SQUIRE PATTON BOGGS

Local Connections. Global Influence.

Preparing for 2023
State Privacy Law Compliance

August 2022

Navigating Compliance in a Patchwork of State Privacy Laws

And then there were five. Legislatures across the country have been busy in the first half of 2022 and, despite dozens of states introducing omnibus privacy bills this term, Utah and Connecticut emerged as the only two to have passed and enacted comprehensive privacy laws. They join California, Virginia and Colorado in the already vexing patchwork of state privacy laws with which organizations will have to comply starting in 2023.

Almost certainly, a greatest common factor approach may be in order with respect to certain compliance obligations. For example, the CPRA's privacy policy disclosure obligations would appear to subsume the more limited requirements under the other state laws. In addition, each of the 2023 state privacy laws' requirements as to data protection assessments are materially aligned. That said, there are a number of obligations across the 2023 state privacy laws that are sufficiently dissimilar from one another, particularly when comparing CPRA to the others, that relying on a single approach may not be possible or advisable from either a business or legal perspective. This is especially true when it comes to consumer rights more generally and also specifically with respect to digital advertising issues, where businesses are facing more than a dozen varied opt-out rights, as well as opt-in obligations for sensitive data in some states.

Another ingredient in this cocktail is the lack of regulatory certainty; the California Privacy Protection Agency (CPPA) announced that it would not meet its July 1, 2022, deadline for final regulations. In May 2022, the CCPA issued a proposed first draft of regulations and an Initial Statement of Reasons, which approved the drafts. The public comment period closed at 5 p.m. on August 23. The CCPA will then consider revisions based on those comments. Colorado is also engaged in active rulemaking activities and we can expect to see regulations there as well. As to the other states, it is not fully clear, as their statutes do not provide direct authority to an agency to issue regulations.

That is not to say organizations should not act now. Given the expansion of consumer rights and business obligations and covered data under all laws as compared to CCPA, and the expansive proviso for regulations in the CPRA, companies should spend this time, at the very least, expanding and updating their data inventories, and understand the new obligations these laws present.

By way of example:

- HR and B-to-B information comes fully into scope under CPRA.
- Sensitive data is a new concept under each of the 2023 laws, requiring either opt-in consent or application of an opt-out right.
- Data retention schedules must be understood on a category-by-category basis for CPRA.
- Changes in the digital advertising industry (i.e., the cookieless future) will require your marketing teams to engage in more complicated and privacy-invasive advertising use cases that need to be understood sooner rather than later.
- Profiling and automated decision-making will become regulated under each law, with the CPRA providing a blank slate to the CPPA on the topic to issue potentially onerous, GDPR-inspired regulations.
- The GDPR-inspired controller/processor scheme in VA, CO, UT, and CT will be new for organizations who did not deal with GDPR and involves markedly different analysis than the business/service provider construct of the CCPA/CPRA, requiring significant work on the vendor management aspect of compliance.

In addition, as organizations prepare for compliance with the 2023 state privacy laws, they should be cognizant of any non-compliance with the currently effective CCPA. The California Attorney General has provided no indication that it plans on stopping enforcement of the law between now and January 1, 2023, when it will share enforcement authority under the CPRA with the CPPA. Among others, cookie/Do Not Sell compliance, financial incentives and technical compliance with privacy policy requirements remain as enforcement priorities for the CalAG.

Below, we provide a comparative analysis of various consumer rights and businesses' obligations – comparing the state laws as to one another and to their forerunners, the CCPA and GDPR – and a suggested roadmap toward compliance for the 2023 state privacy laws.

	California Privacy Rights Act (CPRA)	Virginia Consumer Data Protection Act (VCDPA)	Colorado Privacy Act (CPA)	Utah Consumer Privacy Act (UCPA)	Connecticut SB6 (CTPA)
Overview	Amends the California Consumer Privacy Act (CCPA).	Shares similarities with California's CPRA, with additional concepts inspired by the EU's General Data Privacy Regulation (GDPR), but is sufficiently dissimilar to require a separate compliance strategy.	Largely modeled after the VCDPA, but also overlaps with California's CCPA/CPRA, and uses categories like "controller" and "processor," similar to the GDPR and VCDPA.	Largely modeled after the VCDPA, but also overlaps with the CCPA/CPRA, and uses categories like "controller" and "processor," similar to the GDPR and VCDPA.	Largely modeled after the CPA, VCDPA and UCPA, with some similarities to the CPRA (e.g., express prohibition of "dark patterns).
Effective Date (Enforcement Date and Cure)	January 1, 2023 (Enforcement begins on July 1, 2023; 30-Day Notice and Cure Provision will remain in effect indefinitely for security breach violations only).	January 1, 2023 (Enforcement begins on Effective Date; 30-Day Notice and Cure Provision will remain in effect indefinitely).	July 1, 2023 (Enforcement begins on Effective Date; 60-Day Notice and Cure Provision will remain in effect until January 1, 2025).	December 31, 2023 (Enforcement begins on Effective Date; 30-Day Notice and Cure Provision will remain in effect indefinitely).	July 1, 2023 (Enforcement begins on Effective Date; 30-Day Notice and Cure Provision will remain in effect until December 31, 2024).
Who Is Covered?	For-profit "businesses" that meet thresholds, including affiliates, joint ventures and partnerships that: 1. Have a gross global annual revenue of > US$25 million 2. Annually buy, sell or "share" for cross-context behavioral advertising purposes personal information of US$10,000 or more California consumers or households OR 3. Derive 50% or more of annual revenues from selling or "sharing" for cross-context behavioral advertising California consumers' personal information	Business entities, including for-profit and B-to-B entities, conducting business in Virginia or that produce products or services that target Virginia residents and, during a calendar year, either: 1. Control or process personal data of at least 100,000 Virginia residents OR 2. Derive 50% of gross revenue from the sale of personal data AND control or process personal data of at least 25,000 Virginia residents	Any legal entity that conducts business in Colorado or that produces or delivers commercial products or services that intentionally target Colorado residents and that satisfies one or both of the following: 1. During a calendar year, controls or processes personal data of 100,000 or more Colorado residents OR 2. Both derives revenue or receives discounts from selling personal data and processes or controls the personal data of 25,000 or more Colorado residents	Applies to "controllers" or "processors" who: 1. Conduct business in Utah or produce a product or service targeted to Utah residents 2. Have annual revenue of US$25 million or more AND 3. (a) Control or process data of 100,000 or more Utah residents in a calendar year OR (b) derive over 50% of the entity's gross revenue from the sale of personal data and control or process personal data of 25,000 or more Utah residents	Applies to individuals and entities that do business in Connecticut, or that produce products or services that are targeted to Connecticut residents, that in the preceding year either: 1. Controlled or processed the personal data of at least 100,000 Connecticut residents (excluding for the purpose of completing a payment transaction) OR 2. Controlled or processed the personal data of at least 25,000 Connecticut residents, if the individual or entity derived more than 25% of its annual gross revenue from selling personal data

Scope of Coverage

The following chart demonstrates the similarities and differences of the current US consumer privacy laws of general application, and compares them to the GDPR:

Consumer Right	GDPR	CCPA	CPRA	VCDPA	CPA	UCPA	CTPA	PICICA (NV)
Right to access	✓	✓	✓	✓	✓	✓	✓	x
Right to confirm personal data is being processed	✓	Implied	Implied	✓	✓	✓	✓	x
Right to data portability	✓	✓	✓	✓	✓	✓	✓	x
Right to delete[1]	✓	✓	✓	✓	✓	✓	✓	x
Right to correct inaccuracies/right of rectification	✓	x	✓	✓	✓	x	✓	x
Right to opt-out of sale	✓[2]	✓[3]	✓[3]	✓[4]	✓[3]	✓[4]	✓[3]	✓[5]
Right to opt-out of targeted advertising (CO, VA, UT, CT)/cross-context behavioral advertising sharing (CA)	✓	x[6]	✓	✓	✓	✓	✓	x
Right to object to or opt-out of automated decision-making	✓	x	✓[7]	x	x	x	x	x
Right to object to or opt-out of profiling[8]	✓	x	✓	✓	✓	x	✓	x
Choice required for processing of "sensitive" personal data?	Opt-In	x	Opt-Out[9]	Opt-In	Opt-In	Notice + Opp. to Opt-Out	Opt-In	x
Right to object to/restrict processing generally	✓	x	x	x	x	x	x	x
Right to non-discrimination[10]	Implied	✓	✓	✓	✓	✓	✓	x
Notice at collection requirement	✓	✓	✓	x	x	x	x	x
Specific privacy policy content requirements	✓	✓	✓	✓	✓	✓	✓	✓
Purpose/use/retention limitations	✓	Implied	✓	✓	✓	x	✓	x
Privacy and security impact assessments sometimes required	✓	x	✓	✓	✓	x	✓	x
Obligation to maintain reasonable security	✓	Implied	✓	✓	✓	✓	✓	✓

[1] In California and Utah, deletion obligations are limited to PI collected from the consumer, but in Virginia, Colorado and Connecticut, any PI collected about the consumer is in scope of the deletion right.

[2] Selling personal data under the GDPR generally would require the consent of the data subject for collection and would be subject to the right to object to processing.

[3] Any consideration sufficient, but required.

[4] Cash consideration required.

[5] In NV, website and online service operators are required to offer an "opt-out," but only for limited disclosures of certain information and only if the disclosure is made in exchange for monetary consideration.

[6] However, certain data disclosures inherent in this type of advertising are arguably a "sale," subject to opt-out rights.

[7] Subject to substantial expansion under CPRA regulations. Based on preliminary rulemaking activities, it appears that the CPPA is contemplating a GDPR-like approach for automated decision-making and profiling.

[8] CPRA's concept of profiling subject to change under the regulations. The profiling concepts in the other 2023 state privacy laws require legal or substantially similar effects.

[9] Under the CPRA, the Sensitive PI opt-out right applies to certain processing activities beyond business purposes that are to be defined in CPRA regulations.

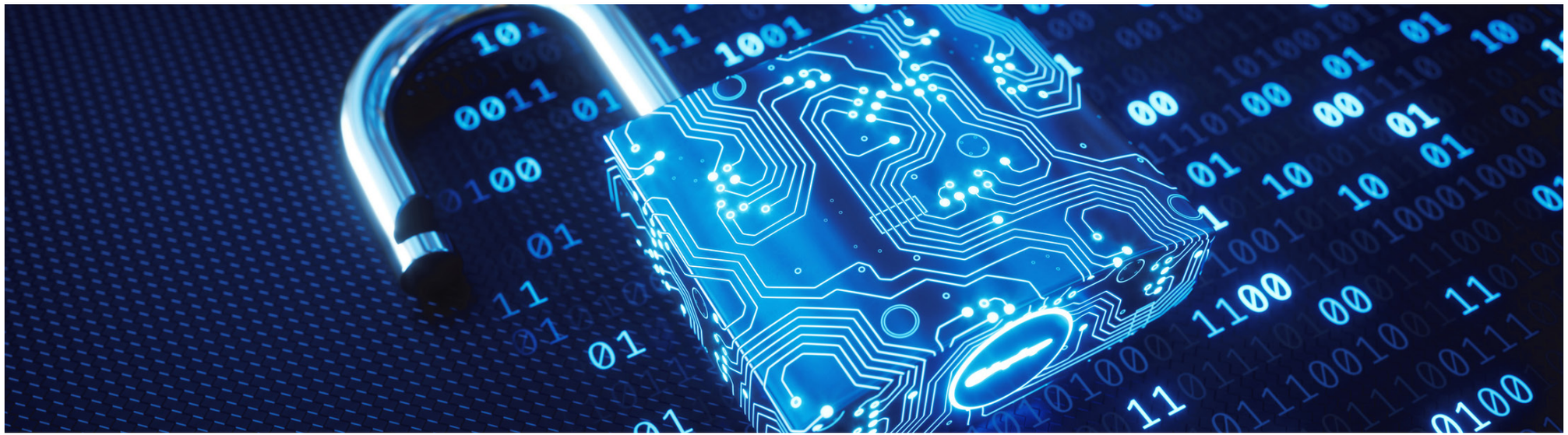
[10] The CCPA (and likely the CPRA) take a more onerous approach to non-discrimination with respect to financial incentives and price/service differences, requiring businesses to prove that they are reasonably related to the value of the consumer's data to the business.

Exemptions and Exclusions

The 2023 state privacy laws each have exclusions and exemptions, some differing from one another in meaningful ways, as illustrated below:

Exemptions and Exclusions	CPRA	VCDPA	CPA	UCPA	CTPA
Employee/HR Data	Fully in scope as of 1/1/23.	Exempt (CCPA-like exemption).	Exempt, but only in so far as maintained as an employment record.	Exempt (CCPA-like exemption).	Exempt (CCPA-like exemption).
B-to-B Contact/ Communications Data	Fully in scope as of 1/1/23.	Specifically exempt + data subjects are only consumers in so far as they act in an individual or household capacity.	Effectively exempt: data subjects are consumers in so far as they act in an individual or household capacity.	Effectively exempt: data subjects are consumers in so far as they act in an individual or household capacity.	Effectively exempt: data subjects are consumers in so far as they are not acting in a commercial or employment context.
Publicly Available	Information that is lawfully made available from federal, state or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media, or by the consumer, or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience. Excluded from the definition of PI.	Information that is lawfully made available through federal, state or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience. Excluded from the definition of PD.	Information that is lawfully made available from federal, state or local government records and information that a controller has a reasonable basis to believe the consumer has lawfully made available to the general public. Excluded from the definition of PD.	Information that a person (a) lawfully obtains from a record of a governmental entity; (b) reasonably believes a consumer or widely distributed media has lawfully made available to the general public; or (c) if the consumer has not restricted the information to a specific audience, obtains from a person to whom the consumer disclosed the information. Excluded from the definition of PD.	Information that (a) is lawfully made available through federal, state or municipal government records or widely distributed media, and (b) a controller has a reasonable basis to believe a consumer has lawfully made available to the general public. Excluded from the definition of PD.
De-identified	Excluded from the definition of PI.	Excluded from the definition of PD.	Excluded from the definition of PD.	Excluded from the definition of PD.	Excluded from the definition of PD.
Household Data	Exempt from right to delete, right to correct and right to access (Sections .105, .106, .110 and .115).	N/A.	N/A.	N/A.	N/A.

Exemptions and Exclusions	CPRA	VCDPA	CPA	UCPA	CTPA
Aggregate	Exempts aggregate consumer information from the definition of personal information.	Exempts aggregated data from the definition of personal data.	No explicit exemption, but would be exempt if failed to meet the definition of personal data.	Exempts aggregated data from the definition of personal data.	No explicit exemption, but would be exempt if failed to meet the definition of personal data.
Government Entities	Exempt as a business, but could be a service provider, contractor or third party.	Any Virginia state or local government agency or body and institutions of higher learning, as defined, are exempt.	Controllers are only regulated if they conduct business in, or produce or deliver commercial goods or services to, CO and meet the processing thresholds. Processors are any person processing on behalf of a controller.	Any government entity or third party under contract with a government entity when the third party is acting on behalf of the government entity, as well as any institution of higher learning, as defined, are exempt.	Any federal, state, municipal or other governmental authorities and institutions of higher education, as defined, are exempt.
Non-profits	Exempt as a business, but could be a service provider, contactor or third party.	Exempts certain types of non-profit organizations (corporations organized under the Virginia Nonstock Corporation Act and organizations exempt from taxation under §§501(c)(3), 501(c)(6) and 501(c)(12) of the Internal Revenue Code).	Controllers are only regulated if they conduct business in, or produce or deliver commercial goods or services to, CO and meet the processing thresholds. Processor is any person processing on behalf of a controller.	Any nonprofit corporation is exempt.	Any nonprofit organization, as defined, is exempt.



Exclusions	CPRA	VCDPA	CPA	UCPA	CTPA
GLBA/Financial Institution	The GLBA exemption in the CCPA/CPRA is data based, rather than GLBA regulated entity-based and, thus, is much narrower than the GLBA exemption in the other 2023 privacy laws.	Exempts financial institutions subject to the GLBA, plus GLBA-regulated data and "PD collected, processed, sold, or disclosed in compliance with the" FFCA.	Financial institutions subject to the GLBA, and their affiliates, plus GLBA-regulated data.	Exempts financial institutions governed by the GLBA and their affiliates, GLBA-regulated data, and personal data collected, processed, sold, or disclosed in accordance with the FFCA.	Financial institutions or data subject to Title V of GLBA exempt.
FCRA/Credit Reporting	Exempts certain activities of consumer reporting agencies, furnishers and users of consumer reports as defined by the FCRA, to the extent such activities are subject to regulation by the FCRA.	Exemption largely tracks CPRA.	Exemption largely tracks CPRA.	Exemption largely tracks CPRA.	Exemption largely tracks CPRA.
HIPAA/Health	Exempts (1) medical information governed by the CA Confidentiality of Medical Information Act (CMIA), (2) protected health information under HIPAA and CMIA providers and HIPAA, (3) providers of healthcare (CMIA) and HIPAA covered entities to the extent they protect patient data as required by the CMIA and HIPAA, respectively, and (4) certain clinical trial data and biomedical research.	Exempts covered entities and business associates, as those terms are defined by HIPAA + protected health information, as defined under HIPAA, and certain other types of health-related information.	Exempts protected health information, as defined under HIPAA, and certain other types of health-related information, much more broadly than under VCDPA or CCPA/CPRA.	Exemption largely tracks VCDPA.	Exemption largely tracks VCDPA.
COPPA/Children	CPRA shall not be deemed to conflict with obligations under the Children's Online Privacy Protection Act (COPPA).	Exempts controllers and processors that comply with the verified parental consent requirements of COPPA.	Exempts personal data that is "regulated by" COPPA provided that it is collected, processed and maintained in compliance with COPPA.	Exemption largely tracks VCDPA.	Exemption largely tracks VCDPA.

Exclusions	CPRA	VCDPA	CPA	UCPA	CTPA
FERPA/Educational	FERPA data clearly in scope, but certain exemptions regarding access to student records under the state Education Code or to opt-in use for production of physical items, such as yearbooks.	Exempts institutions of higher learning as defined by state law and personal data "regulated by" the Family Educational Rights and Privacy Act (FERPA).	Exempts personal data "regulated by" FERPA.	Exempts institutions of higher education and data regulated by FERPA.	Exempts institutions of higher education and personal data regulated by FERPA.
DPPA/Drivers Information	Exempts PI "collected, processed, sold or disclosed pursuant to the Driver's Privacy Protection Act" (DPPA).	Exempts personal data that is "collected, processed, sold, or disclosed … in compliance with" the DPPA.	Exempts personal data that is "collected, processed, sold, or disclosed … pursuant to" DPPA, if such activity "is regulated by that law."	Exemption largely tracks VCDPA.	Exemption largely tracks VCDPA.
Vehicles	Exempts vehicle information and ownership information retained or shared between manufacturers and dealers regarding motor vehicle repair and warrant use and no other purpose. Note: Not all motorized vehicles meet the definition of motor vehicle.	No specific exemption.	No specific exemption.	No specific exemption.	No specific exemption.
Air Carriers	Not exempt (but preemption savings clause).	Not exempt (but preemption savings clause).	Exempt (as defined in 49 U.S.C. §§ 40101, et seq. and 41713).	Exempt (as defined in 49 U.S.C. § 40102).	Exempts personal data collected, processed, sold or disclosed in relation to price, route or service, as such terms are defined, by an air carrier subject to 49 U.S.C. § 40101 et seq.
SEC-Regulated Securities Associations	Not exempt.	Not exempt.	Exempts SEC-registered "national securities associations."	Not exempt.	Not specifically exempt.
Public Utilities	Not specifically exempt.	Not specifically exempt.	Exempts customer data maintained by certain public utilities if "not collected, maintained, disclosed, sold, communicated, or used except as authorized by state and federal law."	Not specifically exempt.	Not specifically exempt. Note that limits on sensitive data (e.g., precise geolocation) do not apply to the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

Exclusions	CPRA	VCDPA	CPA	UCPA	CTPA
DPPA/Drivers Information	Exempts PI "collected, processed, sold or disclosed pursuant to the Driver's Privacy Protection Act" (DPPA).	Exempts personal data that is "collected, processed, sold, or disclosed … in compliance with" the DPPA.	Exempts personal data that is "collected, processed, sold, or disclosed … pursuant to" DPPA, if such activity "is regulated by that law."	Exemption largely tracks VCDPA.	Exemption largely tracks VCDPA.
Vehicles	Exempts vehicle information and ownership information retained or shared between manufacturers and dealers regarding motor vehicle repair and warrant use and no other purpose. Note: Not all motorized vehicles meet the definition of motor vehicle.	No specific exemption.	No specific exemption.	No specific exemption.	No specific exemption.
Air Carriers	Not exempt (but preemption savings clause).	Not exempt (but preemption savings clause).	Exempt (as defined in 49 U.S.C. §§ 40101, et seq. and 41713).	Exempt (as defined in 49 U.S.C. § 40102).	Exempts personal data collected, processed, sold or disclosed in relation to price, route or service, as such terms are defined, by an air carrier subject to 49 U.S.C. § 40101 et seq.
SEC-Regulated Securities Associations	Not exempt.	Not exempt.	Exempts SEC-registered "national securities associations."	Not exempt.	Not specifically exempt.
Public Utilities	Not specifically exempt.	Not specifically exempt.	Exempts customer data maintained by certain public utilities if "not collected, maintained, disclosed, sold, communicated, or used except as authorized by state and federal law."	Not specifically exempt.	Not specifically exempt. Note that limits on sensitive data (e.g., precise geolocation) do not apply to the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.
Activities Protected by Free Speech/First Amendment or Other Constitutional Rights	Exempt.	Exempt.	Exempt.	Exempt.	Exempt.

Recommendations

Below are high-level recommendations for adapting your current privacy program for compliance with the CPRA, VCDPA, CPA, UCPA and CTPA (collectively, the "2023 privacy laws"), and to help prepare for other potential new consumer privacy laws that may follow, along with a summary of workstreams to enable you to do so. A more detailed 40-page version of the workstreams for use with project management is available for a fixed fee.

1. Assess Compliance and Gaps, and Prepare a 2023 Preparedness Plan

Workstream 1: Preliminary Scoping and Information Gathering [Q2 2022]

- Conduct a readiness assessment and gap analysis based on existing privacy compliance materials developed for CCPA compliance (e.g., data maps, internal policies, external privacy policy, rights requests procedures, contracts, training, etc.) and practices (e.g., consumer rights response program, cookie consent management platform, etc.).
- Develop a detailed work plan listing all required/optional tasks to allocate roles and responsibilities and a way to track the status and completion of each task. We have tools available at a fixed fee to enable you to do this. Develop a budget tied to the project plan and obtain approval.

2. Create or Update Data Inventories or Maps and Develop and Deploy Data Management Capabilities

Workstream 2: Data Mapping [Q2 2022 and Throughout 2022]

- Update/develop data map(s) to identify how the following categories of PI1 are collected, used, transferred or disclosed, and for what purposes:
  - Sensitive data
  - B-to-B contact data
  - Employee/contractor/applicant data
- Update data map(s) to account for digital advertising use cases involving both cookie and non-cookie technology and data flows, in view of the cookieless future and new consumer rights under the 2023 state privacy laws.
- Update data maps to account for profiling and automated decision-making processes.
- Identify categories of data that may be totally or partially exempt from the CPRA, VCDPA, CPA, UCPA or CTPA, such as data regulated by the FCRA, GLBA and HIPAA, and certain educational data.
- Determine the reasonably necessary retention period, and the processing purposes, for all data, on a category-by-category basis.

3. Update Privacy Policy(ies) and Remediate Practices

Workstream 3: Annual Privacy Policy Update and Program Audit [Q2 2022]

- Data means personal information or personal data, as defined under the 2023 state privacy laws.

4. Refine Your Consumer Request Procedure

Workstream 4: Consumer Rights [2022]

- Modify processes for responding to requests to exercise existing CCPA consumer rights to address new requirements under each of the 2023 privacy laws(e.g., to reflect the longer look-back period for the right to access). In addition, you will need to expand existing rights processes to apply to B-to-B contact data and applicant/employee/contractor data for rights requests from California residents.

5. Implement Privacy-by-Design and Data Governance

Workstream 5: Privacy Impact Assessments and Cybersecurity Audits [2022]

- CPRA requires businesses that engage in high-risk processing activities to perform impact assessments that must be filed with the California Privacy Protection Agency. Similarly, the VCDPA and CPA require a controller to conduct a data protection assessment of certain processing activities, including targeted advertising, the sale of data, the processing of sensitive data and any other processing activities that present a heightened risk of harm to consumers.
- Consider a privacy impact assessment program for all data processing, to help meet purpose, proportionality, data minimization, retention and other requirements and reduce risks.

6. Update or Implement a Vendor and Data Recipient Management Program

Workstream 6: Vendor/Supplier Contracts [Q2 2022 and Throughout 2022]

- Review and, as necessary, amend/execute (upstream and downstream) contracts to ensure compliance with the 2023 privacy laws. This includes accounting for new requirements under all of the new privacy laws, but also to account for the differing controller/processor scheme under the non-CPRA laws.
- Identify any (upstream and downstream) contracts that involve the processing of "de-identified" data to include new contract terms required by the 2023 state privacy laws.

7. Update Policies

Workstream 7: Review/Develop/Update Policies [2022]

- Update/develop policies to support compliance, including:
  - Privacy policy(ies) and notices (traditional consumer-facing, internal and external HR-facing and B-to-B consumer-facing, as necessary)
  - Consumer rights procedures
  - Privacy impact assessments
  - Audit functions
  - Data retention policies and schedules
  - Record-keeping requirements

8. Implement Reporting, Record-keeping and Training

Workstream 8: Administration and Training [2022]

- Update training materials for personnel with specific responsibilities for handling consumer requests or compliance to reflect new requirements under the 2023 privacy laws. Consider broader training, especially regarding privacy impact assessments and privacy-by-design and security.
- Confirm that record-keeping and reporting meet the requirements of the final regulations, and any new rulemaking as promulgated throughout 2022.

9. Shore-up Data Security and Breach Preparedness

Workstream 9: Other Compliance (Optional But Recommended) [2022]

- Review and update a written information security program plan, including incident response plan, acceptable use policy, cookie management and vendor security program.
- Conduct privacy compliance and security breach preparedness (i.e., "tabletop") exercises.

10. Project Audit and Go-Live [Q4 2022]

Workstream 10: Final Compliance Check and Remediation

- Use a project tracker and compliance checklist to confirm that the responsible persons have signed off on the completion of each task. We have developed such a tool and provide it to clients for a fixed fee.
- Beta test and QA check the new notices and consumer rights tools before going live.

Businesses will benefit from immediately taking steps to develop and implement a 2023 state privacy laws preparedness plan and to thereafter continue to improve compliance on a risk-based basis. Doing so will further help a business prepare for additional consumer privacy laws likely to follow, at the state or federal levels, and will provide the added benefit of better understanding its data and how that can be commercially exploited in a legal and consumer-friendly manner.

Our 2023 State Privacy Compliance Taskforce

Alan L. Friel
Partner, Los Angeles
T +1 213 689 6518
E alan.friel@squirepb.com

Julia B. Jacobson
Partner, New York
T +1 212 872 9832
E julia.jacobson@squirepb.com

Kyle Fath
Partner, Los Angeles
T +1 212 872 9863
E kyle.fath@squirepb.com

Colin Jennings
Partner, Cleveland

Kristin Bryan
Partner, Cleveland

Glenn Brown
Of Counsel, Atlanta

Shea Leitch
Of Counsel, Washington DC

Elizabeth Berthiaume
Associate, Dallas

Kyle Dull
Senior Associate, New York

Niloufar Massachi
Associate, Los Angeles

David Oberly
Senior Associate, Cincinnati

Gicel Tomimbang
Associate, Los Angeles

SQUIRE PATTON BOGGS

squirepattonboggs.com

51550/08/22