SQUIRE PATTON BOGGS

PROJECT WORKSTREAMS FOR THE CALIFORNIA PRIVACY RIGHTS ACT ("CPRA") AND THE VIRGINIA CONSUMER DATA PROTECTION ACT ("CDPA")

*Below are proposed project workstreams for compliance with both the CPRA and CDPA. Most requirements are imposed only on a **business** ("controllers" under the CDPA); **service providers** ("processors" under the CDPA), by contrast, are mainly required to use personal information ("PI") only to provide services to the business/controller and help honor consumer rights. Under the CPRA, **contractors** are entities to whom a business makes PI available for a business purpose (there is no equivalent under the CDPA). This document assumes that the organization is subject to CCPA. A set of detailed work streams, which can be customized, along with a comprehensive project plan and compliance checklist that provides all obligations, with citations noted, and details what will need to be done to meet each obligation, and includes columns to track time goals and progress and to identify the responsible parties, is available. For more information contact Alan.Friel@SquirePB.com.*

WORKSTREAM #1: Preliminary Scoping and Information Gathering

- ☐ Task: Assess whether and to what extent the CPRA and CDPA applies to each of the entities within the organization and determine their respective classification (*e.g.*, business/controller, service provider/processor, contractor, etc.).
- ☐ Task: Gather existing privacy compliance materials developed for CCPA compliance (*e.g.*, data maps, internal policies, external privacy policy, rights requests procedures, contracts, training, etc.). Identify the gaps between any existing CCPA program and requirements of the CPRA or CDPA to inform the work streams below.
- ☐ Task: Confirm that you have a reasonable, documented basis for concluding that its processing of PI is "reasonably necessary and proportionate" to achieve the purposes for which the PI is collected or processed. This data minimization principle is a requirement under the CPRA and the CDPA.
- ☐ Task (Optional): Develop a detailed work plan listing all required/optional tasks to allocate roles and responsibilities.

WORKSTREAM #2: Data Mapping[1]

- ☐ Task: Update/develop data map(s) to identify how the following categories of PI are collected, used, transferred or disclosed and for what purposes:
  - *Sensitive PI*- this is a new category of PI under the CPRA[2] and is also found in the CDPA[3];
  - *B2B Contact PI*- the exemption under CCPA for this type of PI will expire on January 1, 2023; this type of PI is not subject to the CDPA; and

[1] Neither the CPRA nor the CDPA expressly require a "data map." However, it is a very valuable exercise to facilitate compliance generally (*e.g.*, preparing an accurate privacy policy, complying with consumer rights requests). We suggest focusing (at least at first) on data that you handle in the capacity as a business/controller.

[2] The CPRA generally defines the term to include, among other things, PI that reveals a consumer's: (a) social security, driver's license, state identification card, or passport number; (b) account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; (c) precise geolocation; (d) racial or ethnic origin, religious or philosophical beliefs, or union membership; (e) mail, email, and text messages unless the business is the intended recipient of the communication; and (f) genetic data.

[3] The CDPA defines the term to include PI revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; the processing of genetic or biometric data for the purpose of uniquely identifying a natural person; PI collected from a known child; and precise geolocation data.

- *Employee/Contractor PI*- the exemption under CCPA for this type of PI will expire on January 1, 2023; this type of PI is not subject to the CDPA.

☐ Task: Determine which entities within the organization, if any, qualify for the entity-level exemptions in the CDPA for financial institutions subject to Title V of the federal Gramm-Leach-Bliley Act or for covered entities or business associates governed by the Health Insurance Portability and Accountability Act.

☐ Task: Identify categories of PI that may be totally or partially exempt from CPRA or CDPA, such as PI regulated by the FCRA, GLBA and HIPAA and certain educational data.

☐ Task: Determine the reasonably necessary retention period, and the processing purposes, for all PI.

☐ Task (Optional): Conduct "training" sessions to guide internal personnel assisting with data gathering/mapping how to conduct exercise and/or prepare written guidance. If not already using a data mapping and management platform, consider doing so as part of the data mapping update.

WORKSTREAM #3: Privacy Policy (External-Facing)

☐ Task: Update the organization's CCPA-compliant privacy policy to include certain new disclosures required by the CPRA and CDPA.

WORKSTREAM #4: Consumer Rights

☐ Task: Modify processes for responding to requests to exercise existing CCPA consumer rights to address new CPRA and CDPA requirements; *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 B2B contact PI and employee/contractor PI for rights requests from California residents.

☐ Task: Develop substantive processes to honor new consumer rights provided by the CPRA and CDPA- the rights to correct PI, to opt-out of "sharing"[4] or "targeted advertising"[5], to limit the use and disclosure of "sensitive" PI and to opt out of profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.[6]

☐ Task: Develop substantive processes to comply with new CPRA regulations (once issued) granting rights to access and opt-out of automated decision-making.

WORKSTREAM #5: Privacy Impact Assessments and Cybersecurity Audits

☐ Task: CPRA requires businesses that engage in high-risk processing activities to perform privacy impact assessments that must be filed with the California Privacy Protection Agency. The specific requirements, including what constitutes high-risk processing activities, are to be developed through rulemaking. Similarly, the CDPA requires a controller to conduct a data protection assessment of certain processing activities, including targeted advertising, the sale of PI, the processing of sensitive PI and any other processing activities that present a heightened risk of harm to consumers. The Virginia Attorney General may request such assessments, but controllers are not required to submit them to the Attorney General absent a request.

☐ Task: CPRA requires businesses that engage in high-risk processing activities to perform cybersecurity audits, with the specifics to be developed through rulemaking.

---

[4] Under the CPRA, "sharing" is generally defined as disclosing a consumer's PI to a third party for the purpose of "cross contextual behavioral advertising" to the consumer based on the consumer's PI obtained from his or her activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.

[5] Under the CDPA, "targeted advertising" is generally defined as displaying advertisements to a consumer where the advertisement is selected based on PI obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests.

[6] Under the CDPA, this generally means any form of automated processing to evaluate or predict a consumer's economic situation, health, personal preferences, location, or movements, in connection with a controller's decision that results in the provision or denial to the consumer of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water.

- ☐ Task (Optional): Consider a privacy impact assessment program for all PI processing, to help meet purpose, proportionality, data minimization and other requirements and reduce risks.

WORKSTREAM #6: Vendor/Supplier Contracts

- ☐ Task: Review and, as necessary, amend/execute (upstream and downstream) contracts to ensure compliance with CPRA and CDPA (mainly prohibiting secondary uses, allowing for audits and requiring assistance honoring consumer rights) and to avoid transfers of PI being considered a "sale" under the CPRA and to address expanded deletion requirements.
- ☐ Task: Identify any (upstream and downstream) contracts that involve the processing of "de-identified" data to include new contract terms required by CPRA and CDPA.
- ☐ Task: Prepare/update template agreements with appropriate CPRA and CDPA language.
- ☐ Task (Optional): Prepare/update any contracting "playbooks" with key provisions, fallback language, and explanations reflecting new CPRA and CDPA requirements.

WORKSTREAM #7: Develop/Update Policies (Internal-Facing)

- ☐ Task: Update/develop policies to support CPRA and CDPA compliance, including privacy policy, consumer rights procedures, privacy impact assessments, audit functions, data retention policy and schedules, routine updates (to data map, privacy policy, etc.), retention limitations, and training and record keeping requirements and best practices.

WORKSTREAM #8: Training

- ☐ Task: Update training materials for employees with specific responsibilities for handling consumer requests to reflect new CPRA and CDPA requirements. Consider broader training, especially regarding privacy impact assessments and privacy-by-design.
- ☐ Task (Optional): Update any explanatory business guidance documents on critical aspects of the CPRA or CDPA (*e.g.*, definition of "sensitive" PI, what constitutes a "sale/share," activities that may be impermissible "discrimination," service providers/processors vs. contractors vs. third parties, de-identification requirements, comparisons to CCPA, etc.).

WORKSTREAM #9: Security and Compliance

- ☐ Task: Assess data security and remediate vulnerabilities. If this is done at direction of outside counsel there is a basis for taking the position that the work and work product are privileged.
- ☐ Task (Optional): Review and update Written Information Security Program plan, including incident response plan, acceptable use plan, and vendor management program.
- ☐ Task (Optional): Review and update security safeguards to meet California's "reasonableness" standard (which will avoid statutory damage claims for a data breach).
- ☐ Task (Optional): Conduct privacy and security breach preparedness (i.e., "tabletop") exercises.