policy

Control **SDC 154**

Entity has set up mechanisms to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.

Monitored via 1 check

Infrastructure operations person should be assigned

Control **SDC 393**

Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.

Monitored via 2 checks

Business Continuity Plan
Business Continuity & Disaster Recovery Policy

Control **SDC 395**

Entity has documented policies and procedures to facilitate the implementation of personnel security.

Monitored via 2 checks

HR Security Procedure	✓
HR Security Policy	✓

Control **SDC 396**

Entity appoints a People Operations Officer to develop and drive all personnel-related security strategies.

Monitored via 2 checks

People operations person should be assigned	✓
HR Security Policy	✓

Control **SDC 397**

Entity appoints a Compliance Program Manager who is delegated the responsibility of planning and implementing the internal control environment.

Monitored via 3 checks

Compliance program manager should be assigned	✓
Compliance Policy	✓
Compliance Procedure	✓

Control **SDC 431**

Entity has established policies and procedures to help identify and deal with legal, regulatory, and contractual compliance including facilitating relevant audits to review compliance status.

Monitored via 2 checks

Compliance Procedure	✓

Compliance Policy

Control **SDC 432**

Entity outlines and documents cybersecurity responsibilities for all personnel.

Monitored via 1 check

Organization of Information Security Policy

Control **SDC 433**

Entity has documented policy and procedures which provides guidance on integrating privacy principles into the design process that help in complying with privacy regulations.

Monitored via 1 check

Privacy By Design Policy

Control **SDC 392**

Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident

Monitored via 2 checks

Business Continuity Plan

Business Continuity & Disaster Recovery Policy

Control **SDC 58**

Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal

Monitored via 2 checks

Operation Security Policy

Operations Security Procedure

Control SDC 119

Entity has documented guidelines to manage communications protections and network security of critical systems.

Monitored via 2 checks

Network Security Procedure

Communications & Network Security Policy

7010

Overview of Required Disclosures.

7010(a)

Every business that must comply with the CCPA and these regulations shall provide a privacy policy in accordance with the CCPA and section 7011.

INTERNAL CONTROLS AND CHECKS

Control SDC 2

Entity maintains an organizational structure to define authorities, facilitate information flow and establish responsibilities.

Monitored via 5 checks

Org chart should be maintained

Access Control Procedure

HR Security Procedure

HR Security Policy

Access Control Policy

Control **SDC 3**

Entity has established procedures to communicate with staff about their roles and responsibilities.

Monitored via 3 checks

Organization roles and JDs should be validated

HR Security Procedure

HR Security Policy

Control **SDC 5**

Entity has established procedures to perform security risk screening of individuals before authorizing access.

Monitored via 3 checks

Background checks should be conducted for new employees

HR Security Procedure

HR Security Policy

Control **SDC 6**

Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.

Monitored via 1 check

Policies should be acknowledged by onboarded staff

Control SDC 11

Entity systems generate information that is reviewed and evaluated to determine impacts on the functioning of internal controls.

Monitored via 2 checks

Asset Management Policy

Asset Management Procedure

Control SDC 12

Entity has established procedures for staff to acknowledge applicable company policies periodically.

Monitored via 2 checks

Policies should be acknowledged by onboarded staff

Staff should periodically acknowledge policies

Control SDC 19

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

Monitored via 1 check

Risk assessment should be conducted periodically

Control SDC 24

Entity's Senior Management reviews and approves all company policies annually.

Monitored via 1 check

Policies should be reviewed by senior management

Control **SDC 25**

Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

Monitored via 3 checks

Management Review of Internal Audit

Senior management should be assigned

Compliance Policy

Control **SDC 16**

Entity has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the Entity in the event there are problems.

Monitored via 1 check

Customer support page should be available

Control **SDC 31**

Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.

Monitored via 1 check

Org policy should be defined

Control **SDC 64**

Entity has documented policies and procedures to manage changes to its operating environment.

Monitored via 4 checks

Operation Security Policy	✓
SDLC Procedure	✓
Operations Security Procedure	✓
System Acquisition and Development Lifecycle Policy	✓

Control **SDC 67**

Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements

Monitored via 1 check

Risk Assessment & Management Policy	✓

Control **SDC 1**

Entity has a documented policy to define behavioral standards and acceptable business conduct.

Monitored via 1 check

Code of Business Conduct Policy	✓

Control **SDC 15**

Entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.

Monitored via 1 check

Information Security Policy

Control SDC 18

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

Monitored via 2 checks

Risk assessment should be conducted periodically

Risk Assessment & Management Policy

Control SDC 4

Entity has procedures to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.

Monitored via 3 checks

Hiring evaluation of new employee should be recorded

HR Security Procedure

HR Security Policy

Control SDC 9

Entity requires that all employees in client serving, IT, Engineering, and Information Security roles are periodically evaluated regarding their job responsibilities.

Monitored via 3 checks

Staff Performance Evaluations

HR Security Procedure

HR Security Policy

Control **SDC 381**

Entity has documented policies and procedures to manage physical and environmental security.

Monitored via 2 checks

Physical and Environmental Security Procedure

Physical & Environmental Security Policy

Control **SDC 382**

Entity has documented policy and procedures for physical and/or logical labeling of information via documented policy for data classification.

Monitored via 1 check

Data Classification Policy

Control **SDC 389**

Entity periodically updates and reviews the inventory of systems as a part of installations, removals, and system updates.

Monitored via 3 checks

Internal Audit

Asset Management Policy

Asset Management Procedure

Control **SDC 390**

Entity develops, documents, and maintains an inventory of organizational endpoint systems, including all necessary information to achieve accountability.

Monitored via 3 checks

Staff devices health should be monitored regularly	
Endpoint Security Policy	✓
Asset Management Procedure	✓

Control **SDC 391**

Entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.

Monitored via 2 checks

Operation Security Policy	✓
Operations Security Procedure	✓

Control **SDC 393**

Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.

Monitored via 2 checks

Business Continuity Plan	✓
Business Continuity & Disaster Recovery Policy	✓

Control **SDC 394**

Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.

Monitored via 2 checks

Operation Security Policy ✓

Operations Security Procedure ✓

Control **SDC 395**

Entity has documented policies and procedures to facilitate the implementation of personnel security.

Monitored via 2 checks

HR Security Procedure ✓

HR Security Policy ✓

Control **SDC 396**

Entity appoints a People Operations Officer to develop and drive all personnel-related security strategies.

Monitored via 2 checks

People operations person should be assigned ✓

HR Security Policy ✓

Control **SDC 397**

Entity appoints a Compliance Program Manager who is delegated the responsibility of planning and implementing the internal control environment.

Monitored via 3 checks

Compliance program manager should be assigned ✓

Compliance Policy ✓

Compliance Procedure

Control **SDC 398**

Entity has a documented ISMS scope that defines which information and information assets the organization intends to protect.

Monitored via 4 checks

ISMS Scope Document

Compliance Procedure

Compliance Policy

Information Security Policy

Control **SDC 399**

Entity has a documented ISMS Manual which provides a framework that the organization can use to develop, implement, and maintain an effective information security management system.

Monitored via 5 checks

Compliance Procedure

ISMS Manual

Compliance Policy

Information Security Policy

ISMS Information Security Roles & Responsibilities

Control **SDC 433**

Entity has documented policy and procedures which provides guidance on integrating privacy principles into the design process that help in complying with privacy regulations.

Monitored via 1 check

Privacy By Design Policy

Control **SDC 392**

Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident

Monitored via 2 checks

Business Continuity Plan

Business Continuity & Disaster Recovery Policy

7002

Restrictions on the Collection and Use of Personal Information

7002(e)

A business shall obtain the consumer's consent in accordance with section 7004 before collecting or processing, personal information for any purpose that does not meet the requirements set forth in subsection (a).

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7002(f)

A business shall not collect categories of personal information other than those disclosed in its Notice at Collection in accordance with the CCPA and section 7012. If the business intends to collect additional categories of personal information or intends to use the personal information for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected, the business shall provide a new Notice at Collection. However, any additional collecting or processing of personal information shall comply with subsection (a).

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7014

Notice of Right to Limit and the “Limit the Use of My Sensitive Personal Information” Link.

7014(a)

The purpose of the Notice of Right to Limit is to inform consumers of their right to limit a business’s use and disclosure of their sensitive personal information and to provide them with the opportunity to exercise that right. The purpose of the “Limit the Use of My Sensitive Personal Information” link is to immediately effectuate the consumer’s right to limit, or in the alternative, direct the consumer to the Notice of Right to Limit. Accordingly, clicking the business’s “Limit the Use of My Sensitive Personal Information” link will either have the immediate effect of limiting the use and disclosure of the consumer’s sensitive personal information or lead the consumer to a webpage where the consumer can learn about and make that choice.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

7014(b)

The Notice of Right to Limit shall comply with section 7003, subsections (a) and (b).

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7014(c)

The “Limit the Use of My Sensitive Personal Information” link shall be a conspicuous link that complies with section 7003, subsections (c) and (d), and is located at either the header or footer of the business’s internet Homepage(s).

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

7014(d)

In lieu of posting the “Limit the Use of My Sensitive Personal Information” link, a business may provide the Alternative Opt-out Link in accordance with section 7015. The business shall still post a Notice of Right to Limit in accordance with these regulations.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7014(e)

A business that uses or discloses a consumer's sensitive personal information for purposes other than those specified in section 7027, subsection (m), shall provide the Notice of Right to Limit to

consumers as follows:

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7014(e)(1)

A business that uses or discloses a consumer's sensitive personal information for purposes other than those specified in section 7027, subsection (m), shall provide the Notice of Right to Limit to consumers as follows: (1) A business shall post the Notice of Right to Limit on the internet webpage to which the consumer is directed after clicking on the "Limit the Use of My Sensitive Personal Information" link. The notice shall include the information specified in subsection (f) or be a link that takes the consumer directly to the specific section of the business's privacy policy that contains the same information. If clicking on the "Limit the Use of My Sensitive Personal Information" link immediately effectuates the consumer's right to limit, the business shall provide the notice within its privacy policy.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control SDC 144

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7014(e)(2)

A business that uses or discloses a consumer's sensitive personal information for purposes other than those specified in section 7027, subsection (m), shall provide the Notice of Right to Limit to consumers as follows: (2) A business that does not operate a website shall establish, document, and comply with another method by which it informs consumers of their right to limit. That method shall comply with the requirements set forth in section 7003.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 76

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7014(f)

A business shall include the following in its Notice of Right to Limit

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7014(f)(1)

A business shall include the following in its Notice of Right to Limit (1) A description of the consumer's right to limit;

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7014(f)(2)

A business shall include the following in its Notice of Right to Limit (2) Instruction on how the consumer can submit a request to limit. If notice is provided online, the notice shall include the interactive form by which the consumer can submit their request to limit online, as required by section 7027, subsection (b)(1). If the business does not operate a website, the notice shall explain the offline method by which the consumer can submit their request to limit.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7014(g)(1)

A business does not need to provide a Notice of Right to Limit or the “Limit the Use of My Sensitive Personal Information” link if: (1) It only uses and discloses sensitive personal information that it collected about the consumer for the purposes specified in section 7027, subsection (m), and states so in its privacy policy; or

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control SDC 144

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7014(g)(2)

A business does not need to provide a Notice of Right to Limit or the “Limit the Use of My Sensitive Personal Information” link if: (2) It only collects or processes sensitive personal information without the purpose of inferring characteristics about a consumer, and states so in its privacy policy

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 76

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7014(h)

(A business shall not use or disclose sensitive personal information it collected during the time the business did not have a Notice of Right to Limit posted for purposes other than those specified in section 7027, subsection (m), unless it obtains the consent of the consumer.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7010

Overview of Required Disclosures.

7010(c)

Except as set forth in section 7025, subsection (g), a business that sells or shares personal information shall provide a Notice of Right to Opt-out of Sale/Sharing or the Alternative Opt-out Link in accordance with the CCPA and sections 7013 and 7015.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 76

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7010(d)

A business that uses or discloses a consumer's sensitive personal information for purposes other than those specified in section 7027, subsection (m), shall provide a Notice of Right to Limit or the aAlternative Opt-out Link in accordance with the CCPA and sections 7014 and 7015.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7080

Discriminatory Practices.

7080(a)

A price or service difference is discriminatory, and therefore prohibited by Civil Code section 1798.125, if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA or these regulations.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

7080(b)

A business may offer a price or service difference that is nondiscriminatory. A price or service difference is non-discriminatory if it is reasonably related to the value of the consumer's data. If a business is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the price or service difference is reasonably related to the value of the consumer's data, that business shall not offer the price or service difference.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7080(c)

A business's denial of a consumer's request to delete, request to correct, request to know, or request to opt-out of sale/sharing for reasons permitted by the CCPA or these regulations shall not be considered discriminatory.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7080(d)(1)

Illustrative examples follow: (1) Example 1: A music streaming business offers a free service as well as a premium service that costs $5 per month. If only the consumers who pay for the music streaming service are allowed to opt-out of the sale or sharing of their personal information, then the practice is discriminatory, unless the $5-per-month payment is reasonably related to the value of the consumer's data to the business.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7080(d)(2)

Illustrative examples follow: (2) Example 2: A clothing business offers a loyalty program whereby customers receive a $5-off coupon by email after spending $100 with the business. A consumer submits a request to delete all personal information the business has collected about them but also informs the business that they want to continue to participate in the loyalty program. The business may deny their request to delete with regard to their email address and the amount the consumer has spent with the business because that information is necessary for the business to provide the loyalty program requested by the consumer and is reasonably anticipated within the context of the business's ongoing relationship with them pursuant to Civil Code section 1798.105, subdivision (d)(1).

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7080(d)(3)

Illustrative examples follow: 3) Example 3: A grocery store offers a loyalty program whereby consumers receive coupons and special discounts when they provide their phone numbers. A consumer submits a request to opt-out of the sale/sharing of their personal information. The retailer complies with their request but no longer allows the consumer to participate in the loyalty program. This practice is discriminatory unless the grocery store can demonstrate that the value of the coupons and special discounts are reasonably related to the value of the consumer's data to the business.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7080(d)(4)

Illustrative examples follow: (4) Example 4: An online bookseller collects information about consumers, including their email addresses. It offers coupons to consumers through browser pop-up windows while the consumer uses the bookseller's website. A consumer submits a request to delete all personal information that the bookseller has collected about them, including their email address and their browsing and purchasing history. The bookseller complies with the request but stops providing the periodic coupons to the consumer. The bookseller's failure to provide coupons is discriminatory unless the value of the coupons is reasonably related to the value provided to the business by the consumer's data. The bookseller may not deny the consumer's request to delete with regard to the email address because the email address is not necessary to provide the coupons or reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7080(e)

A business shall notify consumers of any financial incentive or price or service difference subject to Civil Code section 1798.125 that it offers in accordance with section 7016.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7080(f)

A business's charging of a reasonable fee pursuant to Civil Code section 1798.145, subdivision (h)(3), shall not be considered a financial incentive subject to these regulations.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7080(g)

A price or service difference that is the direct result of compliance with a state or federal law shall not be considered discriminatory.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7063

Authorized Agents.

7063(a)

When a consumer uses an authorized agent to submit a request to delete, request to correct, or a request to know, a business may require the authorized agent to provide proof that the consumer gave the agent signed permission to submit the request. The business may also require the consumer to do either of the following:

INTERNAL CONTROLS AND CHECKS

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy

Control SDC 77

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

7063(a)(1)

When a consumer uses an authorized agent to submit a request to delete, request to correct, or a request to know, a business may require the authorized agent to provide proof that the consumer gave the agent signed permission to submit the request. The business may also require the consumer to do either of the following: (1) Verify their own identity directly with the business.

INTERNAL CONTROLS AND CHECKS

Control SDC 74

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

7063(a)(2)

When a consumer uses an authorized agent to submit a request to delete, request to correct, or a request to know, a business may require the authorized agent to provide proof that the consumer gave the agent signed permission to submit the request. The business may also require the consumer to do either of the following: (2) Directly confirm with the business that they provided the authorized agent permission to submit the request.

INTERNAL CONTROLS AND CHECKS

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically ✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓
Vendor Management Policy ✓

7063(b)

Subsection (a) does not apply when a consumer has provided the authorized agent with power of attorney pursuant to Probate Code sections 4121 to 4130. A business shall not require power of attorney in order for a consumer to use an authorized agent to act on their behalf.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

7063(c)

An authorized agent shall implement and maintain reasonable security procedures and practices to protect the consumer’s information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 81**

Entity appoints a Data Protection Officer to assess and facilitate the entity's compliance with the provisions of the GDPR

Monitored via 1 check

Privacy officer should be assigned

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

7063(d)

An authorized agent shall not use a consumer's personal information, or any information collected from or about the consumer, for any purposes other than to fulfill the consumer's requests, verification, or fraud prevention.

INTERNAL CONTROLS AND CHECKS

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

7071

Consumers at Least 13 Years of Age and Less Than 16 Years of Age

7071(a)

A business that has actual knowledge that it sells or shares the personal information of consumers at least 13 years of age and less than 16 years of age shall establish, document, and comply with a

reasonable process for allowing such consumers to opt-in to the sale or sharing of their personal information, pursuant to section 7028.

INTERNAL CONTROLS AND CHECKS

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map	✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 97**

Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.

Monitored via 1 check

Disaster recovery

7071(b)

When a business receives a request to opt-in to the sale or sharing of personal information from a consumer at least 13 years of age and less than 16 years of age, the business shall inform the consumer of their ongoing right to opt-out of sale/sharing at any point in the future and of the process for doing so pursuant to section 7026.

INTERNAL CONTROLS AND CHECKS

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map	✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically ✓

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 97**

Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.

Monitored via 1 check

Disaster recovery ✓

7072

Notices to Consumers Less Than 16 Years of Age.

7072(a)

A business subject to sections 7070 and/or 7071 shall include a description of the processes set forth in those sections in its privacy policy.

INTERNAL CONTROLS AND CHECKS

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map	✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control SDC 77

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control SDC 79

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 97

Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.

Monitored via 1 check

Disaster recovery

Control SDC 144

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7072(b)

A business that exclusively targets offers of goods or services directly to consumers under 16 years of age and does not sell or share the personal information without the consent of consumers at least 13 years of age and less than 16 years of age, or the consent of their parent or guardian for consumers under 13 years of age, is not required to provide the Notice of Right to Opt-out of Sale/Sharing.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 76

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control SDC 144

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7023

Requests to Correct

7023(a)

For requests to correct, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 5, the business may deny the request to correct. The business shall inform the requestor that their identity cannot be verified.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7023(b)

In determining the accuracy of the personal information that is the subject of a consumer's request to correct, the business shall consider the totality of the circumstances relating to the contested personal information. A business may deny a consumer's request to correct if it determines that the contested personal information is more likely than not accurate based on the totality of the circumstances.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7023(b)(1)

In determining the accuracy of the personal information that is the subject of a consumer's request to correct, the business shall consider the totality of the circumstances relating to the contested personal information. A business may deny a consumer's request to correct if it determines that the contested

personal information is more likely than not accurate based on the totality of the circumstances. (1) Considering the totality of the circumstances includes, but is not limited to, considering:

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7023(b)(1)(A)

(1) Considering the totality of the circumstances includes, but is not limited to, considering: (A) The nature of the personal information (e.g., whether it is objective, subjective, unstructured, sensitive, etc.).

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7023(b)(1)(B)

(1) Considering the totality of the circumstances includes, but is not limited to, considering: (B) How the business obtained the contested information.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7023(b)(1)(C)

(1) Considering the totality of the circumstances includes, but is not limited to, considering: (C) Documentation relating to the accuracy of the information whether provided by the consumer, the

business, or another source. Requirements regarding documentation are set forth in subsection (d).

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7023(b)(2)

If the business is not the source of the personal information and has no documentation in support of the accuracy of the information, the consumer's assertion of inaccuracy may be sufficient to establish that the personal information is inaccurate.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7023(c)

A business that complies with a consumer's request to correct shall correct the personal information at issue on its existing systems. The business shall also instruct all service providers and contractors that maintain the personal information at issue pursuant to their written contract with the business to make the necessary corrections in their respective systems. Service providers and contractors shall comply with the business's instructions to correct the personal information or enable the business to make the corrections If a business, service provider, or contractor stores any personal information that is the subject of the request to correct on archived or backup systems, it may delay compliance with the consumer's request to correct, with respect to data stored on the archived or backup system, until the archived or backup system relating to that data is restored to an active system or is next accessed or used.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7023(d)(1)

A business shall accept, review, and consider any documentation that the consumer provides in connection with their right to correct whether provided voluntarily or as required by the business. Consumers should make a good-faith effort to provide businesses with all necessary information available at the time of the request.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7023(d)(2)

A business may require the consumer to provide documentation if necessary to rebut its own documentation that the personal information is accurate. In determining the necessity of the documentation requested, the business shall consider the following:

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7023(d)(2)(A)

A business may require the consumer to provide documentation if necessary to rebut its own documentation that the personal information is accurate. In determining the necessity of the documentation requested, the business shall consider the following: (A) The nature of the personal information at issue (e.g., whether it is objective, subjective, unstructured, sensitive, etc.).

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7023(d)(2)(B)

A business may require the consumer to provide documentation if necessary to rebut its own documentation that the personal information is accurate. In determining the necessity of the documentation requested, the business shall consider the following: (B) The nature of the documentation upon which the business considers the personal information to be accurate (e.g., whether the documentation is from a trusted source, whether the documentation is verifiable, etc.)

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7023(d)(2)(C)

A business may require the consumer to provide documentation if necessary to rebut its own documentation that the personal information is accurate. In determining the necessity of the documentation requested, the business shall consider the following: (C) The purpose for which the business collects, maintains, or uses the personal information. For example, if the personal information is essential to the functioning of the business, the business may require more documentation.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7023(d)(2)(D)

A business may require the consumer to provide documentation if necessary to rebut its own documentation that the personal information is accurate. In determining the necessity of the documentation requested, the business shall consider the following: (D) The impact on the consumer. For example, if the personal information has a negative impact on the consumer, the business may require less documentation.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7023(d)(3)

Any documentation provided by the consumer in connection with their request to correct shall only be used and/or maintained by the business for the purpose of correcting the consumer's personal information and to comply with the record-keeping obligations under section 7101.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7023(d)(4)

The business shall implement and maintain reasonable security procedures and practices in maintaining any documentation relating to the consumer's request to correct.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7023(e)

A business may delete the contested personal information as an alternative to correcting the information if the deletion of the personal information does not negatively impact the consumer, or the consumer consents to the deletion. For example, if deleting instead of correcting inaccurate personal information would make it harder for the consumer to obtain a job, housing, credit, education, or other type of opportunity, the business shall process the request to correct or obtain the consumer's consent to delete the information.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7023(f)

In responding to a request to correct, a business shall inform the consumer whether it has complied with the consumer's request. If the business denies a consumer's request to correct in whole or in part, the business shall do the following:

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7023(f)(1)

In responding to a request to correct, a business shall inform the consumer whether it has complied with the consumer's request. If the business denies a consumer's request to correct in whole or in part, the business shall do the following: (1) Explain the basis for the denial, including any conflict with federal or state law, exception to the CCPA, inadequacy in the required documentation, or contention that compliance proves impossible or involves disproportionate effort.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7023(f)(2)

In responding to a request to correct, a business shall inform the consumer whether it has complied with the consumer's request. If the business denies a consumer's request to correct in whole or in part, the business shall do the following: (2) If a business claims that complying with the consumer's request to correct would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot comply with the request. The business shall not simply state that it is impossible or would require disproportionate effort.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7023(f)(3)

In responding to a request to correct, a business shall inform the consumer whether it has complied with the consumer's request. If the business denies a consumer's request to correct in whole or in part, the business shall do the following: (3) If a business denies a consumer's request to correct personal information collected and analyzed concerning a consumer's health, the business shall also inform the consumer that they may provide a written statement to the business to be made part of the consumer's record per Civil Code section 1798.185, subdivision (a)(8)(D). The business shall explain to the consumer that the written statement is limited to 250 words per alleged inaccurate piece of personal information and shall include that the consumer must request that the statement be made part of the consumer's record. Upon receipt of such a statement, the business shall include it with the consumer's record

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7023(f)(4)

In responding to a request to correct, a business shall inform the consumer whether it has complied with the consumer's request. If the business denies a consumer's request to correct in whole or in part, the business shall do the following: (4) If the personal information at issue can be deleted pursuant to a request to delete, inform the consumer that they can make a request to delete the personal information and provide instructions on how the consumer can make a request to delete.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7023(g)

A business may deny a consumer’s request to correct if the business has denied the consumer’s request to correct the same alleged inaccuracy within the past six months of receiving the request. However, the business must treat the request to correct as new if the consumer provides new or additional documentation to prove that the information at issue is inaccurate.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7023(h)

A business may deny a request to correct if it has a good-faith, reasonable, and documented belief that a request to correct is fraudulent or abusive. The business shall inform the requestor that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent or abusive.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7023(i)

Where the business is not the source of the information that the consumer contends is inaccurate, in addition to processing the consumer's request, the business may provide the consumer with the name of the source from which the business received the alleged inaccurate information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7023(j)

Upon request, a business shall disclose specific pieces of personal information that the business maintains and has collected about the consumer to allow the consumer to confirm that the business has corrected the inaccurate information that was the subject of the consumer's request to correct. This disclosure shall not be considered a response to a request to know that is counted towards the limitation of two requests within a 12-month period as set forth in Civil Code section 1798.130, subdivision (b). With regard to a correction to a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics, a business shall not disclose this information, but may provide a way to confirm that the personal information it maintains is the same as what the consumer has provided.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7023(k)

Whether a business, service provider, or contractor has implemented measures to ensure that personal information that is the subject of a request to correct remains corrected factors into whether that business, service provider, or contractor has complied with a consumer's request to correct in accordance with the CCPA and these regulations. For example, a business, service provider, or contractor may supplement personal information it maintains about consumers with information obtained from a data broker. Failing to consider and address the possibility that corrected information may be overridden by inaccurate information subsequently received from a data broker may factor into whether that business, service provider, or contractor has adequately complied with a consumer's request to correct.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7020

Methods for Submitting Requests to Delete, Requests to Correct, and Requests to Know

7020(a)

A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests to delete, requests to correct, and requests to know.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7020(b)

A business that does not fit within subsection (a) shall provide two or more designated methods for submitting requests to delete, requests to correct, and requests to know. One of those methods must be a toll-free telephone number. If the business maintains an internet website, one of the methods for submitting these requests shall be through its website, such as through a webform. Other methods for submitting requests to delete, requests to correct, and requests to know may include, but are not limited to, a designated email address, a form submitted in person, and a form submitted through the mail.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7020(c)

A business shall consider the methods by which it primarily interacts with consumers when determining which methods to provide for submitting requests to delete, requests to correct, and requests to know. If the business interacts with consumers in person, the business shall consider providing an in-person method such as a printed form the consumer can directly submit or send by mail, a tablet or computer portal that allows the consumer to complete and submit an online form, or a telephone with which the consumer can call the business's toll-free number.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7020(d)

A business may use a two-step process for online requests to delete where the consumer must first, submit the request to delete and then second, separately confirm that they want their personal information deleted provided that the business otherwise complies with section 7004.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7020(e)

If a consumer submits a request in a manner that is not one of the designated methods of submission, or is deficient in some manner unrelated to the verification process, the business shall either:

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7021

Timelines for Responding to Requests to Delete, Requests to Correct, and Requests to Know a

7021(a)

No later than 10 business days after Upon receiving a request to delete, request to correct, or request to know a business shall confirm receipt of the request and provide information about how the business will process the request. The information provided shall describe in general the business's verification process and when the consumer should expect a response, except in instances where the business has already granted or denied the request. The confirmation may be given in the same manner in which the request was received. For example, if the request is made over the phone, the confirmation may be given orally during the phone call.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7021(b)

Businesses shall respond to a request to delete, request to correct, and request to know no later than 45 calendar days after it receives the request. The 45- day period will begin on the day that the business receives the request, regardless of time required to verify the request. If the business cannot verify the consumer within the 45-day time period, the business may deny the request. If necessary, businesses may take up to an additional 45 calendar days to respond to the consumer's request, for a maximum total of 90 calendar days from the day the request is received, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7051

Contract Requirements for Service Providers and Contractors

7051(a)(1)

The contract required by the CCPA for service providers and contractors shall: (1) Prohibit the service provider or contractor from selling or sharing personal information it Collects pursuant to the written contract with the business.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management

Vendor Management Policy

Vendor Management Procedure

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

7051(a)(2)

The contract required by the CCPA for service providers and contractors shall: (2) Identify the specific Business Purpose(s) for which the service provider or contractor is processing personal information pursuant to the written contract with the business, and specify that the business is disclosing the personal information to the service provider or contractor only for the limited and specified Business Purpose(s) set forth within the contract. The Business Purpose or service shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

7051(a)(3)

The contract required by the CCPA for service providers and contractors shall: (3) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it Collected pursuant to the written contract with the business for any purposes other than the Business Purpose(s) those specified in the contract or as otherwise permitted by the CCPA and these regulations.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

7051(a)(4)

The contract required by the CCPA for service providers and contractors shall: (4) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it Collected pursuant to the written contract with the business for any commercial purpose other than the Business Purposes specified in the contract, unless expressly permitted by the CCPA or these regulations.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

7051(a)(5)

The contract required by the CCPA for service providers and contractors shall: (5) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it Collected pursuant to the written contract with the business outside the direct business relationship between the service provider or contractor and the business, unless expressly permitted by the CCPA or these regulations. For example, a service provider or contractor shall be prohibited from combining or updating personal information that it Collected pursuant to the written contract with the business with personal information that it received from another source or Collected from its own interaction with the consumer, unless expressly permitted by the CCPA or these regulations.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓

Vendor Management Policy

Vendor Management Procedure

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

7051(a)(6)

The contract required by the CCPA for service providers and contractors shall: (6) Require the service provider or contractor to comply with all applicable sections of the CCPA and these regulations, including—with respect to the personal information that it Collected pursuant to the written contract with the business—providing the same level of privacy protection as required of businesses by the CCPA and these regulations. For example, the contract may require the service provider or contractor to cooperate with the business in responding to and complying with consumers' requests made pursuant to the CCPA, and to implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

7051(a)(7)

The contract required by the CCPA for service providers and contractors shall: (7) Grant the business the right to take reasonable and appropriate steps to ensure that service provider or contractor uses the personal information that it Collected pursuant to the written contract with the business in a

manner consistent with the business's obligations under the CCPA and these regulations. Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider's system and regular internal or third-party assessments, audits, or other technical and operational testing at least once every 12 months.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓

Vendor Management Policy

Control SDC 74

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control SDC 77

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

7051(a)(8)

The contract required by the CCPA for service providers and contractors shall: (8) Require the service provider or contractor to notify the business after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.

INTERNAL CONTROLS AND CHECKS

Control SDC 21

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management ✓

Vendor Management Policy ✓

Vendor Management Procedure ✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy

Control SDC 77

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

7051(a)(9)

The contract required by the CCPA for service providers and contractors shall: (9) Grant the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate the service provider or contractor's unauthorized use of personal information. For example, the business may require the service provider or contractor to provide documentation that verifies that they no longer retain or use the personal information of consumers that have made a valid request to delete with the business.

INTERNAL CONTROLS AND CHECKS

Control SDC 21

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control SDC 29

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

7051(a)(10)

The contract required by the CCPA for service providers and contractors shall: (10) Require the service provider or contractor to enable the business to comply with consumer requests made pursuant to the CCPA or require the business to inform the service provider or contractor of any consumer request made pursuant to the CCPA that they must comply with and provide the information necessary for the service provider or contractor to comply with the request.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management

Vendor Management Policy

Vendor Management Procedure

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

7051(b)

A service provider or contractor that subcontracts with another person in providing services to the business for whom it is a service provider or contractor shall have a contract with the subcontractor that complies with the CCPA and these regulations, including subsection (a).

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

7051(c)

Whether a business conducts due diligence of its service providers and contractors factors into whether the business has reason to believe that a service provider or contractor is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that never enforces the terms of the contract nor exercises its rights to audit or test the service provider's or contractor's systems might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the CCPA and these regulations at the time the business disclosed the personal information to the service provider or contractor.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

7052

Third Parties.

7052(a)

A third party that does not have a contract that complies with section 7053, subsection (a), shall not collect, use, process, retain, sell, or share the personal information that the business made available to it.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

7052(b)

A third party shall comply with the terms of the contract required by the CCPA and these regulations, which include treating the personal information that the business made available to it in a manner consistent with the business's obligations under the CCPA and these regulations.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

7003

Requirements for Disclosures and Communications to Consumers.

7003(a)

Disclosures and communications to consumers shall be easy to read and understandable to consumers. For example, they shall use plain, straightforward language and avoid technical or legal jargon.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7003(b)(1)

Disclosures required under Article 2 shall also: (1) Use a format that makes the disclosure readable, including on smaller screens, if applicable.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7003(b)(2)

Disclosures required under Article 2 shall also: (2) Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7003(b)(3)

Disclosures required under Article 2 shall also: (3) Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the policy in an alternative format.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7102

Requirements for Businesses Collecting Large Amounts of Personal Information.

7102(a)(1)(A)

Compile the following metrics for the previous calendar year: (A) The number of requests to delete that the business received, complied with in whole or in part, and denied

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

7102(a)(1)(B)

Compile the following metrics for the previous calendar year: (B) The number of requests to correct that the business received, complied with in whole or in part, and denied

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

7102(a)(1)(C)

Compile the following metrics for the previous calendar year: (C) The number of requests to know that the business received, complied with in whole or in part, and denied

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

7102(a)(1)(D)

Compile the following metrics for the previous calendar year: (D) The number of requests to opt-out of sale/sharing that the business received, complied with in whole or in part, and denied

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

7102(a)(1)(E)

Compile the following metrics for the previous calendar year: (E) The number of requests to limit that the business received, complied with in whole or in part, and denied

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

7102(a)(1)(F)

Compile the following metrics for the previous calendar year: (F) The median or mean number of days within which the business substantively responded to requests to know, requests to delete, requests to correct, requests to know, requests to opt-out of sale/sharing, and requests to opt-out limit.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

7102(a)(2)

Disclose, by July 1 of every calendar year, the information compiled in subsection (a)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy. (A) In its disclosure pursuant to subsection (ag)(2), a business may choose to disclose the number of requests that it denied in whole or in part because the request was not verifiable, was not made by a consumer, called for information exempt from disclosure, or was denied on other grounds.

INTERNAL CONTROLS AND CHECKS

Control SDC 14

Entity displays the most current information about its services on its website, which is accessible to its customers.

Monitored via 1 check

Product marketing website should be available

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7102(b)

A business may choose to compile and disclose the information required by subsection (a)(1) for requests received from all individuals, rather than requests received from consumers. The business shall state whether it has done so in its disclosure and shall, upon request, compile and provide to the Attorney General the information required by subsection (a)(1) for requests received from consumers.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

7101

Record-Keeping

7101(a)

A business shall maintain records of consumer requests made pursuant to the CCPA and how it responded to the requests for at least 24 months. The business shall implement and maintain reasonable security procedures and practices in maintaining these records.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

7101(b)

The records may be maintained in a ticket or log format provided that the ticket or log includes the date of request, nature of request, manner in which the request was made, the date of the business's response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

7101(c)

A business's maintenance of the information required by this section, where that information is not used for any other purpose, does not taken alone violate the CCPA or these regulations

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

7101(d)

Information maintained for record-keeping purposes shall not be used for any other purpose except as reasonably necessary for the business to review and modify its processes for compliance with the CCPA and these regulations. Information maintained for recordkeeping purposes shall not be shared with any third party except as necessary to comply with a legal obligation.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

7101(e)

Other than as required by subsection (b), a business is not required to retain personal information solely for the purpose of fulfilling a consumer request made under the CCPA.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

7011

Privacy Policy.

7011(a)

The purpose of the privacy policy is to provide consumers with a comprehensive description of a business's online and offline Information Practices. It shall also inform consumers about the rights they have regarding their personal information and provide any information necessary for them to exercise those rights.

INTERNAL CONTROLS AND CHECKS

Control SDC 144

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7011(b)

The privacy policy shall comply with section 7003, subsections (a) and (b).

INTERNAL CONTROLS AND CHECKS

Control SDC 144

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7011(c)

The privacy policy shall be available in a format that allows a consumer to print it out as a document.

INTERNAL CONTROLS AND CHECKS

Control SDC 144

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7011(d)

The privacy policy shall be posted online and accessible through a conspicuous link that complies with section 7003, subsections (c) and (d), using the word “privacy” on the business’s website Homepage(s) or on the download or landing page of a mobile application. If the business has a California-specific description of consumers’ privacy rights on its website, then the privacy policy shall be included in that description. A business that does not operate a website shall make the privacy

policy conspicuously available to consumers. A mobile application may include a link to the privacy policy in the application's settings menu.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7011(e)(1)

The privacy policy shall include the following information: (1) A comprehensive description of the business's online and offline Information Practices, which includes the following

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7011(e)(1)(A)

A comprehensive description of the business's online and offline Information Practices, which includes the following: (A) Identification of the categories of personal information the business has collected about consumers in the preceding 12 months. The categories shall be described using the specific terms set forth in Civil Code section 1798.140, subdivisions (v)(1)(A) to (K) and (ae)(1) to (3). To the extent that the business has discretion in its description, the business shall describe the category in a manner that provides consumers a meaningful understanding of the information being collected.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7011(e)(1)(B)

A comprehensive description of the business's online and offline Information Practices, which includes the following: (B) Identification of the categories of sources from which the personal information is collected

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7011(e)(1)(C)

A comprehensive description of the business's online and offline Information Practices, which includes the following: (C) Identification of the specific business or commercial purpose for collecting personal information from consumers. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is collected

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7011(e)(1)(D)

A comprehensive description of the business's online and offline Information Practices, which includes the following: (D) Identification of the categories of personal information, if any, that the business has sold or shared to third parties in the preceding 12 months. If the business has not sold or shared consumers' personal information in the preceding 12 months, the business shall disclose that fact

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7011(e)(1)(E)

A comprehensive description of the business's online and offline Information Practices, which includes the following: (E) For each category of personal information identified in subsection (e)(1)(D), the categories of third parties to whom the information was sold or shared

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7011(e)(1)(F)

A comprehensive description of the business's online and offline Information Practices, which includes the following: (F) Identification of the specific business or commercial purpose for selling or sharing consumers' personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is sold or shared.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7011(e)(1)(G)

A comprehensive description of the business's online and offline Information Practices, which includes the following: (G) A statement regarding whether the business has actual knowledge that it sells or shares the personal information of consumers under 16 years of age.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7011(e)(1)(H)

A comprehensive description of the business's online and offline Information Practices, which includes the following: (H) Identification of the categories of personal information, if any, that the business has disclosed for a business purpose to third parties in the preceding 12 months. If the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

7011(e)(1)(I)

A comprehensive description of the business's online and offline Information Practices, which includes the following: (I) For each category of personal information identified in subsection (e)(1)(H), the categories of third parties to whom the information was disclosed.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

7011(e)(1)(J)

A comprehensive description of the business's online and offline Information Practices, which includes the following: (J) Identification of the specific business or commercial purpose for disclosing the consumer's personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is disclosed.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7011(e)(1)(K)

A comprehensive description of the business's online and offline Information Practices, which includes the following: (K) A statement regarding whether or not the business uses or discloses sensitive personal information for purposes other than those specified in section 7027, subsection (lm).

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7011(e)(2)

The privacy policy shall include the following information: (2) An explanation of the rights that the CCPA confers on consumers regarding their personal information, which includes the following:

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7011(e)(2)(A)

An explanation of the rights that the CCPA confers on consumers regarding their personal information, which includes the following: (A) The right to know what personal information the business has collected about the consumer, including the categories of personal information, the categories of sources from which the personal information is collected, the business or commercial purpose for collecting, selling, or sharing personal information, the categories of third parties to whom the business discloses personal information, and the specific pieces of personal information the business has collected about the consumer;

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7011(e)(2)(B)

An explanation of the rights that the CCPA confers on consumers regarding their personal information, which includes the following: (B) The right to delete personal information that the business has collected from the consumer, subject to certain exceptions;

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7011(e)(2)(C)

An explanation of the rights that the CCPA confers on consumers regarding their personal information, which includes the following: (C) The right to correct inaccurate personal information that a business maintains about a consumer;

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7011(e)(2)(D)

An explanation of the rights that the CCPA confers on consumers regarding their personal information, which includes the following: (D) If the business sells or shares personal information, the right to opt-out of the sale or sharing of their personal information by the business;

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7011(e)(2)(E)

An explanation of the rights that the CCPA confers on consumers regarding their personal information, which includes the following: (E) If the business uses or discloses sensitive personal information for reasons other than those set forth in section 7027, subsection (lm), the right to limit the use or disclosure of sensitive personal information by the business;

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7011(e)(2)(F)

An explanation of the rights that the CCPA confers on consumers regarding their personal information, which includes the following: (F) The right not to receive discriminatory treatment by the business for the exercise of privacy rights conferred by the CCPA, including an employee's, applicant's, or independent contractor's right not to be retaliated against for the exercise of their CCPA rights

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7011(e)(3)

The privacy policy shall include the following information: (3) An explanation of how consumers can exercise their CCPA rights and what consumers can expect from that process, which includes the following:

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7011(e)(3)(A)

An explanation of how consumers can exercise their CCPA rights and what consumers can expect from that process, which includes the following: (A) An explanation of the methods by which the consumer can exercise their CCPA rights;

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7011(e)(3)(B)

An explanation of how consumers can exercise their CCPA rights and what consumers can expect from that process, which includes the following: (B) Instructions for submitting a request under the CCPA, including any links to an online request form or portal for making such a request, if offered by the business;

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7011(e)(3)(C)

An explanation of how consumers can exercise their CCPA rights and what consumers can expect from that process, which includes the following: (C) If the business sells or shares personal information, and is required to provide a Notice of Right to Opt-out of Sale/Sharing, the contents of the Notice of Right to Opt-out of Sale/Sharing or a link to that notice in accordance with section 7013, subsection (f);

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7011(e)(3)(D)

An explanation of how consumers can exercise their CCPA rights and what consumers can expect from that process, which includes the following: (D) If the business uses or discloses sensitive personal information for purposes other than those specified in section 7027, subsection (lm), and is required to provide a Notice of Right to Limit, the contents of the Notice of Right to Limit or a link to that notice in accordance with section 7014, subsection (f);

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

7011(e)(3)(E)

An explanation of how consumers can exercise their CCPA rights and what consumers can expect from that process, which includes the following: (E) A general description of the process the business uses to verify a consumer request to know, request to delete, and request to correct, when applicable, including any information the consumer must provide;

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

7011(e)(3)(F)

An explanation of how consumers can exercise their CCPA rights and what consumers can expect from that process, which includes the following: (F) Explanation of how an opt-out preference signal will be processed for the consumer (i.e., whether the signal applies to the device, browser, consumer account, and/or offline sales, and in what circumstances) and how the consumer can use an opt-out preference signal;

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7011(e)(3)(G)

An explanation of how consumers can exercise their CCPA rights and what consumers can expect from that process, which includes the following: (G) If the business processes opt-out preference signals in a frictionless manner, information on how consumers can implement opt-out preference signals for the business to process in a frictionless manner;

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7011(e)(3)(H)

An explanation of how consumers can exercise their CCPA rights and what consumers can expect from that process, which includes the following: (H) Instructions on how an authorized agent can make a request under the CCPA on the consumer’s behalf;

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7011(e)(3)(l)

An explanation of how consumers can exercise their CCPA rights and what consumers can expect from that process, which includes the following: (l) If the business has actual knowledge that it sells the personal information of consumers under 16 years of age, a description of the processes required by sections 7070 and 7071;

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

Control **SDC 112**

Entity has documented guidelines on notifying customers and other stakeholders in case of a breach.

Monitored via 3 checks

Data Breach Notification Policy ✓

Personal Data Breach Notification Procedure

PHI Data breach Notification Procedure

Control **SDC 433**

Entity has documented policy and procedures which provides guidance on integrating privacy principles into the design process that help in complying with privacy regulations.

Monitored via 1 check

Privacy By Design Policy

Control **SDC 1105**

Entity has documented guidelines on notifying customers and other stakeholders in case of a PII breach.

Monitored via 1 check

Personal Data Breach Notification Procedure

7011(e)(3)(J)

An explanation of how consumers can exercise their CCPA rights and what consumers can expect from that process, which includes the following: (J) A contact for questions or concerns about the business's privacy policies and Information pPractices using a method reflecting the manner in which the business primarily interacts with the consumer.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7011(e)(4)

The privacy policy shall include the following information: (4) Date the privacy policy was last updated.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7011(e)(5)

The privacy policy shall include the following information: (5) If subject to the data reporting requirements set forth in section 7102, the information required under section 7102, or a link to such information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7012(a)

(a) The purpose of the Notice at Collection is to provide consumers with timely notice, at or before the point of collection, about the categories of personal information to be collected from them, the purposes for which the personal information is collected or used, and whether that information is sold or shared, so that consumers have a tool to exercise meaningful control over the business's use of their personal information. For example, upon receiving the Notice at Collection, the consumer can use the information in the notice as a tool to choose whether to engage with the business, or to direct the business not to sell or share their personal information and to limit the use and disclosure of their sensitive personal information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7012

Notice at Collection of Personal Information.

7012(b)

(b) The nNotice at cCollection shall comply with section 7003, subsections (a) and (b).

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7012(c)

The Notice at Collection shall be made readily available where consumers will encounter it at or before the point of collection of any personal information. Illustrative examples follow

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7012(c)(1)

The Notice at Collection shall be made readily available where consumers will encounter it at or before the point of collection of any personal information. Illustrative examples follow. (1) When a business collects consumers' personal information online, it may post a conspicuous link to the notice on the introductory page of the business's website and on all webpages where personal information is collected.

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7012(c)(2)

The Notice at Collection shall be made readily available where consumers will encounter it at or before the point of collection of any personal information. Illustrative examples follow. (2) When a

business collects consumers' personal information through a webform, it may post a conspicuous link to the notice in close proximity to the fields in which the consumer inputs their personal information, or in close proximity to the button by which the consumer submits their personal information to the business.

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7012(c)(3)

The Notice at Collection shall be made readily available where consumers will encounter it at or before the point of collection of any personal information. Illustrative examples follow. (3) When a business collects personal information through a mobile application, it may provide a link to the notice on the mobile application's download page and within the application, such as through the application's settings menu.

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7012(c)(4)

The Notice at Collection shall be made readily available where consumers will encounter it at or before the point of collection of any personal information. Illustrative examples follow. (4) When a business collects consumers' personal information offline, it may include the notice on printed forms that collect personal information, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to where the notice can be found online.

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7012(c)(5)

The Notice at Collection shall be made readily available where consumers will encounter it at or before the point of collection of any personal information. Illustrative examples follow. (5) When a business collects personal information over the telephone or in person, it may provide the notice orally.

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7012(d)

(d) If a business does not give the Notice at Collection to the consumer at or before the point of collection of their personal information, the business shall not collect personal information from the consumer.

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7012(e)(1)

A business shall include the following in its Notice at Collection: (1) A list of the categories of personal information about consumers, including categories of sensitive personal information, to be collected. Each category of personal information shall be written in a manner that provides consumers a meaningful understanding of the information being collected.

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7012(e)(2)

A business shall include the following in its Notice at Collection: (2) The purpose(s) for which the categories of personal information, including categories of sensitive personal information, are collected and used.

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7012(e)(3)

A business shall include the following in its Notice at Collection: (3) Whether each the category of personal information identified in subsection (e)(1) is sold or shared.

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7012(e)(4)

A business shall include the following in its Notice at Collection: (4) The length of time the business intends to retain each category of personal information identified in subsection (e)(1), or if that is not possible, the criteria used to determine the period of time it will be retained.

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7012(e)(5)

A business shall include the following in its Notice at Collection: (5) If the business sells or shares personal information, the link to the Notice of Right to Opt-out of Sale/Sharing, or in the case of offline notices, where the webpage can be found online.

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7012(e)(6)

A business shall include the following in its Notice at Collection: (6) A link to the business's privacy policy, or in the case of offline notices, where the privacy policy can be found online.

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7012(f)

(f) If a business collects personal information from a consumer online, the Notice at Collection may be given to the consumer by providing a link that takes the consumer directly to the specific section of the business's privacy policy that contains the information required in subsection (e)(1) through (6). Directing the consumer to the beginning of the privacy policy, or to another section of the privacy policy that does not contain the required information, so that the consumer is required to scroll through other information in order to determine the categories of personal information to be collected and/or whether the business sells or shares the personal information collected, does not satisfy this standard.

INTERNAL CONTROLS AND CHECKS

Control SDC 76

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7012(g)

(g) Third Parties that Control the Collection of Personal Information. This subsection shall not affect the first party's obligations under the CCPA to comply with a consumer's request to opt-out of sale/sharing.

INTERNAL CONTROLS AND CHECKS

Control SDC 76

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7012(g)(1)

Third Parties that Control the Collection of Personal Information. This subsection shall not affect the first party's obligations under the CCPA to comply with a consumer's request to opt-out of sale/sharing. (1) For purposes of giving Notice at Collection, more than one business may control the collection of a consumer's personal information, and thus, have an obligation to Page 22 of 73 provide a Notice at Collection in accordance with the CCPA and these regulations. For example, a first party may allow another business, acting as a third party, to control the collection of personal information from consumers browsing the first party's website. Both the first party that allows the third parties to collect personal information via its website, as well as the third party controlling the collection of personal information, shall provide a Notice at Collection. The first party and third parties may provide a single Notice at Collection that includes the required information about their collective Information Practices.

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7012(g)(2)

Third Parties that Control the Collection of Personal Information. This subsection shall not affect the first party's obligations under the CCPA to comply with a consumer's request to opt-out of sale/sharing. (2) A business that, acting as a third party, controls the collection of personal information on another business's physical premises, such as in a retail store or in a vehicle, shall provide a Notice at Collection in a conspicuous manner at the physical location(s) where it is collecting the personal information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7012(g)(3)(A)

Illustrative examples follow (A) Business F allows Business G, a third party ad network, to collect consumers' personal information through Business F's website. Business F may post a conspicuous

link to its Notice at Collection on its Homepage(s). Business G shall provide a Notice at Collection on its Homepage(s) or include the required information about its Information Practices in Business F's Notice at Collection

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7012(g)(3)(B)

Illustrative examples follow (B) Business H, a coffee shop, allows Business I, a business providing Wi-Fi services, to collect personal information from consumers using Business I's services on Business H's premises. Business H may post conspicuous signage at the entrance of the store or at the point-of-sale directing consumers to where the Notice at Collection for Business H can be found online. In addition, Business I shall post its own Notice at cCollection on the first webpage or other interface consumers see before connecting to the Wi-Fi services offered.

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7012(g)(3)(C)

Illustrative examples follow (C) Business J, a car rental business, allows Business K to collect personal information from consumers within the vehicles Business J rents to consumers. Business J may give its Notice at Collection to the consumer at the point of sale, i.e., at the rental counter, either in writing or orally. Business K may provide its own Notice at Collection within the vehicle, such as through signage on the vehicle's computer dashboard directing consumers to where the notice can be found online.

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7012(h)

A business that neither collects nor controls the collection of personal information directly from the consumer does not need to provide a Notice at Collection to the consumer if it neither sells nor shares the consumer's personal information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7012(i)

(i) A data broker registered with the Attorney General pursuant to Civil Code section 1798.99.80 et seq., where it collects personal information from a source other than directly from the consumer, does

not need to provide a Notice at Collection to the consumer if it has included in its registration submission a lin to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out of sale/sharing.

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7004

Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent.

7004(a)

Except as expressly allowed by the CCPA and these regulations, businesses shall design and implement methods for submitting CCPA requests and obtaining consumer consent that incorporate the following principles.

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

7004(a)(1)

Except as expressly allowed by the CCPA and these regulations, businesses shall design and implement methods for submitting CCPA requests and obtaining consumer consent that incorporate the following principles. (1) Easy to understand. The methods shall use language that is easy for consumers to read and understand. When applicable, they shall comply with the requirements for disclosures to consumers set forth in section 7003.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7004(a)(2)

Except as expressly allowed by the CCPA and these regulations, businesses shall design and implement methods for submitting CCPA requests and obtaining consumer consent that incorporate the following principles. (2) Symmetry in choice. The path for a consumer to exercise a more privacy-protective option shall not be longer or more difficult or time-consuming than the path to exercise a less privacy-protective option because that would impair or interfere with the consumer's ability to make a choice. Illustrative examples follow

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7004(a)(2)(A)

Symmetry in choice. The path for a consumer to exercise a more privacy-protective option be longer or more difficult or time-consuming than the path to exercise a less privacy-protective option because that would impair or interfere with the consumer's ability to make a choice. Illustrative examples follow (A) It is not symmetrical when a business's process for submitting a request to optout of sale/sharing requires more steps than that business's process for a consumer to opt-in to the sale of personal information after having previously opted out. The number of steps for submitting a request to opt-out of sale/sharing is measured from when the consumer clicks on the "Do Not Sell or Share My Personal Information" link to completion of the request. The number of steps for submitting a request to opt-in to the sale of personal information is measured from the first indication by the consumer to the business of their interest to opt-in to completion of the request.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 76

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7004(a)(2)(B)

Symmetry in choice. The path for a consumer to exercise a more privacy-protective option be longer or more difficult or time-consuming than the path to exercise a less privacy-protective option because that would impair or interfere with the consumer's ability to make a choice. Illustrative examples follow (B) A choice to opt-in to the sale of personal information that only provides the two choices, "Yes" and "Ask me later," is not equal or symmetrical because there is no option to decline the opt-in. "Ask me later" implies that the consumer has not declined but delayed the decision and that the business will continue to ask the consumer to opt-in. Framing the consumer's options in this manner impairs the consumer's ability to make a choice. An equal or symmetrical choice could be "Yes" and "No."

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7004(a)(2)(C)

Symmetry in choice. The path for a consumer to exercise a more privacy-protective option be longer or more difficult or time-consuming than the path to exercise a less privacy-protective option because that would impair or interfere with the consumer's ability to make a choice. Illustrative examples follow (C) A website banner that provides only the two choices when seeking the consumer's consent to use their personal information, "Accept All" and "More Information," or "Accept All" and "Preferences," is not equal or symmetrical because the method allows the consumer to "Accept All" in one step, but requires the consumer to take additional steps to exercise their rights over their personal information. Framing the consumer's options in this manner impairs the consumer's ability to make a choice. An equal or symmetrical choice could be "Accept All" and "Decline All."

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7004(a)(3)

Avoid language or interactive elements that are confusing to the consumer. The methods should not use double negatives. Toggles or buttons must clearly indicate the consumer's choice. Illustrative examples follow.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7004(a)(3)(A)

Avoid language or interactive elements that are confusing to the consumer. The methods should not use double negatives. Toggles or buttons must clearly indicate the consumer’s choice. Illustrative examples follow. (A) Giving the choice of “Yes” or “No” next to the statement “Do Not Sell or Share My Personal Information” is a double negative and a confusing choice for a consumer.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7004(a)(3)(B)

Avoid language or interactive elements that are confusing to the consumer. The methods should not use double negatives. Toggles or buttons must clearly indicate the consumer's choice. Illustrative examples follow. (B) Toggles or buttons that state "on" or "off" may be confusing to a consumer and may require further clarifying language.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7004(a)(3)(C)

Avoid language or interactive elements that are confusing to the consumer. The methods should not use double negatives. Toggles or buttons must clearly indicate the consumer's choice. Illustrative examples follow. (C) Unintuitive placement of buttons to confirm a consumer's choice may be confusing to the consumer. For example, it is confusing to the consumer when a business at first consistently offers choices in the order of Yes, then No, but then offers choices in the opposite order—No, then Yes—when asking the consumer something that would benefit the business and/or contravene the consumer's expectation.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7004(a)(4)

Except as expressly allowed by the CCPA and these regulations, businesses shall design and implement methods for submitting CCPA requests and obtaining consumer consent that incorporate the following principles. (4) Avoid choice architecture that impairs or interferes with the consumer's ability to make a choice. Businesses should also not design their methods in a manner that would impair the consumer's ability to exercise their choice because consent must be freely given, specific, informed, and unambiguous. Illustrative examples follow.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7004(a)(4)(A)

Except as expressly allowed by the CCPA and these regulations, businesses shall design and implement methods for submitting CCPA requests and obtaining consumer consent that incorporate the following principles. (A) Requiring the consumer to click through disruptive screens before they are able to submit a request to opt-out of sale/sharing is a choice architecture that impairs or interferes with the consumer’s ability to exercise their choice.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7004(a)(4)(B)

Except as expressly allowed by the CCPA and these regulations, businesses shall design and implement methods for submitting CCPA requests and obtaining consumer consent that incorporate the following principles. (B) Bundling choices so that the consumer is only offered the option to consent to using personal information for purposes that meet the requirements set forth in section 7002, subsection (a), together with purposes that are incompatible with the context in which the personal information was collected is a choice architecture that impairs or interferes with the consumer's ability to make a choice. For example, a business that provides a location-based service, such as a mobile application that posts gas prices within the consumer's location, shall not require the consumer to consent to incompatible uses (e.g., sale of the consumer's geolocation to data brokers) together with a reasonably necessary and proportionate use of geolocation information for providing the location-based services, which does Page 13 of 73 not require consent. This type of choice architecture does not allow consent to be freely given, specific, informed, or unambiguous because it requires the consumer to consent to incompatible uses in order to obtain the expected service. The business should provide the consumer a separate option to consent to the business's use of personal information that does not meet the requirements set forth in section 7002, subsection (a).

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7004(a)(5)

Except as expressly allowed by the CCPA and these regulations, businesses shall design and implement methods for submitting CCPA requests and obtaining consumer consent that incorporate the following principles. (5) Easy to execute. The business shall not add unnecessary burden or friction to the process by which the consumer submits a CCPA request. Methods should be tested to ensure that they are functional and do not undermine the consumer's choice to submit the request. Illustrative examples follow.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7004(a)(5)(A)

Except as expressly allowed by the CCPA and these regulations, businesses shall design and implement methods for submitting CCPA requests and obtaining consumer consent that incorporate the following principles. (A) Upon clicking the “Do Not Sell or Share My Personal Information” link, the business shall not require the consumer to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt-out of sale/sharing.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7004(a)(5)(B)

Except as expressly allowed by the CCPA and these regulations, businesses shall design and implement methods for submitting CCPA requests and obtaining consumer consent that incorporate the following principles. (B) A business that knows of, but does not remedy, circular or broken links, and nonfunctional email addresses, such as inboxes that are not monitored or have aggressive filters that screen emails from the public, may be in violation of this regulation.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7004(a)(5)(C)

Except as expressly allowed by the CCPA and these regulations, businesses shall design and implement methods for submitting CCPA requests and obtaining consumer consent that incorporate the following principles. (C) Businesses that require the consumer to unnecessarily wait on a webpage as the business processes the request may be in violation of this regulation.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7004(b)

(b) A method that does not comply with subsection (a) may be considered a dark pattern. Any agreement obtained through the use of dark patterns shall not constitute consumer consent. For example, a business that uses dark patterns to obtain consent from a consumer to sell their personal information shall be in the position of never having obtained the consumer’s consent to do so.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7004(c)

(c) A user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decisionmaking, or choice. A business's intent in designing the interface is not determinative in whether the user interface is a dark pattern, but a factor to be considered. If a business did not intend to design the user interface to subvert or impair user choice, but the business knows of and does not remedy a user interface that has that effect, the user interface may still be a dark pattern. Similarly, a business's deliberate ignorance of the effect of its user interface may also weigh in favor of establishing a dark pattern

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 76

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7028

Requests to Opt-In After Opting-Out of the Sale or Sharing of Personal Information

7028(a)

Requests to opt-in to sale or sharing of personal information shall use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7028(b)

If a consumer who has opted-out of the sale or sharing of their personal information initiates a transaction or attempts to use a product or service that requires the sale or sharing of their personal information, the business may inform the consumer that the transaction, product, or service requires the sale of their personal information and provide instructions on how the consumer can provide consent to opt-in to the sale or sharing of their personal information. The business shall comply with section 7004 when obtaining the consumer's consent.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7013

Notice of Right to Opt-Out of Sale/Sharing and the “Do Not Sell or Share My Personal Information” Link.

7013(a)

The purpose of the Notice of Right to Opt-out of Sale/sSharing is to inform consumers of their right to direct a business that sells or shares their personal information to stop selling or sharing their personal information and to provide them with the opportunity to exercise that right. The purpose of the “Do Not Sell or Share My Personal Information” link is to immediately effectuate the consumer’s right to opt-out of sale/sharing, or in the alternative, direct the consumer to the Notice of Right to oOpt-out of sSale/Sharing . Accordingly, clicking the business’s “Do Not Sell or Share My Personal Information” link will either have the immediate effect of opting the consumer out of the sale or sharing of personal information or lead the consumer to a webpage where the consumer can learn about and make that choice.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7013(b)

The Notice of Right to Opt-out of Sale/Sharing shall comply with section 7003, subsections (a) and (b).

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7013(c)

The “Do Not Sell or Share My Personal Information” link shall be a conspicuous link that complies with section 7003, subsections (c) and (d) and is located at either the header or footer of the business’s internet Homepage(s).

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7013(d)

In lieu of posting the “Do Not Sell or Share My Personal Information” link, a business may provide the Alternative Opt-out Link in accordance with section 7015 or process opt-out preference signals in a frictionless manner in accordance with section 7025, subsections (f) and (g). The business must still post a Notice of Right to Opt-out of Sale/Sharing in accordance with these regulations.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7013(e)

A business that sells or shares the personal information of consumers shall provide the Notice of Right to Opt-out of Sale/Sharing to consumers as follows:

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

7013(e)(1)

A business that sells or shares the personal information of consumers shall provide the Notice of Right to Opt-out of Sale/Sharing to consumers as follows: (1) A business shall post the Notice of Right to Opt-out of Sale/Sharing on the internet webpage to which the consumer is directed after clicking on the “Do Not Sell or Share My Personal Information” link. The notice shall include the information specified in subsection (f) or be a link that takes the consumer directly to the specific section of the business’s privacy policy that contains the same information. If clicking on the “Do Not Sell or Share My Personal Information” link immediately effectuates the consumer’s right to opt-out of sale/sharing

or if the business processes opt-out preference signals in a frictionless manner and chooses not to post a link, the business shall provide the notice within its privacy policy.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7013(e)(2)

A business that sells or shares the personal information of consumers shall provide the Notice of Right to Opt-out of Sale/Sharing to consumers as follows: (2) A business that does not operate a website shall establish, document, and comply with another method by which it informs consumers of their right to opt-out of sale/sharing. That method shall comply with the requirements set forth in section 7004

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control SDC 144

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7013(e)(3)

A business that sells or shares the personal information of consumers shall provide the Notice of Right to Opt-out of Sale/Sharing to consumers as follows: (3) A business shall also provide the notice to opt-out of sale/sharing in the same manner in which it collects the personal information that it sells or shares. Illustrative examples follow.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 76

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control SDC 144

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7013(e)(3)(A)

A business shall also provide the notice to opt-out of sale/sharing in the same manner in which it collects the personal information that it sells or shares. Illustrative examples follow. (A) A business that sells or shares personal information that it collects in the course of interacting with consumers offline, such as in a brick-and-mortar store, shall provide notice through an offline method, e.g., on the paper forms that collect the personal information or by posting signage in the area where the personal information is collected directing consumers to where the notice can be found online.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7013(e)(3)(B)

A business shall also provide the notice to opt-out of sale/sharing in the same manner in which it collects the personal information that it sells or shares. Illustrative examples follow. (B) A business

that sells or shares personal information that it collects over the phone shall provide notice orally during the call when the information is collected.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7013(f)(1)

A business shall include the following in its Notice of Right to Opt-out of Sale/Sharing: (1) A description of the consumer's right to opt-out of the sale or sharing of their personal information by the business;

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7013(f)(2)

(2) Instructions on how the consumer can submit a request to opt-out of sale/sharing. If notice is provided online, the notice shall include the interactive form by which the consumer can submit their request to opt-out of sale/sharing online, as required by section 7026, subsection (a)(1). iIf the business does not operate a website, the notice shall explain the offline method by which the consumer can submit their request to opt-out of sale/sharing.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7013(g)(1)

A business does not need to provide a Notice of Right to Opt-out of Sale/Sharing or the “Do Not Sell or Share My Personal Information” link if: (1) (1) It does not sell or share personal information;

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

7013(g)(2)

A business does not need to provide a Notice of Right to Opt-out of Sale/Sharing or the “Do Not Sell or Share My Personal Information” link if: (2) It states in its privacy policy that it does not sell or share personal information

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7013(h)

A business shall not sell or share the personal information it collected during the time the business did not have a Notice of Right to Opt-out of Sale/Sharing posted unless it obtains the consent of the

consumer

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7026

Requests to Opt-Out of Sale/Sharing.

7026(a)

A business that sells or shares personal information shall provide two or more designated methods for submitting requests to opt-out of sale/sharing. A business shall consider the methods by which it interacts with consumers, the manner in which the business collects the personal information that it makes available to third parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out of sale/sharing. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer. Illustrative examples follow.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7026(a)(1)

A business that sells or shares personal information shall provide two or more designated methods for submitting requests to opt-out of sale/sharing. A business shall consider the methods by which it interacts with consumers, the manner in which the business collects the personal information that it makes available to third parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out of sale/sharing. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer. Illustrative examples follow. (1) A business that collects personal information from consumers online, shall, at a minimum, allow consumers to submit requests to opt-out of sale/sharing through an opt-out preference signal and at least one of the following methods—an interactive form accessible via the “Do Not Sell or Share My Personal Information” link, the Alternative Opt-out Link, or the business’s privacy policy if the business processes an opt-out preference signal in a frictionless manner.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 76

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control SDC 144

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7026(a)(2)

A business that sells or shares personal information shall provide two or more designated methods for submitting requests to opt-out of sale/sharing. A business shall consider the methods by which it interacts with consumers, the manner in which the business collects the personal information that it makes available to third parties, available technology, and ease of use by the consumer when

determining which methods consumers may use to submit requests to opt-out of sale/sharing. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer. Illustrative examples follow. (2) A business that interacts with consumers in person and online may provide an inperson method for submitting requests to opt-out of sale/sharing in addition to the opt-out preference signal.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7026(a)(3)

A business that sells or shares personal information shall provide two or more designated methods for submitting requests to opt-out of sale/sharing. A business shall consider the methods by which it interacts with consumers, the manner in which the business collects the personal information that it makes available to third parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out of sale/sharing. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer. Illustrative examples follow. (3) Other methods for submitting requests to opt-out of the sale/sharing include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, and a form submitted through the mail.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

7026(a)(4)

A business that sells or shares personal information shall provide two or more designated methods for submitting requests to opt-out of sale/sharing. A business shall consider the methods by which it interacts with consumers, the manner in which the business collects the personal information that it makes available to third parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out of sale/sharing. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer. Illustrative examples follow. (4) A notification or tool regarding cookies, such as a cookie banner or cookie controls, is not by itself an acceptable method for submitting requests to opt-out of sale/sharing because cookies concern the collection of personal information and not the sale or sharing of personal information. An acceptable method for submitting requests to opt-out of sale/sharing must address the sale and sharing of personal information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7026(b)

A business's methods for submitting requests to opt-out of sale/sharing shall be easy for consumers to execute, shall require minimal steps, and shall comply with section 7004

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control SDC 76

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

Control SDC 144

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

7026(c)

A business shall not require a consumer submitting a request to opt-out of sale/sharing to create an account or provide additional information beyond what is necessary to direct the business not to sell or share the consumer's personal information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

7026(d)

A business shall not require request to opt-out need not be a verifiable consumer request for a request to opt-out of sale/sharing. A business may ask the consumer for information necessary to complete the request, such as information necessary to identify the consumer whose information shall cease to be sold or shared by the business. However, to the extent that the business can comply with a request to opt-out of sale/sharing without additional information, it shall do so.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

Control **SDC 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

Monitored via 2 checks

Incident Management Procedure

Incident Management Policy

Control **SDC 112**

Entity has documented guidelines on notifying customers and other stakeholders in case of a breach.

Monitored via 3 checks

Data Breach Notification Policy

Personal Data Breach Notification Procedure

PHI Data breach Notification Procedure

7026(e)

If a business, has a good-faith, reasonable, and documented belief that a request to opt-out of sale/sharing is fraudulent, the business may deny the request. The business shall inform the requestor that it will not comply with the request and shall provide to the requestor an explanation why it believes the request is fraudulent.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be

retained by individuals.

Monitored via 1 check

Review of the privacy policy

7026(f)(1)

A business shall comply with a request to opt-out of sale/sharing by: (1) Ceasing to sell to and/or share with third parties the consumer's personal information as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. Service providers or contractors Collecting personal information pursuant to the written contract with the business required by the CCPA and these regulations does not constitute a sale or sharing of personal information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

7026(f)(2)

A business shall comply with a request to opt-out of sale/sharing by: (2) Notifying all third parties to whom the business has sold or shared the consumer's personal information, after the consumer submits the request to opt-out of sale/sharing and before the business complies with that request, that the consumer has made a request to opt-out of sale/sharing and directing them to comply with the consumer's request and forward the request to any other person to whom the third party has made the personal information available during that time period.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

7026(f)(g)

A business may provide a means by which the consumer can confirm that their request to opt-out of sale/sharing has been processed by the business. For example, the business may display on its website “Consumer Opted Out of Sale/Sharing” or display through a toggle or radio button that the consumer has opted out of the sale of their personal information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7026(f)(h)

In responding to a request to opt-out of sale/sharing, a business may present the consumer with the choice to opt-out of the sale or sharing of personal information for certain uses as long as a single option to opt-out of the sale or sharing of all personal information is also offered. However, doing so in response to an opt-out preference signal will prevent the business from using the exception set forth in Civil Code section 1798.135, subdivision (b)(1).

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

7026(f)(i)

A business that responds to a request to opt-out of sale/sharing by informing the consumer of a charge for the use of any product or service shall comply with Article 7 and shall provide the consumer with a nNotice of fFinancial iIncentive that complies with section 7016 in its response. However, doing so in response to an opt-out preference signal will prevent the business from using the exception set forth in Civil Code section 1798.135, subdivision (b)(1).

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control SDC 144

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7026(f)(j)

A consumer may use an authorized agent to submit a request to opt-out of sale/sharing on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent does not provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf. The requirement to obtain and provide written permission from the consumer does not apply to requests made by an opt-out preference signal.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 76

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

7026(f)(k)

Except as allowed by these regulations, a business shall wait at least 12 months from the date the consumer’s request before asking a consumer who has opted out of the sale or sharing of their personal information to consent to the sale or sharing of their personal information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 76

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control SDC 144

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7015

Alternative Opt-Out Link

7015(a)

The purpose of the Alternative Opt-out Link is to provide businesses the option of providing consumers with a single, clearly-labeled link that allows consumers to easily exercise both their right to opt-out of sale/sharing and right to limit, instead of posting the two separate “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links. The Alternative Opt-out Link shall direct the consumer to a webpage that would inform them of both their right to opt-out of sale/sharing and right to limit and provide them with the opportunity to exercise both rights.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

7015(b)

A business that chooses to use an Alternative Opt-out Link shall title the link, “Your Privacy Choices” or “Your California Privacy Choices,” and shall include the following optout icon to the right or left of adjacent to the title. The link shall be a conspicuous link that complies with section 7003, subsections (c) and (d), and is located at either the header or footer of the business’s internet Homepage(s). The icon shall be approximately the same size as other icons used by the business in the header or footer of its webpage.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7015(c)(1)

The Alternative Opt-out Link shall direct the consumer to a webpage that includes the following information: (1) A description of the consumer's right to opt-out of sale/sharing and right to limit, which shall comply with section 7003, subsections (a) and (b);

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

7015(c)(2)

The Alternative Opt-out Link shall direct the consumer to a webpage that includes the following information: (2) The interactive form or mechanism by which the consumer can submit their request to opt-out of sale/sharing and their right to limit online. The method shall be easy for consumers to execute, shall require minimal steps, and shall comply with section 7004.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7016

Notice of Financial Incentive.

7016(a)

The purpose of the Notice of Financial Incentive is to explain to the consumer the material terms of a financial incentive or price or service difference the business is offering so that the consumer may make an informed decision about whether to participate. A business that does not offer a financial incentive or price or service difference is not required to provide a Notice of Financial Incentive.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

7016(b)

The Notice of Financial Incentive shall comply with section 7003, subsections (a) and (b).

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

7016(c)

The Notice of Financial Incentive shall be readily available where consumers will encounter it before opting-in to the financial incentive or price or service difference. If the business offers the financial incentive or price or service difference online, the notice may be given by providing a link that takes the consumer directly to the specific section of a business's privacy policy that contains the information required in subsection (d)

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

7016(d)

A business shall include the following in its Notice of Financial Incentive:

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

7016(d)(1)

A business shall include the following in its Notice of Financial Incentive: (1) A succinct summary of the financial incentive or price or service difference offered;

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7016(d)(2)

A business shall include the following in its Notice of Financial Incentive: (2) A description of the material terms of the financial incentive or price or service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference and the value of the consumer’s data;

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7016(d)(3)

A business shall include the following in its Notice of Financial Incentive: (3) How the consumer can opt-in to the financial incentive or price or service difference

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7016(d)(4)

A business shall include the following in its Notice of Financial Incentive: (4) A statement of the consumer’s right to withdraw from the financial incentive at any time and how the consumer may exercise that right;

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

7016(d)(5)

(5) An explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer’s data, including

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7016(d)(5)(A)

An explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer’s data, including (A) A good-faith estimate of the value of the consumer’s data that forms the basis for offering the price or service difference;

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7016(d)(5)(B)

An explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data, including (B) A description of the method(s) the business used to calculate the value of the consumer's data.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

7025

Opt-Out Preference Signals.

7025(a)

The purpose of an opt-out preference signal is to provide consumers with a simple and easyto-use method by which consumers interacting with businesses online can automatically exercise their right to opt-out of sale/sharing. Through an opt-out preference signal, a consumer can opt -out of sale and sharing of their personal information with all businesses they interact with online without having to make individualized requests with each business.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 76

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

7025(b)(1)

A business that sells or shares personal information shall process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing: (1) The signal shall be in a format commonly used and recognized by businesses. An example would be an HTTP header field or JavaScript object.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 76

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

7025(b)(2)

A business that sells or shares personal information shall process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing: (2) The platform, technology, or mechanism that sends the opt-out preference signal shall make clear to the consumer, whether in its configuration or in disclosures to the public, that the use of the signal is meant to have the effect of opting the consumer out of the sale and sharing of their personal information. The configuration or disclosure does not need to be tailored only to California or to refer to California.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

7025(c)(1)

When a business that collects personal information from consumers online receives or detects an opt-out preference signal that complies with subsection (b): (1) The business shall treat the opt-out

preference signal as a valid request to opt-out of sale/sharing submitted pursuant to Civil Code section 1798.120 for that browser or device and any consumer profile associated with that browser or device, including pseudonymous profiles. If known, the business shall also treat the opt-out preference signal as a valid request to opt-out of sale/sharing for the consumer. This is not required for a business that does not sell or share personal information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

7025(c)(2)

When a business that collects personal information from consumers online receives or detects an opt-out preference signal that complies with subsection (b): (2)The business shall not require a consumer to provide additional information beyond what is necessary to send the signal. However, a business may provide the consumer with an option to provide additional information if it will help facilitate the consumer's request to opt-out of sale/sharing. Any information provided by the consumer shall not be used, disclosed, or retained for any purpose other than processing the request to optout of sale/sharing. For example, a business may give the consumer the option to provide information that identifies the consumer so that the request to opt-out of sale/sharing can apply to offline sale or sharing of personal information. However, if the consumer does not respond, the business shall still

process the opt-out preference signal as a valid request to opt-out of sale/sharing for that browser or device and any consumer profile the business associates with that browser or device, including pseudonymous profiles.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

7025(c)(3)

When a business that collects personal information from consumers online receives or detects an opt-out preference signal that complies with subsection (b): (3)If the opt-out preference signal conflicts with a consumer's business-specific privacy setting that allows the business to sell or share their personal information, the business shall process the opt-out preference signal as a valid request to opt-out of sale/sharing, but may notify the consumer of the conflict and provide the consumer with an opportunity to consent to the sale or sharing of their personal information. The business shall comply with section 7004 in obtaining the consumer's consent to the sale or sharing of their personal information. If the consumer consents to the sale or sharing of their personal information, the business may ignore the opt-out preference signal for as long as the consumer is known to the business.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 76

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

7025(c)(4)

When a business that collects personal information from consumers online receives or detects an opt-out preference signal that complies with subsection (b): (4) If the opt-out preference signal conflicts with the consumer's participation in a business's financial incentive program that requires the consumer to consent to the sale or sharing of personal information, the business may notify the consumer that processing the opt-out preference signal as a valid request to opt-out of sale/sharing would withdraw the consumer from the financial incentive program and ask the consumer to affirm that they intend to withdraw from the financial incentive program. If the consumer affirms that they intend to withdraw from the financial incentive program, the business shall process the consumer's request to opt-out of sale/sharing. If the business asks and the consumer does not affirm their intent to withdraw, the business may ignore the opt-out preference signal with respect to that consumer's participation in the financial incentive program for as long as the consumer is known to the business. . If the business does not ask the consumer to affirm their intent with regard to the financial incentive program, the business shall still process the opt-out preference signal as a valid request to opt-out of sale/sharing for that browser or device and any consumer profile the business associates with that browser or device.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 76

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

7025(c)(5)

When a business that collects personal information from consumers online receives or detects an opt-out preference signal that complies with subsection (b): (5) Where the consumer is known to the business, the A business shall not interpret the absence of an opt-out preference signal after the consumer previously sent an opt-out preference signal as consent to opt-in to the sale or sharing of personal information.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

7025(c)(6)

When a business that collects personal information from consumers online receives or detects an opt-out preference signal that complies with subsection (b): (6) A business may display whether it has processed the consumer's optout preference signal as a valid request to opt-out of sale/sharing on its website. For example, the business may display on its website "Opt-Out Preference Signal Honored" when a browser, device, or consumer using an opt-out preference signal visits the website, or display through a toggle or radio button that the consumer has opted out of the sale of their personal information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

7025(c)(7)(A)

Illustrative examples follow. (A) Caleb visits Business N's website using a browser with an opt-out preference signal enabled, but he is not otherwise logged into his account and the business cannot otherwise associate Caleb's browser with a consumer profile the business maintains. Business N collects and shares Caleb's personal information tied to his browser identifier for cross-contextual advertising. Upon receiving the opt-out preference signal, Business N shall stop selling and sharing Caleb's information linked to Caleb's browser identifier for cross-contextual advertising, but it would not be able to apply the request to opt-out of the sale/sharing to Caleb's account information because the connection between Caleb's browser and Caleb's account is not known to the business.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

7025(c)(7)(B)

Illustrative examples follow. (B) Noelle has an account with Business O, an online retailer who manages consumer's privacy choices through a settings menu. Noelle's privacy settings default to allowing Business O to sell and share her personal information with the business's marketing partners. Noelle enables an opt-out preference signal on her browser and then visits Business O's website. Business O recognizes that Noelle is visiting its website because she is logged into her account. Upon receiving Noelle's opt-out preference signal, Business O shall treat the signal as a valid request to opt-out of sale/sharing and shall apply it to her device and/or browser and also to her account and any offline sale or sharing of personal information. Business O may inform Noelle that her opt-out preference signal differs from her current privacy settings and provide her with an opportunity to consent to the sale or sharing of her personal information, but it must process the request to opt-out of sale/sharing unless Noelle instructs otherwise. Business O must also wait at least 12 months before asking Noelle to opt-in to the sale or sharing of her personal information in accordance with section 7026, subsection (k). In addition, Business O's notification would not allow it to fall within the exception set forth in Civil Code section 1798.135, subdivision (b)(1), because it would not be complying with the requirements set forth in subsection (f).

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

7025(c)(7)(C)

Illustrative examples follow. (C) Angela also has an account with Business O and has enabled an opt-out preference signal on her browser while logged into her account. Business O applies the opt-out preference signal as a valid request to opt-out of sale/sharing not only to Angela's current browser, but also to Angela's account because she is known to the business while making the request. Angela later logs into her account with Business O using that does not have the opt-out preference signal enabled. Business O shall not interpret the absence of the opt-out preference signal as consent to opt-in to the sale of personal information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

7025(c)(7)(D)

Illustrative examples follow. (D) Ramona participates in Business P's financial incentive program where she receives coupons in exchange for allowing the business to pseudonymously track and share her online browsing habits to marketing partners. Ramona enables an opt-out preference signal on her browser and then visits Business P's website. Business P knows that it is Ramona through a cookie that has been placed on her browser, but also detects the opt-out preference signal. Business P may ignore the opt-out preference signal and notify Ramona that her opt-out preference signal

conflicts with her participation in the financial incentive program and ask whether she intends to withdraw from the financial incentive program. If Ramona does not affirm her intent to withdraw, Business P may ignore the opt-out preference signal and place Ramona on a whitelist so that Business P does not have to notify Ramona of the conflict again.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

7025(c)(7)(E)

Illustrative examples follow. (E) Ramona clears her cookies and revisits Business P's website with the opt-out preference signal enabled. Business P no longer knows that it is Ramona visiting its website. Business P shall honor Ramona's opt-out preference signal as it pertains to her browser or device and any consumer profile the business associates with that browser or device.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

7025(d)

The business and the platform, technology, or mechanism that sends the opt-out preference signal shall not use, disclose, or retain any personal information collected from the consumer in connection with the sending or processing the request to opt-out of sale/sharing for any purpose other than sending or processing the opt-out preference signal.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

7025(e)

Civil Code section 1798.135, subdivisions (b)(1) and (3), provides a business the choice between (1) processing opt-out preference signals and providing the “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links or the Alternative Opt-out Link; or (2) processing opt-out preference signals in a frictionless manner in accordance with these regulations and not having to provide the “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links or the Alternative Opt-out Link. It does not give the business the choice between posting the above-referenced links or honoring opt-out preference signals. Even if the business posts the above-referenced links, the business must still process opt-out preference signals, though it may do so in a non-frictionless manner. If a business processes opt-out preference signals in a frictionless manner in accordance with subsections (f) and (g) of this regulation, then it may, but is not required to, provide the above-referenced links.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

7025(f)(1)

Except as allowed by these regulations, processing an opt-out preference signal in a frictionless manner as required by Civil Code section 1798.135, subdivision (b)(1), means that the business shall not: (1) Charge a fee or require any valuable consideration if the consumer uses an opt-out preference signal.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

7025(f)(2)

Except as allowed by these regulations, processing an opt-out preference signal in a frictionless manner as required by Civil Code section 1798.135, subdivision (b)(1), means that the business shall not: (2) Change the consumer's experience with the product or service offered by the business. For example, the consumer who uses an opt-out preference signal shall have the same experience with regard to how the business's product or service functions compared to a consumer who does not use an opt-out preference signal.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

7025(f)(3)

Except as allowed by these regulations, processing an opt-out preference signal in a frictionless manner as required by Civil Code section 1798.135, subdivision (b)(1), means that the business shall not: (3) Display a notification, pop-up, text, graphic, animation, sound, video, or any interstitial content in response to the opt-out preference signal. A business's display of whether the consumer visiting their website has opted out of the sale or sharing their personal information shall not be in violation of this regulation. The business may also provide a link to a privacy settings page, menu, or similar interface that enables the consumer to consent to the business ignoring the optout preference signal with respect to the business's sale or sharing of the consumer's personal information provided that it complies with subsections (f)(1) through (3).

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 76

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

7025(g)(1)

(g) A business meeting the requirements of Civil Code section 1798.135, subdivision (b)(1) is not required to post the “Do Not Sell or Share My Personal Information” link or the Alternative Opt-out Link if it meets all of the following additional requirements: (1) Processes the opt-out preference signal in a frictionless manner in accordance with the CCPA and these regulations.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 76

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

7025(g)(2)(A)

Includes in its privacy policy the following information: (A) A description of the consumer's right to opt-out of the sale or sharing of their personal information by the business;

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

7025(g)(2)(B)

Includes in its privacy policy the following information: (B) A statement that the business processes opt-out preference signals in a frictionless manner;

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

7025(g)(2)(C)

Includes in its privacy policy the following information: (C) Information on how consumers can implement opt-out preference signals for the business to process in frictionless manner;

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

7025(g)(2)(D)

Includes in its privacy policy the following information: (D) Instructions for any other method by which the consumer may submit a request to opt-out of sale/sharing.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

7025(g)(3)

Allows the opt-out preference signal to fully effectuate the consumer's request to optout of sale/sharing. For example, if the business sells or shares personal information offline and needs to request from the consumer additional information that is not provided by the opt-out preference signal in order to apply the request to opt-out of sale/sharing to offline sales and sharing of personal information, then the business has not fully effectuated the consumer's request to opt-out of sale/sharing. Illustrative examples follow.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control SDC 76

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

7025(g)(3)(A)

Allows the opt-out preference signal to fully effectuate the consumer's request to optout of sale/sharing. For example, if the business sells or shares personal information offline and needs to request from the consumer additional information that is not provided by the opt-out preference signal in order to apply the request to opt-out of sale/sharing to offline sales and sharing of personal information, then the business has not fully effectuated the consumer's request to opt-out of sale/sharing. Illustrative examples follow. (A) Business Q collects consumers' online browsing history and shares it with third parties for cross-contextual advertising purposes. Business Q also sells consumers' personal information offline to marketing partners. Business Q cannot fall within the exception set forth in Civil Code section 1798.135, subdivision (b)(1) because a consumer's opt-out preference signal would only apply to Business Q's online sharing of personal information about the consumer's browser or device; the consumer's opt-out preference signal would not apply to Business Q's offline selling of the consumer's information because Business Q could not apply it to the offline selling without additional information provided by the consumer, i.e., the logging into an account.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

7025(g)(3)(B)

Allows the opt-out preference signal to fully effectuate the consumer's request to optout of sale/sharing. For example, if the business sells or shares personal information offline and needs to request from the consumer additional information that is not provided by the opt-out preference signal in order to apply the request to opt-out of sale/sharing to offline sales and sharing of personal information, then the business has not fully effectuated the consumer's request to opt-out of sale/sharing. Illustrative examples follow. (B) Business R only sells and shares personal information online for cross-contextual advertising purposes. Business R may use the exception set forth in Civil Code section 1798.135, subdivision (b)(1) and not post the "Do Not Sell or Share My Personal Information" link because a consumer using an opt-out preference signal would fully effectuate their right to opt-out of the sale or sharing of their personal information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

7070

Consumers Less Than 13 Years of Age.

7070(a)

Process for Opting-In to Sale or Sharing of Personal Information

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

7070(a)(1)

Process for Opting-In to Sale or Sharing of Personal Information: (1)A business that has actual knowledge that it sells or shares the personal information of a consumer less than the age of 13 shall establish, document, and comply with a reasonable method for determining that the person consenting to the sale or sharing of the personal information about the child is the parent or guardian of that child. This consent to the sale or sharing of personal information is in addition to any verifiable parental consent required under COPPA.

INTERNAL CONTROLS AND CHECKS

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy

Vendor Management Procedure

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically 

Vendor Management Policy 

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically 

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 97**

Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.

Monitored via 1 check

Disaster recovery

7070(a)(2)(A)

Methods that are reasonably calculated to ensure that the person providing consent is the child's parent or guardian include, but are not limited to: (A) Providing a consent form to be signed by the parent or guardian under penalty of perjury and returned to the business by postal mail, facsimile, or electronic scan;

INTERNAL CONTROLS AND CHECKS

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy

Vendor Management Procedure

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically 

Vendor Management Policy 

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically 

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 97**

Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.

Monitored via 1 check

Disaster recovery ✓

7070(a)(2)(B)

Methods that are reasonably calculated to ensure that the person providing consent is the child's parent or guardian include, but are not limited to: (B) Requiring a parent or guardian, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;

INTERNAL CONTROLS AND CHECKS

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy ✓

Vendor Management Procedure ✓

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 97

Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.

Monitored via 1 check

Disaster recovery

7070(a)(2)(C)

Methods that are reasonably calculated to ensure that the person providing consent is the child's parent or guardian include, but are not limited to: (C) Having a parent or guardian call a toll-free telephone number staffed by trained personnel;

INTERNAL CONTROLS AND CHECKS

Control SDC 68

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy

Vendor Management Procedure

Control SDC 75

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 97**

Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.

Monitored via 1 check

Disaster recovery

7070(a)(2)(D)

Methods that are reasonably calculated to ensure that the person providing consent is the child's parent or guardian include, but are not limited to: (D) Having a parent or guardian connect to trained personnel via video-conference;

INTERNAL CONTROLS AND CHECKS

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy

Vendor Management Procedure

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing

Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically ✓

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 97**

Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.

Monitored via 1 check

Disaster recovery

7070(a)(2)(E)

Methods that are reasonably calculated to ensure that the person providing consent is the child's parent or guardian include, but are not limited to: (E) Having a parent or guardian communicate in person with trained personnel;

INTERNAL CONTROLS AND CHECKS

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy

Vendor Management Procedure

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 97**

Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.

Monitored via 1 check

Disaster recovery ✓

7070(a)(2)(F)

Methods that are reasonably calculated to ensure that the person providing consent is the child's parent or guardian include, but are not limited to: (F) Verifying a parent or guardian's identity by checking a form of governmentissued identification against databases of such information, as long as the parent or guardian's identification is deleted by the business from its records promptly after such verification is complete.

INTERNAL CONTROLS AND CHECKS

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy ✓

Vendor Management Procedure ✓

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 97**

Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.

Monitored via 1 check

Disaster recovery

7070(b)

When a business receives consent to the sale or sharing of personal information pursuant to subsection (a), the business shall inform the parent or guardian of the right to opt-out of sale/sharing and of the process for doing so on behalf of their child pursuant to section 7026, subsections (a)-(f).

INTERNAL CONTROLS AND CHECKS

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy

Vendor Management Procedure

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 97**

Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.

Monitored via 1 check

Disaster recovery

7070(c)

A business shall establish, document, and comply with a reasonable method, in accordance with the methods set forth in subsection (a)(2), for determining that a person submitting a request to delete, request to correct, or request to know the personal information of a child under the age of 13 is the parent or guardian of that child.

INTERNAL CONTROLS AND CHECKS

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy

Vendor Management Procedure

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 97**

Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.

Monitored via 1 check

Disaster recovery

7024

Requests to Know

7024(a)

For requests that seek the disclosure of specific pieces of information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 5, the business shall not disclose any specific pieces of personal information to the requestor and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall also evaluate the consumer's request as if it is seeking the disclosure of categories of personal information about the consumer pursuant to subsection (b).

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

Control **SDC 114**

Entity appoints a Privacy Officer to assess and facilitate the entity's compliance with relevant regulatory requirements.

Monitored via 1 check

Privacy officer should be assigned

7024(b)

For requests that seek the disclosure of categories of personal information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 5, the business may deny the request to disclose the categories and other information

requested and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall provide or direct the consumer to its Information Practices set forth in its privacy policy.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7024(c)

In responding to a request to know, a business is not required to search for personal information if all of the following conditions are met:

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7024(c)(1)

In responding to a request to know, a business is not required to search for personal information if all of the following conditions are met: (1)The business does not maintain the personal information in a searchable or reasonably accessible format;

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7024(c)(2)

In responding to a request to know, a business is not required to search for personal information if all of the following conditions are met: (2) The business maintains the personal information solely for legal or compliance purposes;

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7024(c)(3)

In responding to a request to know, a business is not required to search for personal information if all of the following conditions are met: (3) The business does not sell the personal information and does not use it for any commercial purpose; and

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7024(c)(4)

In responding to a request to know, a business is not required to search for personal information if all of the following conditions are met: (4) The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7024(d)

A business shall not disclose in response to a request to know a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics. The business shall, however, inform the consumer with sufficient particularity that it has collected the type of information. For example, a business shall respond that it collects "unique biometric data including a fingerprint scan" without disclosing the actual fingerprint scan data.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7024(e)

If a business denies a consumer's verified request to know specific pieces of personal information, in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA, the business shall inform the requestor and explain the basis for the denial, unless prohibited from doing so by law. If the request is denied only in part, the business shall disclose the other information sought by the consumer.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7024(f)

A business shall use reasonable security measures when transmitting personal information to the consumer.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7024(g)

If a business maintains a password-protected account with the consumer, it may comply with a request to know by using a secure self-service portal for consumers to access, view, and receive a portable copy of their personal information if the portal fully discloses the personal information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 5.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7024(h)

In response to a request to know, a business shall provide all the personal information it has collected and maintains about the consumer on or after January 1, 2022, including beyond the 12-month period preceding the business's receipt of the request, unless doing so proves impossible or would involve disproportionate effort, or the consumer requests data for a specific time period. That information shall

include any personal information that the business's service providers or contractors Collected pursuant to their written contract with the business. If a business claims that providing personal information beyond the 12-month period would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot provide personal information beyond the 12-month period. The business shall not simply state that it is impossible or would require disproportionate effort.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7024(i)

A service provider or contractor shall provide assistance to the business in responding to a verifiable consumer request to know, including by providing the business the consumer's personal information it has in its possession that it Collected pursuant to their written contract with the business, or by enabling the business to access that personal information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7024(j)

In responding to a consumer's verified request to know categories of personal information, categories of sources, and/or categories of third parties, a business shall provide an individualized response to the consumer as required by the CCPA. It shall not refer the consumer to the businesses' Information Practices outlined in its privacy policy unless its response would be the same for all consumers and the privacy policy discloses all the information that is otherwise required to be in a response to a request to know such categories.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7024(k)

In responding to a verified request to know categories of personal information, the business shall provide:

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7024(k)(1)

In responding to a verified request to know categories of personal information, the business shall provide: (1) The categories of personal information the business has collected about the consumer

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7024(k)(2)

In responding to a verified request to know categories of personal information, the business shall provide: (2) The categories of sources from which the personal information was collected;

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7024(k)(3)

In responding to a verified request to know categories of personal information, the business shall provide: (3) The business or commercial purpose for which it collected or sold the personal information;

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7024(k)(4)

In responding to a verified request to know categories of personal information, the business shall provide: (4) The categories of third parties with whom the business shares personal information;

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7024(k)(5)

In responding to a verified request to know categories of personal information, the business shall provide: (5) The categories of personal information that the business sold, and for each category identified, the categories of third parties to whom it sold that particular category of personal information;

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7024(k)(6)

In responding to a verified request to know categories of personal information, the business shall provide: (6) The categories of personal information that the business disclosed for a business Purpose, and for each category identified, the categories of third parties to whom it disclosed that particular category of personal information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7024(l)

A business shall identify the categories of personal information, categories of sources of personal information, and categories of third parties to whom a business sold or disclosed personal information, in a manner that provides consumers a meaningful understanding of the categories listed.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7060

General Rules Regarding Verification

7060(a)

For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 5, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7060(b)

A business shall not require a consumer to verify their identity to make a request to opt-out of sale/sharing or to make a request to limit. A business may ask the consumer for information necessary to complete the request; however, it shall not be burdensome on the consumer. For example, a business may ask the consumer for their name, but it shall not require the consumer to take a picture of themselves with their driver's license.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7060(c)(1)

In determining the method by which the business will verify the consumer's identity, the business shall: (1) Whenever feasible, match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business, or use a third-party identity verification service that complies with this section.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7060(c)(2)

In determining the method by which the business will verify the consumer's identity, the business shall: (2) Avoid collecting the types of personal information identified in Civil Code section 1798.81.5, subdivision (d), unless necessary for the purpose of verifying the consumer.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7060(c)(3)(A)

Consider the following factors: (A) The type, sensitivity, and value of the personal information collected and maintained about the consumer. Sensitive personal information shall warrant a more stringent verification process.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7060(c)(3)(B)

Consider the following factors: (B) The risk of harm to the consumer posed by any unauthorized deletion, correction, or access. A greater risk of harm to the consumer by unauthorized deletion, correction, or access shall warrant a more stringent verification process.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7060(c)(3)(C)

Consider the following factors: (C) The likelihood that fraudulent or malicious actors would seek the personal information. The higher the likelihood, the more stringent the verification process shall be.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7060(c)(3)(D)

Consider the following factors: (D) Whether the personal information to be provided by the consumer to verify their identity is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7060(c)(3)(E)

Consider the following factors: (E) The manner in which the business interacts with the consumer

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7060(c)(3)(F)

Consider the following factors: (F) Available technology for verification

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7060(d)

A business shall generally avoid requesting additional information from the consumer for purposes of verification. If, however, the business cannot verify the identity of the consumer from the information already maintained by the business, the business may request additional information from the consumer, which shall only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA, security, or fraud-prevention. The business shall delete any new personal information collected for the purposes of verification as soon as practical after processing the consumer's request, except as required to comply with section 7101.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7060(e)

A business shall not require the consumer or the consumer's authorized agent to pay a fee for the verification of their request to delete, request to correct, or request to know. For example, a business may not require a consumer to provide a notarized affidavit to verify their identity unless the business compensates the consumer for the cost of notarization.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7060(f)

A business shall implement reasonable security measures to detect fraudulent identityverification activity and prevent the unauthorized deletion, correction, or access of a consumer’s personal information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7060(g)

If a business maintains consumer information that is deidentified, a business is not obligated to provide or delete this information in response to a consumer request or to reidentify individual data to verify a consumer request.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7060(h)

For requests to correct, the business shall make an effort to verify the consumer based on personal information that is not the subject of the request to correct. For example, if the consumer is contending that the business has the wrong address for the consumer, the business shall not use address as a means of verifying the consumer's identity

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7061

Verification for Password-Protected Accounts.

7061(a)

If a business maintains a password-protected account with the consumer, the business may verify the consumer's identity through the business's existing authentication practices for the consumer's account, provided that the business follows the requirements in section 7060. The business shall also require a consumer to re-authenticate themselves before deleting, correcting, or disclosing the consumer's data.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7061(b)

If a business suspects fraudulent or malicious activity on or from the password-protected account, the business shall not comply with a consumer's request to delete, request to correct, or request to know until further verification procedures determine that the consumer request is authentic and the consumer making the request is the person about whom the business has collected information. The business may use the procedures set forth in section 7062 to further verify the identity of the consumer.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7062

Verification for Non-Accountholders.

7062(a)

If a consumer does not have or cannot access a password-protected account with a business, the business shall comply with this section, in addition to section 7060.

INTERNAL CONTROLS AND CHECKS

Control **SDC 33**

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

Monitored via 2 checks

Access Control Procedure	✓
Access Control Policy	✓

Control **SDC 34**

Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.

Monitored via 6 checks

User access to critical system should be validated by roles	⏱
Role based access should be setup	✓
Access Control Procedure	✓
HR Security Procedure	✓
HR Security Policy	✓
Access Control Policy	✓

Control **SDC 35**

Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.

Monitored via 5 checks

Offboarded staff access to critical systems should be revoked	✓
Access Control Procedure	✓
HR Security Procedure	✓
HR Security Policy	✓
Access Control Policy	✓

Control **SDC 37**

Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.

Monitored via 4 checks

Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓
Access Control Procedure	✓
Access Control Policy	✓

Control **SDC 39**

Entity requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor-authentication.

Monitored via 4 checks

Access should be protected with secure login mechanism ✓
Critical systems should be protected with a secure login mechanism ✓
Access Control Procedure ✓
Access Control Policy ✓

Control **SDC 42**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

Monitored via 4 checks

Access to critical systems should be reviewed ✓
Users of critical system should be identified ✓
Access Control Procedure ✓
Access Control Policy ✓

Control **SDC 43**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

Monitored via 4 checks

Access to critical systems should be reviewed ✓
Users of critical system should be identified ✓
Access Control Procedure ✓

Access Control Policy

Control **SDC 44**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.

Monitored via 5 checks

Staff devices should have antivirus running
Endpoint Security Policy
Asset Management Policy
Physical and Environmental Security Procedure
Asset Management Procedure

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7062(b)

A business's compliance with a request to know categories of personal information requires that the business verify the identity of the consumer making the request to a reasonable degree of certainty. A reasonable degree of certainty may include matching at least two data points provided by the consumer with data points maintained by the business that it has determined to be reliable for the purpose of verifying the consumer.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7062(c)

A business's compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty. A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. If a business uses this method for verification, the business shall maintain all signed declarations as part of its record-keeping obligations.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7062(d)

A business's compliance with a request to delete or a request to correct may require that the business verify the identity of the consumer to a reasonable or reasonably high degree of certainty depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion or correction. For example, the deletion of family photographs or the correction of contact information may require a reasonably high degree of certainty, while the deletion of browsing history or correction of marital status may require only a reasonable degree of certainty. A business shall act in good faith when determining the appropriate standard to apply when verifying the consumer in accordance with these regulations.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7062(e)

Illustrative examples follow:

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7062(e)(1)

Illustrative examples follow: (1) Example 1: If a business maintains personal information in a manner associated with a named actual person, the business may verify the consumer by requiring the consumer to provide evidence that matches the personal information maintained by the business. For example, if a retailer maintains a record of purchases made by a consumer, the business may require the consumer to identify items that they recently purchased from the store or the dollar amount of their most recent purchase to verify their identity to a reasonable degree of certainty.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7062(e)(2)

Illustrative examples follow: (2) Example 2: If a business maintains personal information in a manner that is not associated with a named actual person, the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with the personal information. For example, a business may have a mobile application that collects personal information about the consumer but does not require an account. The business may determine whether, based on the facts and considering the factors set forth in section 7060, subsection (b)(3), it may reasonably verify a consumer by asking them to provide information that only the person who used the mobile application may know or by requiring the consumer to respond to a notification sent to their device.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7062(f)

A business shall deny a request to know specific pieces of personal information if it cannot verify the identity of the requestor pursuant to these regulations.

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7062(g)

If there is no reasonable method by which a business can verify the identity of the consumer to the degree of certainty required by this section, the business shall state so in response to any request and explain why it has no reasonable method by which it can verify the identity of the requestor. If the business has no reasonable method by which it can verify any consumer, the business shall explain why it has no reasonable verification method in its privacy policy. The business shall evaluate and document whether a reasonable method can be established at least once every 12 months, in connection with the requirement to update the privacy policy set forth in Civil Code section 1798.130, subdivision (a)(5).

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7022

Requests to Delete.

7022(a)

For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 5, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7022(b)(1)

A business shall comply with a consumer's request to delete their personal information by: (1) Permanently and completely erasing the personal information from its existing systems except archived or back-up systems, deidentifying the personal information; deidentifying the personal information;

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7022(b)(2)

A business shall comply with a consumer's request to delete their personal information by: (2) Notifying the business's service providers or contractors to delete from their records the consumer's personal information that they Collected pursuant to their written contract with the business, or if enabled to do so by the service provider or contractor, the business shall delete the personal information that the service provider or contractor Collected pursuant to their written contract with the business;

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7022(b)(3)

A business shall comply with a consumer's request to delete their personal information by: (3) Notifying all third parties to whom the business has sold or shared the personal information to delete the consumer's personal information unless this proves impossible or involves disproportionate effort. If a business claims that notifying some or all third parties would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot notify all third parties. The business shall not simply state that notifying all third parties is impossible or would require disproportionate effort.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7022(c)(1)

A service provider or contractor shall, with respect to personal information that they Collected pursuant to their written contract with the business and upon notification by the business, cooperate with the business in responding to a request to delete by: (1) Permanently and completely erasing the personal information from its existing systems except archived or back-up systems, deidentifying the personal information, or aggregating the consumer information, or enabling the business to do so;

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7022(c)(2)

A service provider or contractor shall, with respect to personal information that they Collected pursuant to their written contract with the business and upon notification by the business, cooperate with the business in responding to a request to delete by: (2) To the extent that an exception applies to the deletion of personal information, deleting or enabling the business to delete the consumer's personal information that is not subject to the exception and refraining from using the consumer's personal information retained for any purpose other than the purpose provided for by that exception;

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7022(c)(3)

A service provider or contractor shall, with respect to personal information that they Collected pursuant to their written contract with the business and upon notification by the business, cooperate with the business in responding to a request to delete by: (3) Notifying any of its own service providers or contractors to delete from their records in the same manner the consumer's personal information that they Collected pursuant to their written contract with the service provider or contractor

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7022(c)(4)

A service provider or contractor shall, with respect to personal information that they Collected pursuant to their written contract with the business and upon notification by the business, cooperate with the business in responding to a request to delete by: (4) Notifying any other service providers, contractors, or third parties that may have accessed personal information from or through the service provider or contractor, unless the information was accessed at the direction of the business, to delete the consumer's personal information unless this proves impossible or involves disproportionate effort.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7022(d)

If a business, service provider, or contractor stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored

on the archived or backup system, until the archived or backup system relating to that data is restored to an active system or is next accessed or used for a sale, disclosure, or commercial purpose.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7022(e)

In responding to a request to delete, a business shall inform the consumer whether or not it has complied with the consumer's request. The business shall also inform the consumer that it will maintain a record of the request as required by section 7101, subsection (a). A business, service provider, contractor, or third party may retain a record of the request for the purpose of ensuring that the consumer's personal information remains deleted from its records.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7022(f)(1)

In cases where a business denies a consumer's request to delete in whole or in part, the business shall do all of the following: (1) Provide to the consumer a detailed explanation of the basis for the denial, including any conflict with federal or state law, or exception to the CCPA, or factual basis for contending that compliance would be impossible or involve disproportionate effort, unless prohibited from doing so by law;

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7022(f)(2)

In cases where a business denies a consumer’s request to delete in whole or in part, the business shall do all of the following: (2) Delete the consumer’s personal information that is not subject to the exception;

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7022(f)(3)

In cases where a business denies a consumer’s request to delete in whole or in part, the business shall do all of the following: (3) Not use the consumer’s personal information retained for any other purpose than provided for by that exception;

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7022(f)(4)

In cases where a business denies a consumer's request to delete in whole or in part, the business shall do all of the following: (4) Instruct its service providers and contractors to delete the consumer's personal information that is not subject to the exception and to not use the consumer's personal information retained for any purpose other than the purpose provided for by that exception.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations 

7022(g)

If a business that denies a consumer's request to delete sells or shares personal information and the consumer has not already made a request to opt-out of sale/sharing, the business shall ask the consumer if they would like to opt-out of the sale or sharing of their personal information and shall include either the contents of, or a link to, the Notice of Right to Opt-out of Sale/sSharing in accordance with section 7013.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

7022(h)

In responding to a request to delete, a business may present the consumer with the choice to delete select portions of their personal information as long as a single option to delete all personal information is also offered. A business that provides consumers the ability to delete select categories of personal information (e.g., purchase history, browsing history, voice recordings) in other contexts, however, must inform consumers of their ability to do so and direct them to how they can do so. For example, a business may provide the consumer with a link to a support page or other resource that explains consumers' data deletion options

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

7050

Service Providers and Contractors.

7050(a)(1)

A service provider or contractor shall not retain, use, or disclose personal information Collected pursuant to its written contract with the business except: (1) For the specific Business Purpose(s) and service(s) set forth in, the written contract between the business and the service provider or contractor that is required by the CCPA and these regulations.;

INTERNAL CONTROLS AND CHECKS

Control SDC 21

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management

Vendor Management Policy

Vendor Management Procedure

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

7050(a)(2)

A service provider or contractor shall not retain, use, or disclose personal information Collected pursuant to its written contract with the business except: (2) To retain and employ another service provider or contractor as a subcontractor, where the subcontractor meets the requirements for a service provider or contractor under the CCPA and these regulations.;

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management

Vendor Management Policy

Vendor Management Procedure

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

7050(a)(3)

A service provider or contractor shall not retain, use, or disclose personal information Collected pursuant to its written contract with the business except: (3) For internal use by the service provider or contractor to build or improve the quality of the services it is providing to the business, even if this Business Purpose is not specified in the written contract required by the CCPA and these regulations, provided that the service provider or contractor does not use the personal information to perform services on behalf of another person Illustrative examples follow.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management

Vendor Management Policy

Vendor Management Procedure

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

7050(a)(3)(A)

For internal use by the service provider or contractor to build or improve the quality of the services it is providing to the business, even if this Business Purpose is not specified in the written contract required by the CCPA and these regulations, provided that the service provider or contractor does not use the personal information to perform services on behalf of another person Illustrative examples follow. (A) An email marketing service provider can send emails on a business's behalf using the business's customer email list. The service provider could analyze those customers' interactions with the marketing emails to improve its services and offer those improved services to everyone. But the service provider cannot use the original email list to send marketing emails on behalf of another business.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

7050(a)(3)(B)

For internal use by the service provider or contractor to build or improve the quality of the services it is providing to the business, even if this Business Purpose is not specified in the written contract required by the CCPA and these regulations, provided that the service provider or contractor does not

use the personal information to perform services on behalf of another person Illustrative examples follow. (B) A shipping service provider that delivers businesses' products to their customers may use the addresses received from their business clients and their experience delivering to those addresses to identify faulty or incomplete addresses, and thus, improve their delivery services. However, the shipping service provider cannot compile the addresses received from one business to send advertisements on behalf of another business, or compile addresses received from businesses to sell to data brokers.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

7050(a)(4)

A service provider or contractor shall not retain, use, or disclose personal information Collected pursuant to its written contract with the business except: (4) To prevent, detect, or investigate data security incidents or protect against malicious, deceptive, fraudulent or illegal activity, even if this Business Purpose is not specified in the written contract required by the CCPA and these regulations.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

7050(a)(5)

A service provider or contractor shall not retain, use, or disclose personal information Collected pursuant to its written contract with the business except: (5) For the purposes enumerated in Civil Code section 1798.145, subdivisions (a)(1) through (a)(7).

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

7050(b)

A service provider or contractor cannot contract with a business to provide crosscontextual behavioral advertising. Per Civil Code section 1798.140, subdivision (e)(6), a service provider or contractor may contract with a business to provide advertising and marketing services, but the service provider or contractor hall not combine the personal information of consumers who have opted-out of the sale/sharing that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or collects from its own interaction with consumers. A person who contracts with a business to provide cross-contextual behavioral advertising is a third party and not a service provider or contractor with respect to cross-contextual behavioral advertising services. Illustrative examples follow.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management

Vendor Management Policy

Vendor Management Procedure

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

7050(b)(1)

A service provider or contractor cannot contract with a business to provide crosscontextual behavioral advertising. Per Civil Code section 1798.140, subdivision (e)(6), a service provider or contractor may contract with a business to provide advertising and marketing services, but the service provider or contractor hall not combine the personal information of consumers who have opted-out of the sale/sharing that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or collects from its own interaction with consumers. A person who contracts with a business to provide cross-contextual behavioral advertising is a third party and not a service provider or contractor with respect to cross-contextual behavioral advertising services. Illustrative examples follow. (1) Business S, a clothing company, hires a social media company as a service provider for the purpose of providing Business S's advertisements on the social media company's platform. The social media company can serve Business S by providing non-personalized advertising services on its platform based on aggregated or demographic information (e.g., advertisements to women, 18-30 years old, that live in Los Angeles). However, it cannot use a list of customer email addresses provided by Business S to identify users on the social media company's platform to serve advertisements to them.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

7050(b)(2)

A service provider or contractor cannot contract with a business to provide crosscontextual behavioral advertising. Per Civil Code section 1798.140, subdivision (e)(6), a service provider or contractor may contract with a business to provide advertising and marketing services, but the service provider or contractor hall not combine the personal information of consumers who have opted-out of the sale/sharing that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or collects from its own interaction with consumers. A person who contracts with a business to provide cross-contextual behavioral advertising is a third party and not a service provider or contractor with respect to cross-contextual behavioral advertising services. Illustrative examples follow. (2) Business T, a company that sells cookware, hires an advertising company as a service provider for the purpose of advertising its services. The advertising agency can serve Business T by providing contextual advertising services, such as placing advertisements for Business T’s products on websites that post recipes and other cooking tips.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓

Vendor Management Policy

7050(c)

If a service provider or contractor receives a request made pursuant to the CCPA directly from a the consumer, the service provider or contractor shall either act on behalf of the business in accordance with the business's instructions for responding to the request or inform the consumer that the request cannot be acted upon because the request has been sent to a service provider or contractor.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management

Vendor Management Policy

Vendor Management Procedure

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

7050(d)

A service provider or contractor that is a business shall comply with the CCPA and these regulations with regard to any personal information that it collects, maintains, or sells outside of its role as a service provider or contractor.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

7050(e)

A person who does not have a contract that complies with section 7051, subsection (a), is not a service provider or a contractor under the CCPA. For example, a business's disclosure of personal information to a person who does not have a contract that complies with section 7051, subsection (a) may be considered a sale or sharing of personal information for which the business must provide the consumer with the right to opt-out of sale/sharing.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management

Vendor Management Policy

Vendor Management Procedure

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

7050(f)

A service provider or a contractor shall comply with the terms of the contract required by the CCPA and these regulations.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓

Vendor Management Policy

Vendor Management Procedure

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

7050(g)

Whether an entity that provides services to a Nonbusiness must comply with a consumer's CCPA request depends upon whether the entity is a "business," as defined by Civil Code section 1798.140, subdivision (d).

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓

Vendor Management Policy

Control SDC 74

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control SDC 77

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

7053

Contract Requirements for Third Parties

7053(a)(1)

A business that sells or shares a consumer’s personal information with a third party shall enter into an agreement with the third party that: (1) Identifies the limited and specified purpose(s) for which the personal information is made available to the third party sold or disclosed. The purpose shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

7053(b)

(b) Whether a business conducts due diligence of the third party factors into whether the business has reason to believe that the third party is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that never enforces the terms of the contract might not be able to rely on the defense that it did not have reason to believe that the third party intends to use the personal information in violation of the CCPA and these regulations at the time of the business disclosed the personal information to the third party.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓
Vendor Management Policy ✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management ✓
Vendor Management Policy ✓
Vendor Management Procedure ✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓
Vendor Management Policy ✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓
Vendor Management Policy ✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

7053(a)(2)

A business that sells or shares a consumer’s personal information with a third party shall enter into an agreement with the third party that: (2) Specifies that the business is making the personal information available to the third party only for the limited and specified purposes set forth within the contract and requires the third party to use it only for those limited and specified purposes.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management

Vendor Management Policy

Vendor Management Procedure

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

7053(a)(3)

A business that sells or shares a consumer’s personal information with a third party shall enter into an agreement with the third party that: (3) Requires the third party to comply with all applicable sections of the CCPA and these regulations, including—with respect to the personal information that the business makes available to the third party—providing the same level of privacy protection as required of businesses by the CCPA and these regulations. For example the contract may require the third party to comply with a consumer’s request to opt-out of sale/sharing forwarded to it by a first party business and to implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management

Vendor Management Policy

Vendor Management Procedure

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

7053(a)(4)

A business that sells or shares a consumer’s personal information with a third party shall enter into an agreement with the third party that: (4) Grants the business the right—with respect to the personal information that the business makes available to the third party—to take reasonable and appropriate steps to ensure that the third party uses it in a manner consistent with the business’s obligations under the CCPA and these regulations. For example, the business may require the third party to attest that it treats the personal information the business made available to it in the same manner that the business is obligated to treat it under the CCPA and these regulations

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

7053(a)(5)

A business that sells or shares a consumer's personal information with a third party shall enter into an agreement with the third party that: (5) Grants the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information made available to the third party. For example, the business may require the third party to provide documentation that verifies that it no longer retains or uses the personal information of consumers who have had their requests to opt-out of sale/sharing forwarded to it by the first party business.

INTERNAL CONTROLS AND CHECKS

Control SDC 21

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control SDC 29

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control SDC 30

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control SDC 74

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

7053(a)(6)

A business that sells or shares a consumer’s personal information with a third party shall enter into an agreement with the third party that: (6) Requires the third party to notify the business after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓

Vendor Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management

Vendor Management Policy

Vendor Management Procedure

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

7003

Requirements for Disclosures and Communications to Consumers.

7081

Calculating the Value of Consumer Data

7081(a)

A business offering a price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good faith method for calculating the value of the consumer's data. The business shall consider one or more of the following:

INTERNAL CONTROLS AND CHECKS

Control **SDC 19**

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 20**

Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.

Monitored via 1 check

Risk assessment should be conducted periodically ✓

Control **SDC 27**

Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.

Monitored via 2 checks

Risk assessment should be reviewed by senior management ✓

Risk Assessment & Management Policy ✓

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

Monitored via 2 checks

Risk assessment should be conducted periodically ✓

Risk Assessment & Management Policy ✓

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically ✓

7081(a)(1)

A business offering a price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good faith method for calculating the value of the consumer's data. The business shall consider one or more of the following: (1) The marginal value to the business of the sale, collection, or deletion of a consumer's data.

INTERNAL CONTROLS AND CHECKS

Control **SDC 19**

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

Monitored via 1 check

Risk assessment should be conducted periodically ✓

Control **SDC 20**

Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.

Monitored via 1 check

Risk assessment should be conducted periodically ✓

Control **SDC 27**

Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.

Monitored via 2 checks

Risk assessment should be reviewed by senior management ✓

Risk Assessment & Management Policy ✓

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

Monitored via 2 checks

Risk assessment should be conducted periodically	✓
Risk Assessment & Management Policy	✓

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically	✓

7081(a)(2)

A business offering a price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good faith method for calculating the value of the consumer’s data. The business shall consider one or more of the following: (2) The average value to the business of the sale, collection, or deletion of a consumer’s data.

INTERNAL CONTROLS AND CHECKS

Control **SDC 19**

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

Monitored via 1 check

Risk assessment should be conducted periodically	✓

Control **SDC 20**

Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.

Monitored via 1 check

Risk assessment should be conducted periodically ✓

Control **SDC 27**

Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.

Monitored via 2 checks

Risk assessment should be reviewed by senior management ✓

Risk Assessment & Management Policy ✓

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

Monitored via 2 checks

Risk assessment should be conducted periodically ✓

Risk Assessment & Management Policy ✓

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically ✓

7081(a)(3)

A business offering a price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good faith method for calculating the value of the consumer’s data. The business shall consider one or more of the following: (3) The aggregate value to the business of the sale, collection, or deletion of consumers’ data divided by the total number of consumers.

INTERNAL CONTROLS AND CHECKS

Control **SDC 19**

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

Monitored via 1 check

Risk assessment should be conducted periodically ✓

Control **SDC 20**

Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.

Monitored via 1 check

Risk assessment should be conducted periodically ✓

Control **SDC 27**

Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.

Monitored via 2 checks

Risk assessment should be reviewed by senior management ✓

Risk Assessment & Management Policy ✓

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

Monitored via 2 checks

Risk assessment should be conducted periodically ✓

Risk Assessment & Management Policy ✓

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically ✓

7081(a)(4)

A business offering a price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good faith method for calculating the value of the consumer’s data. The business shall consider one or more of the following: (4) Revenue generated by the business from sale, collection, or retention of consumers’ personal information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 19**

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

Monitored via 1 check

Risk assessment should be conducted periodically

Control SDC 20

Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.

Monitored via 1 check

Risk assessment should be conducted periodically

Control SDC 27

Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.

Monitored via 2 checks

Risk assessment should be reviewed by senior management

Risk Assessment & Management Policy

Control SDC 18

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

Monitored via 2 checks

Risk assessment should be conducted periodically

Risk Assessment & Management Policy

Control SDC 79

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically

7081(a)(5)

A business offering a price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good faith method for calculating the value of the consumer’s data. The business shall consider one or more of the following: (5) Expenses related to the sale, collection, or retention of consumers’ personal information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 19**

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 20**

Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 27**

Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.

Monitored via 2 checks

Risk assessment should be reviewed by senior management

Risk Assessment & Management Policy

Control SDC 18

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

Monitored via 2 checks

Risk assessment should be conducted periodically

Risk Assessment & Management Policy

Control SDC 79

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically

7081(a)(6)

A business offering a price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good faith method for calculating the value of the consumer’s data. The business shall consider one or more of the following: (6) Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference.

INTERNAL CONTROLS AND CHECKS

Control SDC 19

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 20**

Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 27**

Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.

Monitored via 2 checks

Risk assessment should be reviewed by senior management

Risk Assessment & Management Policy

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

Monitored via 2 checks

Risk assessment should be conducted periodically

Risk Assessment & Management Policy

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically

7081(a)(7)

A business offering a price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good faith method for calculating the value of the consumer's data. The business shall consider one or more of the following: (7) Profit generated by the business from sale, collection, or retention of consumers' personal information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 19**

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 20**

Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 27**

Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.

Monitored via 2 checks

Risk assessment should be reviewed by senior management	✓
Risk Assessment & Management Policy	✓

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

Monitored via 2 checks

Risk assessment should be conducted periodically	✓
Risk Assessment & Management Policy	✓

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically	✓

7081(a)(8)

A business offering a price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good faith method for calculating the value of the consumer’s data. The business shall consider one or more of the following: (8) Any other practical and reasonably reliable method of calculation used in good faith.

INTERNAL CONTROLS AND CHECKS

Control **SDC 19**

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

Monitored via 1 check

Risk assessment should be conducted periodically ✓

Control **SDC 20**

Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.

Monitored via 1 check

Risk assessment should be conducted periodically ✓

Control **SDC 27**

Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.

Monitored via 2 checks

Risk assessment should be reviewed by senior management ✓

Risk Assessment & Management Policy ✓

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

Monitored via 2 checks

Risk assessment should be conducted periodically ✓

Risk Assessment & Management Policy

Control SDC 79

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically

7081(b)

For the purpose of calculating the value of consumer data, a business may consider the value to the business of the data of all natural persons in the United States and not just consumers.

INTERNAL CONTROLS AND CHECKS

Control SDC 19

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

Monitored via 1 check

Risk assessment should be conducted periodically

Control SDC 20

Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 27**

Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.

Monitored via 2 checks

Risk assessment should be reviewed by senior management	✓
Risk Assessment & Management Policy	✓

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

Monitored via 2 checks

Risk assessment should be conducted periodically	✓
Risk Assessment & Management Policy	✓

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically	✓

7100

Training.

7100(a)

All individuals responsible for handling consumer inquiries about the business's Practices or the business's compliance with the CCPA shall be informed of all of the requirements in the CCPA and these regulations and how to direct consumers to exercise their rights under the CCPA and these regulations.

INTERNAL CONTROLS AND CHECKS

Control **SDC 7**

Entity provides information security and privacy training to staff that is relevant to their job function.

Monitored via 2 checks

Security training provider should be configured	✓
HR Security Policy	✓

Control **SDC 387**

Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.

Monitored via 3 checks

Infosec training should be completed by onboarded staff	✓
HR Security Procedure	✓
HR Security Policy	✓

Control **SDC 388**

Entity documents, monitors, and retains individual training activities and records.

Monitored via 2 checks

Infosec training should be completed by onboarded staff	✓
Staff should periodically complete security training	⏱

Control **SDC 383**

Entity requires that all staff members complete Information Security Awareness training annually.

Monitored via 4 checks

Infosec training should be completed by onboarded staff	✓
Staff should periodically complete security training	⏱
HR Security Procedure	✓
HR Security Policy	✓

7100(b)

A business that knows or reasonably should know that it, alone or in combination, buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year shall establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests made under the CCPA or the business's compliance with the CCPA are informed of all the requirements in these regulations and the CCPA.

INTERNAL CONTROLS AND CHECKS

Control **SDC 7**

Entity provides information security and privacy training to staff that is relevant to their job function.

Monitored via 2 checks

Security training provider should be configured	✓
HR Security Policy	✓

Control **SDC 387**

Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.

Monitored via 3 checks

Infosec training should be completed by onboarded staff	✓
HR Security Procedure	✓
HR Security Policy	✓

Control **SDC 388**

Entity documents, monitors, and retains individual training activities and records.

Monitored via 2 checks

Infosec training should be completed by onboarded staff	✓
Staff should periodically complete security training	⏱

Control **SDC 383**

Entity requires that all staff members complete Information Security Awareness training annually.

Monitored via 4 checks

Infosec training should be completed by onboarded staff	✓
Staff should periodically complete security training	⏱
HR Security Procedure	✓
HR Security Policy	✓

About Sprinto

Sprinto is a modern platform for continuous compliance monitoring. It automates the detection, remediation, and management of security risks, ensuring ongoing compliance with leading security and privacy standards.