MEMO

From: Andrew Mirsky (Mirsky & Company, PLLC)
Date: March 9, 2023
Re: **State Law Privacy Compliance – Compliance Checklist**

Below is a checklist for compliance (summary checklist + detail) with new or amended state consumer privacy laws in California, Colorado, Connecticut, Utah and Virginia. While the laws are all effective beginning in January 2023, California in particular (with the strictest and most comprehensive requirements among these laws) will not enforce compliance until July 2023. Please let me know if you need assistance with implementing these recommendations. Andy Mirsky

State Law Privacy Compliance

New or amended laws (effective 2023) in CA, CO, CT, UT and VA

Compliance Checklist

(SUMMARY)

2 things to do first:

1. Determine which state laws apply to your business. CA has the strictest (and most comprehensive) requirements and almost certainly applies to any business with a national reach. Other states have enacted similar and sometimes conflicting requirements. Some compliance requirements are unique to just one state, and some are common among several states and for GDPR.

2. Map or inventory all PI your business processes. Document all personal data that your business holds or processes. You likely did this in 2018 and 2020 to comply with GDPR and CCPA. Bring it up to date, but CA now requires inclusion of personal data of employees and job applicants. This may simply involve updating data mapping you did previously. Please see the detail (attached) for examples.

4 external-facing things to do:

1. Update your public-facing privacy policy. In particular: New disclosure requirements about collecting "sensitive information", processing PI for targeted advertising and automated decision-making or data profiling. Please see the detail (attached) for specific changes. Please also contact me for examples.

2. Update contracts with your customers and service providers. If you receive PI from other businesses (clients, customers, other data sources) or if you transfer PI to other businesses (technology partners, vendors, subcontractors), the new or amended consumer privacy laws require written contracts with those other businesses. This requirement is not new, but it is newly important with increasingly detailed requirements, typically under a Data Processing Addendum (DPA). You may already have some of these DPAs in place, and please see the detail (attached) for specific changes. Please also contact me for examples.

3. Update / install new homepage opt-out buttons. Required to allow opt-outs of "Selling" or "Sharing" PI, and to opt-out of processing "sensitive information". If you do not engage in these activities, some or all of these requirements will not apply to your business. NOTE: Transfers of PI to a vendor for ccb advertising = "Sharing" (requiring opt-out button). But transfers of PI for other purposes (non-ccb advertising) is generally not "Sale" or "Sharing". Please see the detail (attached) for the specific requirements.

4. Implement affirmative consent (opt-in) for collecting "sensitive information" or collecting PI for targeted advertising. Required where you collect information directly from individuals, rather than indirectly via 3rd parties. BUT: In those cases, you must get contract assurances of compliance from the 3rd party. Please see the detail (attached) for the specific requirements.

6 internal things to do:

1. Conduct Data Protection Impact Assessment(s) (DPIAs) (particularly if you use PI for targeted advertising, profiling or if you process "sensitive data"). A DPIA is a formal, written internal audit where you assess a proposed product or service involving PI by comparing the benefits (for your business, consumers and other stakeholders) with potential risks (to consumer rights), together with an operational plan to minimize those risks. DPIAs have been required in the EU under GDPR since 2018 and are a new (2023) requirement in the US under various state laws when your business provides certain types of services, particularly targeted advertising, profiling or if you process "sensitive data". Please see the detail (attached) for specifics. Please also contact me for examples.

2. Implement new HR data privacy requirements. HR data *had* been exempted from CA compliance requirements, but that exemption ended on December 31, 2022. New specific requirements: (a) Separate privacy policy for HR Data and (b) written notice at collection to employees (current and former), contractors and job applicants (whether or not hired). Please see the detail (attached) for specifics. Please also contact me for examples.

3. DSARs: Revise SOPs for receiving and responding to consumer data access requests (DSARs). Medium-size list of consumer data subject access rights (DSARs) under the various state laws (and GDPR), but also important new opt-out rights from "Selling" and "Sharing" PI. Revise your SOP (or create new SOP) for receiving and responding to DSARs. This may simply involve updating your existing SOP, which should include processes for validating identification of requestors. Please also contact me for examples.

4. Review and update your data security and other internal policies to align with new privacy requirements. Examples: Business Continuity, Disaster Recovery and Incident Response Policies. And if you haven't already done so, create and adopt these important internal security policies. Please contact me for examples of these policies. Implementation should be led by someone internally.

5. Review and update data security controls: "Reasonable and proportional technical, organizational and physical security measures". Guidelines: Statutory and regulatory requirements, industry best practices (including self-regulatory principles) and contract requirements. Please contact me for guidelines, but this should be led by someone internally.

6. Train your people: Conduct training (ongoing, regular, mandatory) for all staff on PI privacy responsibilities and data security controls. Conduct (or continue to conduct) a regular training program for incident response and day-to-day compliance measures. You can create an internal training program or engage external professional trainings. I can also help in various ways, including with training materials and conducting regular training.

[Please see the following pages for detailed guidance on the above requirements.]

State Law Privacy Compliance
New or amended laws (effective 2023) in CA, CO, CT, UT and VA
Compliance Checklist
(DETAILED)

Do these 2 things first.

1. Determine which state laws apply to your business. Why this matters? This compliance checklist is a practical but general guide for most businesses for most state requirements. CA has the strictest (and most comprehensive) requirements and almost certainly applies to any business with a national reach. Other states have enacted similar and sometimes conflicting requirements. Some compliance requirements are unique to just one state, and some are common among several states and for GDPR. Depending on where your business is located and where your business operates (separate questions), you may be subject to additional state-based requirements. For these reasons, a national compliance approach may make practical sense for your business, but please discuss your specific circumstances with legal counsel.

- **CA:** Any for-profit business that operates in CA and (a) has a gross annual revenue of at least $25 million; (b) buys, sells, or shares personal data of at least 100,000 CA residents or households or (c) derives at least 50% of its revenue from selling or sharing personal data of CA residents.
- **CO:** Any for-profit business that operates in CO or targets products and services at residents of CO *and* either (a) annually processes PI of at least 100,000 CO residents or (b) benefits via revenue or discounts on goods by selling personal data.
- **CT:** Any business (including not-for-profits) that operates in CT or targets products and services at residents of CT which controls or processes the personal data of (a) at least 100,000 consumers or (b) 25,000 consumers and derives at least 25% of gross revenue from the sale of personal data.
- **UT:** Any business (including not-for-profits) that (a) operates in UT, and (b) has an annual gross revenue of at least $25 million and (c) (i) annually controls or processes the personal data of at least 100,000 UT residents or (ii) controls or processes the personal data or at least 25,000 UT residents and derives at least 50% of its annual revenue from sale of personal data.
- **VA:** Any for-profit business that operates in VA or targets products and services at residents of VA and either (a) annually processes PI of at least 100,000 VA residents or (b) at least 50% of whose annual revenue is derived from sale of personal data.

2. Map or inventory all PI your business processes. Document all PI that your business holds or processes. You likely did this in 2018 and 2020 to comply with GDPR and CCPA. Bring it up to date, and CA now requires inclusion of PI of employees (including 1099 contractors) and job applicants.

- What is a Data Map? A visual, consolidated record of all PI "processed" by your business (collecting, use, retention and storage, and transfers), categories of PI and categories of data subjects, categories of recipients to whom PI is disclosed, and time limits for erasure.
- Why a Data Map? Compliance with (a) recordkeeping obligations (various US state laws, GDPR), (b) your own Privacy Policy, (c) data security obligations (you can't secure it if you can't locate it!), (d) responding to data access requests and (e) data breach response obligations.
- What does the Data Map show? (a) why data is collected, (b) types of data collected, (c) types of individuals whose data is collected, (d) sources of the data, legal basis of data collection and use, (e) how data is used (and by whom), (f) how and where data is stored (and for how long) and (g) to whom data is transferred.
- Employee Data (new CA requirement): Important to now include PI of employees (current and former), contractors (including freelancers and consultants), and job applicants.

This may simply involve updating data mapping you did previously. In addition, these resources should be helpful guidance and examples:

* Get started organizing and inventorying your data with this easy-to-use questionnaire: https://mstreetlegal.com/s/Data-Inventory-Worksheet-Questionnaire.pdf

* An excellent 1-page illustration of a data map/data inventory published by the Isle of Man (UK) government, visually showing the "why, who, when, where and what" for mapping PI of your business: https://mstreetlegal.com/s/Data-Map-Visual-Example.pdf

4 external-facing things to do.

1. Update your public-facing privacy policy. In particular: New disclosure requirements about collecting "sensitive information", processing PI for targeted advertising and automated decision-making or data profiling. Specific requirements to add to the Privacy Policy (if not already included):

- Whether (or not) the business collects and processes "sensitive data" and whether that information is sold to or shared with third parties. If the business does collect "sensitive data", disclosure of the categories of "sensitive data" you collect. ("Sensitive information" refers to private personal data, for example passport number, driver's license number, social security number, health information, information about racial and ethnic origin or religious beliefs, and financial information.)
- Whether (or not) the business uses PI for automated decision-making or data profiling.
- Whether (or not) the business processes PI for targeted advertising.
- Data retention periods for each category of PI that you collect. Or, if that is not practical, the criteria used to determine retention periods.
- New data access and opt-out rights for individuals, with clear instructions on how individuals may exercise these rights. (See section below discussing these rights.)
- Individuals' rights to appeal decisions by the business on individual data access rights requests, and information on how to submit appeals.
- Whether (or not) the business recognizes and complies with a consumer's browser opt-out preference signal to opt-out of the Sale or Sharing of PI and to limit the use of "sensitive data".

Please contact me for examples.

2. Update contracts with your customers and service providers. The new or amended consumer privacy laws require written contracts documenting all relationships with third parties involving sharing or receiving PI. Includes all contracts with technology and data providers you receive PI from or provide PI to: Vendors, subcontractors, data sources and other technology providers. Includes all contracts with customers you receive PI from or provide PI to. 2 categories of contracts:

- Contracts with third parties to whom you transfer PI or give access to PI.
- Contracts with third parties from whom you receive PI or access to PI.

The written contract requirement is not new (already required under GDPR and CCPA), but it is newly important with increasingly detailed requirements, typically under a Data Processing Addendum (DPA). Specific requirements to add to contracts (if not already included):

- Instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties.
- Prohibiting service providers from retaining, using, or disclosing PI outside of the direct business relationship with the business.

- Prohibiting service providers from combining PI received from one business with information received from another business.
- Requiring service providers to provide the same level of privacy protections as required by the various privacy laws.
- Prohibiting service providers from Selling or Sharing PI.
- Requiring service providers and third parties to comply with notifications from the business to delete an individual's PI upon receiving the individual's request, to opt-out of Sharing PI and to opt-out from Sales of PI.

Please contact me for examples.

3. Update / install new homepage opt-out buttons.

Website homepage buttons required to allow opt-outs of "Selling" or "Sharing" PI, and to opt-out of processing "sensitive information". NOTE: Transfers of PI to a vendor for targeted advertising = "Sharing" (requiring opt-out button). Transfers of PI for many other purposes (non- targeted advertising) is not a "Sale" or "Sharing" of PI:

- Right to opt-out of Sale of PI.
- Right to opt-out of Sharing of PI used for targeted advertising.
- Right to opt-out of use of "sensitive data" (includes healthcare data).
- CA: Homepage button not required if your business recognizes and honors browser opt-out preference signals from sale or sharing of PI and use of sensitive information. BUT: If you rely on browser signals, you must disclose this in your Privacy Policy.
- CO: Homepage button not required until 7/1/24. Until 7/1/24, businesses that process PI for targeted advertising or sales may allow and rely on browser signals.

I can help you with examples of the required opt-out buttons, but opt-outs will have to be tied to internal implementation.

What is (and is not) "Sale" and "Sharing"?

"Sale" of PI: The new or amended consumer privacy laws define the "**Sale**" of PI as transferring PI to a third party for something of value, usually money. CA's definition broadens the language to include selling, renting, releasing, disclosing, disseminating, making available, transferring, or communicating orally, in writing, or by electronic or other means. All of the new or amended consumer privacy laws grant consumers some version of the right to opt-out of the "Sale" of their PI. Plain English: While a "Sale" could mean a transfer of PI in exchange for something other than cash currency, a consumer's right to "opt out of Sale of PI" generally means opting out from your business transferring PI to another business in exchange for money.

"Sharing" PI: "Sharing" is a new concept unique to CA, where PI is transferred "for cross-context behavioral advertising" (CCBA), and is not dependent on money being exchanged, and includes "sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information." Plain English: A consumer's right to "opt out of Sharing PI" means opting out from your business transferring PI to another business for use for CCBA.

Not "Sale" or "Sharing": Not all transfers of PI are "Sales" or "Sharing". With the major exception of transfers for purposes of cross-context behavioral advertising" (CCBA) (which are always "Sharing"), transfers of PI to service providers or contractors for purposes of performing outsourced business purposes are generally not "Sales" or "Sharing". This is important because consumer opt-out rights apply to Sales and

Sharing but do not apply to transfers to service providers or contractors. This is also an important reason for the newly important requirement of having written detailed contracts with service providers, where PI is shared for a business purpose and which state in particular that the service provider limits its collection, sale, and use of the PI to perform the business purpose.

4. Implement affirmative consent (opt-in) for collecting "sensitive information" or collecting PI for targeted advertising.

- NOTE: Consent requirement only applies where you collect information directly. If you receive PI or sensitive information from 3rd parties, then instead the consent obligation is on the 3rd party. BUT: In those cases, you must get contract assurances of compliance from the 3rd party.
- "Sensitive information" = private personal data, e.g. account login information, passport number, driver's license number, social security number, health information, information about racial and ethnic origin or religious beliefs, and financial information.
- VA and CO: New affirmative consent (opt-in) requirement to collecting "sensitive information" (for any purpose) or other PI (for targeted advertising).
- CA: No opt-in requirement, but CA requires homepage opt-out buttons (see separate section on Opt-Out Buttons).

* * *

6 internal-facing things to do.

1. Conduct Data Protection Impact Assessment(s) (DPIAs) (particularly if you use PI for targeted advertising, profiling or if you process "sensitive data")**.** A DPIA is a formal, written internal audit where you assess a proposed product or service involving PI, by comparing the benefits (for your business, consumers and other stakeholders) with potential risks (to consumer rights), together with an operational plan to minimize those risks. DPIAs have been required in the EU under GDPR since 2018, and are a new (2023) requirement in the US under various state laws when your business provides certain types of services, particularly targeted advertising, profiling or if you process "sensitive data".

Please contact me for examples.

When is a DPIA required?

- A DPIA is required when a proposed processing of PI creates a "heightened risk of harm" to consumers. This always includes targeted advertising, sales of PI, certain types of profiling services using PI and processing "sensitive data" such as healthcare data.
- Profiling that risks "reputational injury" requires a DPIA in VA, but not CO.
- CA law has no formal DPIA requirement, but CA requires annual "thorough and independent" risk assessments for businesses that process PI which may pose a "significant risk" to consumers. These terms are not currently defined, but rules and regulations are expected soon.

What specifically should a DPIA include? A DPIA should include the following steps:

- Explanation of the determination for conducting a DPIA.
- Description of the processing your product/feature will conduct.
- Assessment of the necessity of processing this PI and whether the level and type of PI collected is proportional to business needs.
- Identification and assessment of the risks that arise with the types of PI processed.
- Determination of ways to mitigate the identified risks.

- Recordkeeping of the outcome of the DPIA.
- Integration of the outcome of the DPIA into a plan.
- Implementation of the plan.
- Periodic review of the plan and conducting additional DPIAs as needed.

2. Implement new HR data privacy requirements. Effective January 1, 2023, PI of employees (current and former), contractors and job applicants (whether or not hired) is now "personal information" similar to any other individual's data, and subject to all compliance requirements. (CA-specific requirement.) Specific requirements:

- New separate privacy policy for HR Data. A new, separate Privacy Policy covering HR Data is recommended (or a new section of your general Privacy Policy). This is a simplified version of the general Privacy Policy disclosing data collection and use practices specific to PI of job applicants, employees and contractors.
- Written notice at collection to job applicants, employees and contractors. A notice must be provided at the time the PI is collected, which must include (a) the categories of PI to be collected and (b) the purposes of use for each category of PI.
- "Sensitive personal information". SPI will typically be collected from job applicants and certainly from employees (Social Security number, financial information, health information). But: You are not required to present this information as SPI in the notice (and therefore subject to subsequent opt-out in CA) unless the information is collected or processed for the purposes of "inferring characteristics" about the individual. Uses for traditional HR functions are not for the purposes of "inferring characteristics".
- Job applicants, employees and contractors are now entitled to the same data access rights for PI as other consumers, with certain HR-specific exemptions such as limitations on the right to delete and opt-outs.

Please contact me for examples. Your HR team will need to integrate these requirements into HR processes.

3. DSARs: Revise SOPs for receiving and responding to consumer data access requests (DSARs). Medium-size list of consumer data subject access rights (DSARs) under the various state laws (and GDPR), but also important new opt-out rights from "Selling" and "Sharing" PI. Revise your SOP (or create new SOP) for receiving and responding to DSARs. Specific DSAR rights to be covered:

- Right to correct personal data if inaccurate or outdated in any way.
- Right to delete any collected PI.
- Right to access what PI has been collected and whether the PI was used (including where it was sold or shared, and how it was used).
- Right to opt-out of targeted advertising.
- Right to opt-out of automated decision-making (or profiling) in furtherance of decisions that produce legal or similarly significant effects concerning a consumer.
- Right to opt-out of Sale of PI.
- Right to opt-out of Sharing of PI (with third parties) used for "cross-context behavioral advertising" (i.e. targeted advertising) (CA only).
- Right to opt-out of use of sensitive information (CA only).

You must make 2 methods available for consumers to submit requests:

- Toll-free number requirement (CA only, not required if your business "operates exclusively online and has a direct relationship with the customer"), plus ...
- One of the following methods: Email, link to website form or US mail (required).

If you receive valid data deletion or non-processing requests from individuals, you must also notify your service providers or third parties to similarly comply.

IMPORTANT CAVEATS: There are many exceptions to these data access rights, e.g. CT's protection of trade secrets and CA limitations on employee opt-out rights from uses of sensitive information. Most states also allow denial of access requests when "unduly burdensome". Businesses also may (and should) employ reasonable efforts to validate the identity of requestors.

This may simply involve updating your existing SOP, which should include processes for validating identification of requestors. Please also contact me for examples.

4. Review and update your data security and other internal policies to align with new privacy requirements. Examples:

- Acceptable Use
- Business Continuity
- Disaster Recovery
- Incident Response
- Record Retention

Please contact me for examples of these policies. Implementation should be led by someone internally.

5. Review and update data security controls: "Reasonable and proportional technical, organizational and physical security measures".

- Consider encryption, masking, pseudonymization, deidentification, and access controls.
- Conduct Annual Cybersecurity Audit (CA only).

Guidelines: Statutory and regulatory requirements, industry best practices (including self-regulatory principles) and contract requirements. Please contact me for guidelines, but this should be led by someone internally.

6. Train your people: Conduct training (ongoing, regular, mandatory) for all staff on PI privacy responsibilities and data security controls. Conduct (or continue to conduct) a regular training program for incident response and day-to-day compliance measures.

You can create an internal training program or engage external professional trainings. I can also help in various ways, including with training materials and conducting regular training.