A P M
& C O

AMIT, POLLAK, MATALON

July 2023

US PRIVACY LAW HANDBOOK

APM & Co. Technology & Regulation Department

APM & Co. Amit, Pollak, Matalon - 18 Raoul Wallenberg St., Tel Aviv, 6971915, Israel

When will the acts come into effect?

- Colorado – July 1st, 2023 with a 60-day cure period "grace" by AG until 31 December 2024.
- Connecticut – July 1st, 2023 with a 60-day cure period "grace" by AG until 31 December 2024.
- Utah – December 31st, 2023 with a 3-day cure period.
- Indiana – January 1st, 2026
- Iowa – January 1st, 2026
- Montana – October 1st, 2024
- Tennessee – July 1st, 2024

Threshold:

As can see in the table below, the thresholds are "anti-AdTech" and every website using third-party cookies or AdTech company are likely to reach such threshold.

1. **Montana**: Threshold of 25,000 consumers and 25% revenue of sale of personal information.
2. **Iowa**: Threshold of 25,000 consumers and 25% revenue of sale of personal information.
3. **Indiana**: Threshold of 25,000 consumers and 50% revenue of personal information.
4. **Utah**: Threshold of 25,000 consumers and 50% revenue of personal information.
5. **Connecticut**: Threshold of 25,000 consumers and 25% revenue of personal information.
6. **Colorado**: Most rigorous with a threshold of only 25,000 consumers, **without requirements of derived revenue of the sale of personal information**.

We further recommend to join the IAB Multi State Platform and enabling the GPP Signal, as this is the only applicable signal for the multi-currently enforces states (California, Connecticut, Colorado, Virginia and soon Utah). For more information, please reach out.

Data Processing Assessment:

The new acts also highlight the significance of Data Protection Assessment ("DPA") requirements, these requirements across states show strong similarities and are influenced by the GDPR. Note that in Connecticut, Colorado, and Virginia require specifically any use of Personal Data for "Targeted Advertising" requires a DPA.

Law	Applicability	Exemptions	Personal Data Sensitive Data	Is consent required and when?	Is a privacy policy required?	Data breach requirements	Is a Data processing Agreement needed?
Colorado Privacy Act (CPA)	Applicable to "**controllers**" that: operate in Colorado, directly targeting Colorado residence; and one or both thresholds apply: **(i)** of one hundred thousand consumers or more during a calendar year (note, "process" includes also merely storing); **(ii)** profits from selling personal data of 25,000 or more consumers. "***Sale***" is defined as "the exchange of personal data for monetary or other valuable consideration by a controller to a third party."	Personal data that is already covered by federal laws or certain state law fall outside of the scope of the CPA, such as health data, financial data, etc. these include specifically the **COPPA, FCRA, FERPA, GLBA, HIPAA, national SEC, higher education data, etc.** Further, employment data and commercial B2B data are exempt. Public information, and de-identified data are exempt from the scope. Restrictions on processor or controller **do not apply** to personal data processed for research, internal process, improving the services, identify and repair errors, provide the services and products, protection of fraud, security incident, safeguard consumer rights, etc. (similar version of the GDPR various lawful basis, besides consent, such as legitimate interest,	"***Personal Data***" means information that is linked or reasonably linkable to an identified or identifiable individual. It does **not** include de-identified data or publicly available information. "***Publicly available information***" refers to data lawfully made available from federal, state; **or** local government records; **or** data that a controller reasonably believes the consumer has lawfully made available to the general public. "***De-identified Data***" means data that cannot reasonably be used to infer information or link to and individual. **Sensitive Data** includes **(i)** racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life or sexual orientation; **(ii)** Genetic or biometric data that	"***Consent***" similar to GDPR, consent means "*clear, affirmative, **freely given, specific, informed, and unambiguous".*** ***Consent shall be obtained upon an affirmative action.*** ***The following does not constitute consent: acceptance of the privacy policy in general, hover over, agreement through dark patterns.*** ***Consent is required*** for the following: **(i)** before processing Sensitive Data; **(ii)** use personal data for purposes **other than the initial disclosed purposes**. A Data Processing Assessment is required when processing sensitive data, heightened risk, selling data, processing data for targeted advertising, and in	**Yes.** Controllers need to provide a privacy notice that identifies the categories of personal data that are collected or processed, the purposes, how consumers can exercise their rights, and **appeal** such decision, categories of third-parties the controller shares or sells the personal data, or sells the personal data for advertising and how to opt-out. Controllers are required to minimization, specification, of processing data. To apply a duty of care and avoid secondary use of personal data (without obtaining consent).	The requirement is **not** under CPA, but rather §6-1-716 of the Colorado Revised Statutes. **Security breach:** the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity. The covered entity that owns the personal data, is required to notify, including any service provider they use are required to notify the owner. AG notification solely if over 500 individuals were affected, through this link. Covered entities are required to promptly notify **affected individuals** and entities after a security breach (no later then 30-day).[2]	**Yes.** A data processing agreement is required between the controller and the processor. The agreement should include **instructions** for processing, types and duration of processing, compliance requirements, notification in data breach, opportunity to object a new sub-processor, and additional provisions such as data deletion or return, providing information for demonstrating compliance, assisting with DPA, and the option for audits and inspections[3]. Both the controller and processor are required to **implement technical organizational measures**. Confidentiality Duties and Ensure Subcontractors Comply. Assisting the controller in conducting a DPA and demonstrating compliance.

2 The notification obligation does not apply to information that is encrypted, so long as the encryption key was not accessed or acquired. A covered entity that maintains its own notification procedures as a part of an information security policy for the treatment of personal information and whose procedures are otherwise consistent with the timing requirements will be deemed to be in compliance with the breach notification requirements if the covered entity notifies affected Colorado customers in accordance with its policies in the event of a breach of security of the system.

3 Note, may controllers require indemnification for data breach and processor to adhere expenses of notification, this is not required under CPA, solely required to notify.

		contract necessity, vital public interest, etc.[1]). These exemptions shall apply to consumer requests as well.	can be processed to uniquely identify an individual; or **(iii)** child data.	certain cases when profiling consumers.		Exemption apply.	
Connecticut Data Privacy Act (CTDPA)	Applicable to **people** who: Conduct business in Connecticut or produce products or services targeted towards Connecticut residents, that, during the prior calendar year, controlled or processed the personal data of: **(i)** at least 100,000 consumers (excluding data solely processed for payment transactions); **OR (ii)** 25,000 or more consumers **and** derive more than 25% of their gross revenue from the sale of personal data. "***Sale of personal data***" is defined	Restrictions on processor or controller do **not** apply to personal data processed for research, internal process, improving the services, identify and repair errors, provide the services and products, protection of fraud, security incident, safeguard consumer rights, complying with federal laws, taking steps in accordance with customer contract, etc. These exemptions shall apply to consumer requests as well. The controller, or processor, may collect, process and retain Personal Data for internal research and development of the services, product recall, repair errors, performance of contract and internal operations in which the consumer has reasonable expectation such use.	"***Personal data***" means any information that is linked or reasonably linkable to an identified or identifiable individual. **It does not include de-identified data or publicly available information**. "***Publicly available information***" means information that is lawfully made available through federal, state municipal government records widely distributed media, and a controller has a **reasonable** basis to believe a consumer has lawfully made available to the general public. "***De-identified Data***" means data that cannot reasonably be used to infer information or link to and individual.	"***Consent***" similar to GDPR, consent means "***clear, affirmative, freely given, specific, informed, and unambiguous".*** ***Consent shall be obtained upon an affirmative action.*** ***The following does not constitute consent: acceptance of the privacy policy in general, hover over, agreement through dark patterns. Consent can be withdraw within 15-days of notice.*** Consent is required for the following: Before processing sensitive data. In the case of processing sensitive data concerning a known child, without first obtaining consent from the child's parent or	**Yes** A controller must provide consumers with a clear and accessible privacy notice that includes: categories of personal data processed, purpose of processing, instructions for exercising consumer rights and appealing decisions, categories of personal data shared with third parties, categories of third parties with whom data is shared, and any sale of data or targeted advertising. The notice shall include an active email address for how to contact the controller.	It is a requirement to notify data breaches under §36a-701b of the General Statutes of Connecticut. **Breach of security**: unauthorised access to or unauthorised acquisition of electronic files, media, databases or computerised data, containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable. Notifying **affected individuals** without unreasonable delay, but no later than 60 days after the breach discovery. The covered entity that owns the personal data,	**Yes** The contract should include instructions, purpose of processing, type of data processing, duration, and the rights and obligations of both parties. The processor must assist the controller in meeting obligations, ensure data security, provide necessary information, engage subcontractors, and allow assessments. Both the controller and processor remain liable. Determining roles depends on adherence to instructions, and non-compliance may lead to enforcement actions. Confidentiality Duties.

1 CPA lists in the Applicability Part four sections. Section 1 sets out the threshold, Section 2 sets out the laws (federal laws, health and finance laws) or data sets (de-identified, employment data, public data) which are exempt from the CAP applicability, leaving the applicability to solely Colorado consumers, and Section 3 sets out the type of processing which is further exempt from CPA requirements, certain requirements, to clarify, similar to the GDPR that lays out six lawful basis for processing, the CPA sets out various types of processing such as vital public interest, protection of other consumers, security, errors, fraud prevention, internal enhancement and improvement, research, etc. this is a closed list of exemptions and is not bound to be interpreted.

	as *"the exchange of personal data for monetary or other valuable consideration by the controller to a third party."*	State and local government, nonprofit organizations, financial institutions, and higher education are exempt. GLBA, HIPAA, the FCRA, and the Family Educational Rights and Privacy Act, etc. are further exempt. Employment and commercial B2B data are exempt, as well as de-identified and public information.	"***Sensitive Data***": means data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, citizenship, or immigration status; The processing of genetic or biometric data for the purpose of uniquely identifying an individual; Personal data collected from a known child; Precise geolocation data.	lawful guardian. As well as for targeted advertising of consumers aged 13-16. Consent is further required for use personal data for purposes other than the initial disclosed purposes. A Data Processing Assessment is required when processing sensitive data, heightened risk, selling data, **processing data for targeted advertising,** and in certain cases when profiling consumers.		is required to notify, including any service provider they use are required to notify the owner. To report a breach of security, to AG through this email ag.breach@ct.gov. Exemption apply.	
Utah Consumer Data Privacy Act (UCPA)	Applicable to any controller or processor who: Conduct business in Utah or produce products or services targeted towards stateresidents that: Have an annual gross revenue of $25,000,000 or more; **AND (i)** Control or process personal data of 100,000 or more consumers in a calendar year; or	HIPAA entities GLBA entities, Nonprofits Higher education FCRA Employment data Commercial B2B data are exempt. De-identified Data and Publicly Available Data are exempt. The requirements described in this chapter do not restrict a controller's or processor's ability to: comply with federal law, perform contract, investigate a legal claim, vital public interest, research, or process personal data for: internal	"***Personal Data***" refers that is linked or **reasonably** linkable to an identifiable individual, and does not include de-identified data and publicly available data. ***"Publicly available Data***" refers to information that a person: lawfully obtains from a record of a governmental entity; or the controller reasonably believes a consumer **or** widely distributed media has made available to the general public.	"***Consent***" means an affirmative act by a consumer that unambiguously indicates the consumer's voluntary and informed agreement to allow a person to process personal data related to the consumer. Controller must present **notice** and opportunity to opt out, not consent. Only children data requires consent.	**Yes** The Notice shall include: Categories of data Purpose for processing each category; How to exercise consumer rights; Categories of data shared with third parties; Categories of third parties with whom data is shared Any sale of data or targeted advertising and how to opt out.	There is a requirement to notify data breaches pursuant to the Protection of Personal Information Act under §13-44-101 et seq. of Chapter 44 of Title 13 of the Utah Code ('Utah Code'). **Breach of system security**: An unauthorised acquisition of computerised data maintained by a person that compromises the security, confidentiality, or integrity of personal information. Breach of system security does not include the acquisition of	**Yes** Before a processor undertakes processing activities on behalf of a controller, they must establish a contract that includes clear instructions for processing personal data, outlining the nature, purpose, type of data, duration, and the rights and obligations of both parties. The contract should also mandate the processor to enforce confidentiality obligations for all individuals involved in processing personal data.

	(ii) Derive over 50% of gross revenue from the sale of personal data **and** control or process personal data of 25,000 or more consumers. "***Sale***," "***sell***," or "***sold***" refers to *"the exchange of personal data by a controller to a third party in return for* ***monetary consideration****."* Actual money.	operations, providing the services, retain the email address for the suppression list, etc.	"***Sensitive Data***": race or ethnicity; religion; health; sexual orientation; citizenship; genetic or biometric data used to identify a person; and precise geolocation.	**Conducting a DPA is not required.**		personal information by an employee or agent of the person possessing unencrypted computerised data unless the personal information is used for an unlawful purpose or disclosed in an unauthorised manner. The covered entity that owns the personal data, is required to notify, including any service provider they use are required to notify the owner. Notification of a breach should be made in the most expedient time possible and without unreasonable delay, consistent with the needs of law enforcement and once the scope of the breach has been determined and the integrity of the system has been restored. Notice to AG not required. Exemption apply.	Additionally, if the processor engages any subcontractors, there must be a written contract in place requiring them to uphold the same obligations regarding the personal data as the processor.
Indiana Consumer Protection Act (ICDPA)	Applicable to a person who conducts business in the state of Indiana or produce products or	HIPPA, COPPA, Family Education Rights and Privacy Act, Driver Privacy Act, Farm Credit Act, GLBA, FCRA, Higher education institutions, Government organizations, Nonprofits.	"***Personal data***" refers to information that is connected or reasonably capable of being connected to a known or identifiable individual, does not include data	"***Consent***" is defined as a clear affirmative act that signifies a consumer's freely given, specific, informed, and unambiguous	**Yes.** Controllers must provide consumers with a clear and accessible privacy notice that includes	There is a requirement to notify data breaches under § 24-4.9-1 et seq. of Article 4.9 of Title 24 of the Indiana Code.	**Yes** The DPA must be binding and include instructions for processing personal data, details about the nature and purpose of processing,

	services targeted to Indiana residents during a calendar year, and **(i)** process personal data of at least 100,000 consumers; or **(ii)** Control or process personal data of at least 25,000 consumers **and** derive over 50% of gross revenue from the sale of personal data. "***Sale of personal data***" is defined as: *"the exchange of personal data for* ***monetary consideration*** *by a controller to a third party."* Note that Indiana, similarly to Utah, does not include non-monetary "other valuable consideration" options as a sale.	Employment data is exempt. does not apply to personal data in the context of a purely personal or household activity. Shall not restrict the ability of controllers or processors to: conduct internal research to develop, improve, or repair products, services, or technology, recall, performing internal operations that are reasonably aligned with the expectations of the consumer, prevent fraud, security risk.	that has been **de-identified**; data that has been combined to create summaries or generalizations; or information that is openly accessible to the public. "***Publicly available information***" means information that: is lawfully made available through federal, state, or local government records; or 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. ***"Sensitive Data":*** information revealing racial or ethnic origin, religious beliefs, a mental or physical health diagnosis made by a healthcare provider, sexual orientation, or citizenship or immigration status; Genetic or biometric data that is processed for the purpose of uniquely identifying a specific	agreement to process personal data relating to the consumer, which includes a written statement, including one written by electronic means, or any other unambiguous affirmative action. Consent is required for the following: **(i)** Process of personal data for purposes that are neither reasonably necessary for nor compatible with the disclosed purposes for which the personal data is process, unless first receiving the consumer's consent; **(ii)** Before processing sensitive data. In the case of processing sensitive data concerning a known child, without first obtaining consent from the child's parent or lawful guardian. **Controllers are required to conduct and document DPIAs:** processing for targeted advertising, substantial injuries to consumers; or processing sensitive data, or in the event of heightened risk.	the categories of personal data processed, purpose of processing, instructions for exercising consumer rights, and how they may appeal, categories of personal data shared with third parties, and categories of third parties involved. If a controller sells personal data or uses it for targeted advertising, they must clearly disclose such activities and provide opt-out or preference management information for consumers.	**Data Breach:** The unauthorised acquisition of computerised data that compromises the security, confidentiality, or integrity of personal information maintained by a person. Notice must be provided by the database owner, in addition, a person that maintains computerised data but that is not a database owner must notify the database owner if the person discovers that personal information was or may have been acquired by an unauthorised person. If a database owner must notify an Indiana resident, then notification must also be made to the AG through this form.	the type of data being processed, the duration of processing, and the rights and obligations of both parties. The DPA also mandates that the processor ensures confidentiality, deletes or returns data as directed by the controller, provides necessary information to demonstrate compliance, allows reasonable assessments, and engages subcontractors under written contracts that impose the same obligations on them. The DPA shall also include assisting the controller in meeting its obligation to respond to consumer rights requests by appropriate technical and organizational measures, insofar as this is reasonably practicable, and taking into account the nature of processing and the information available to the processor.

			individual; Personal data collected from a known child; Precise geolocation data.				
Iowa Consumer Data Protection Act (IDCPA)	Doing business in Iowa or marketing goods or services to Iowa residents is the baseline threshold for who falls under the law's scope **and (i)** collect, store, or sell personal data for 100,000; **OR (ii)** Process personal data for 25,000+ consumers **AND** receive over 50% of annual gross revenue from selling personal data "***Sale of personal data***" is to *"the exchange of personal data for* ***monetary consideration*** *by the controller to a third party."*	HIPPA, COPPA, Family Education Rights and Privacy Act, Driver Privacy Act, Farm Credit Act, GLBA, FCRA, Higher education institutions, Government organizations, Nonprofits. Employment data is exempt. Shall not restrict the ability of controllers or processors to: conduct internal research to develop, improve, or repair products, services, or technology, recall, identify and fix technical errors performing internal operations that align with consumer expectations or are reasonably anticipated based on the consumer's existing relationship with the controller.	"***Personal data***" refers to any information that is connected or reasonably capable of being connected to a known or identifiable individual and does not include data that has been **de-identified** or aggregated, or information that is publicly available. "***De-identified data***" means data that cannot reasonably be linked to an identified or identifiable natural person. "***Publicly available information***" means information that is lawfully made available through federal, state, or local government records, or information that a business has 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	"***Consent***" means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. Consent may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action. **The ICDPA does not outline consent as a lawful basis for data processing.** **Conducting a DPA is not required.**	**Yes** Controllers must provide consumers with a privacy notice that is accessible, clear, and meaningful. It should include categories of personal data processed, purpose of processing, instructions for exercising rights (including appeals), details on sharing with third parties, and categories of third parties involved. If personal data is sold or used for targeted advertising, clear disclosure and opt-out options are required. Secure means for submitting rights requests should also be established as described in the notice.	There is a requirement to notify breaches under §715C.1 et seq. of Title XVI of the Iowa Code ('the Iowa Code'). **Breach of security**: Unauthorised acquisition of personal information maintained in computerised form by a person that compromises the security, confidentiality, or integrity of the personal information. Notice must be provided to any consumer whose personal information was included in the information that was breached. Notification must be made in the most expeditious manner possible and without unreasonable delay. If an individual was subject to a breach of security requiring notification to more than 500 residents of Iowa, notice of the breach must also be given to the Director of the Consumer Protection Division of the	**Yes** The DPA must include clear instructions for processing personal data, specify the nature and purpose of processing, identify the type of data involved, determine the duration of processing, and outline the rights and duties of both parties. Additionally, the DPA mandates that the processor ensures confidentiality, deletes or returns data as instructed by the controller, provides necessary information for compliance demonstration upon request, and engages subcontractors through written contracts that impose the same duties regarding personal data. Establishing a DPA is crucial for ensuring compliance and safeguarding the interests of both the controller and the processor.

			the information to a specific audience. "***Sensitive Data***" means racial or ethnic origin, genetic or biometric, precise location, child data, etc.			Office of the Attorney General ('AG'). Exemptions apply.	
Montana Consumer Data Privacy Act (MCDPA)	Applicable for persons that conduct business in Montana or market commercial products or services that are targeted to Montana residents **and**: **(i)** Control or process the personal data of at least 50,000 consumers, excluding data solely processed for payment transactions; or **(ii)** Control or process the personal data of at least 25,000 consumers and derive more than 25% of gross revenue from the sale of personal data. "***Sale of personal data***" is defined as "*the exchange of personal data for monetary or*	HIPPA, COPPA, Family Education Rights and Privacy Act, Driver Privacy Act, Farm Credit Act, GLBA, FCRA, Higher education institutions, Government organizations, Nonprofits. Employment data is exempt. Shall not restrict the ability of controllers or processors to: collect, use, and retain personal data internally without restrictions. This includes conducting research for product development, improvement, repair, recalls, fixing technical errors, and performing internal operations aligned with consumer expectations.	"***Personal data***" refers to any information that is connected or reasonably capable of being connected to a known or identifiable individual. The term excludes deidentified data and publicly available information. "***Publicly available information***" means information that: is lawfully made available through federal, state, or municipal government records or widely distributed media; **or** a controller has a reasonable basis to believe a consumer has lawfully made available to the public. "***Sensitive Data"*** means racial or ethnic origin, health, genetic or biometric, child data, Precise geolocation data, etc.	"***Consent***" means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to allow the processing of personal data relating to the consumer. The term may include a written statement, a statement by electronic means, or any other unambiguous affirmative action. Consent is required for the following: **(i)** For the processing of personal data for purposes that are not reasonably necessary to or compatible with the disclosed purposes for which the personal data is processed as disclosed to the consumer unless the controller obtains the consumer's consent. **(ii)** Before processing sensitive data; and **(iii)** for targeted advertising	**Yes.** Controllers must provide consumers with an accessible and clear privacy notice that includes: categories of personal data processed, purpose of processing, categories of personal data shared with third parties (if applicable), categories of third parties involved, contact information, and instructions for exercising consumer rights and appealing decisions.	There is a requirement to notify breaches under §30-14-1704 of Part 17 of Chapter 14 of Title 30 of the Montana Code Annotated 2017. **Breach of the security of the data system:** Unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person or business and causes or is reasonably believed to cause loss or injury to a Montana resident. The covered entity that owns the personal data, is required to notify, including any service provider they use are required to notify the owner. Montana residents must be notified if their unencrypted personal information is acquired by an unauthorized	**Yes.** The DPA between the controller and the processor is necessary to govern the processing of personal data on behalf of the controller. The DPA must be binding and include clear instructions for data processing, specifying the purpose, duration, and types of data involved. It should also establish confidentiality obligations, require the return or deletion of data at the controller's request, and enable the controller to access information to verify compliance. The DPA should address subcontractors' obligations, and the processor must cooperate with assessments of their data protection measures. Overall, the DPA ensures proper data handling and protection between the controller and processor.

	other valuable consideration by the controller to a third party."			of consumers aged 13-16. **A Data Processing Assessment is required** when processing activities that presents a heightened risk harm including processing of personal data for purposes of targeted advertising, sale of personal data and in certain cases when profiling consumers.		person. The disclosure must be made without unreasonable delay. Any person or business that is required to issue a notification to residents must simultaneously notify the OCP at ocpdatabreach@mt.gov.	
Tennessee Information Protection Act (TIPA)	Applicable for persons that conduct business in Tennessee or produce product or services that are targeted to the residents of Tennessee **and (i)** Exceed 25,00.000 in revenue; **and**: control or process personal information of at least 100,000 consumers during a calendar year; **or (ii)** Control or process personal information of at least 25,000 consumers and derive more than 50% of gross revenue from the sale of personal information.	HIPPA, COPPA, Family Education Rights and Privacy Act, Driver Privacy Act, Farm Credit Act, GLBA, FCRA, Higher education institutions, Government organizations, Nonprofits. Employment data is exempt. Shall not restrict the ability of controllers or processors to: conduct internal research, recall, repair technical errors, and perform internal operations aligned with consumer expectations. These activities should also be compatible with processing data to provide requested products or services or fulfill contractual obligations.	"***Personal information***" means data that identifies, relates to, or describes a consumer or can be associated with them. It includes identifiers, such as name, address, social security number, and other similar information, as well as characteristics, commercial records, biometric data, online activity, and more. The term does not include publicly available information or de-identified/aggregate consumer data. "***Publicly available information***" means information that is lawfully made available through federal, state, or local government records, or information that a business has a	"***Consent***" means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal information relating to the consumer. Consent is required when: **(i)** Processing personal information for purposes beyond what is reasonably necessary and compatible with the disclosed purposes, unless obtained from the consumer. **(ii)** Before processing sensitive information. In the case of processing sensitive data concerning a known child, without first obtaining consent	**Yes** A controller must provide a privacy notice that is easily accessible, clear, and meaningful. The notice should include the categories of personal information processed, the purpose of processing, instructions for consumers to exercise their consumer rights, details on any sale of personal information to third parties, and information on how consumers can opt out of processing for targeted advertising.	There is a requirement to notify data breaches under §47-18-2107 of the Tennessee Code, as amended in 2017 ('the Tenn. Code Ann.'). **Breach of system security:** Unauthorised acquisition of computerised data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person or business and causes or is reasonably believed to cause loss or injury to a Montana resident. Tennessee residents must be notified if their personal information is acquired by an unauthorized person. Notification should be	**Yes** A DPA which governs data processing between the controller and processor is needed. The DPA governs data processing, specifying instructions, duration, and rights. The processor must ensure confidentiality, delete or return data, demonstrate compliance, cooperate with assessments, and engage compliant subcontractors. Liabilities remain for both parties. Determining controller or processor status depends on the context, with continued adherence to instructions defining the processor's role.

	"***Sale of personal information***" is defined as "*the exchange of personal information for valuable monetary consideration by the controller to a third party.*"		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. ***"Sensitive Data"*** includes data 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; The personal information collected from a known child; or Precise geolocation data.	from the child's parent or lawful guardian.. **A Data Processing Assessment is required** when processing activities that presents the sale of personal information, processing for purposes of profiling in certain case, processing of personal data, and processing involving heightened risk of harm to consumers.		made within 45 days of discovering the breach. Encryption exempts the need for notification, unless the encryption key is accessed. Information holders with their own notification procedures are considered compliant. GLBA and HIPAA entities are exempt from the requirements. Notice to AG not required.	
New Hampshire	Applicable persons that conduct business in New Hampshire or persons that produce products or services that are targeted to the residents of New Hampshire.	HIPPA, COPPA, Family Education Rights and Privacy Act, Farm Credit Act, GLBA, FCRA, Higher education institutions, Government organizations, Nonprofits, etc. Employment data is exempt. Shall not restrict the ability of controllers or processors to: conduct internal	"***Personal data***" means any information that is linked or reasonably linkable to an identified or identifiable individual. "***Publicly available information***" means information that is lawfully made available through federal, state, municipal government records, or widely distributed media, and a controller has a	"***Consent***" means a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement to allow the processing of personal data relating to the consumer. Consent is required for: **(i)** Processing personal data beyond what is	**Yes** Controllers must provide consumers with an accessible, clear, and meaningful privacy notice. It should include categories of personal data processed, purpose of processing, instructions for exercising consumer	There is a requirement to notify data breaches pursuant to the New Hampshire right to privacy act under §359-C:1 et seq. of Title XXXI of the New Hampshire Revised Statutes ('N.H. Rev. Stat. Ann.'). **Security breach**: Unauthorized acquisition of computerized data that compromises the	**Yes** The DPA should govern the processor's data processing procedures and clearly outline instructions, responsibilities, and obligations. The contract must ensure confidentiality, require the deletion or return of personal data, enable the controller to access necessary information for

		research, recall, repair technical errors, and perform internal operations aligned with consumer expectations. These activities should also be compatible with processing data to provide requested products or services or fulfill contractual obligations.	reasonable basis to believe a consumer has lawfully made available to the general public. **"*Sensitive Data*"** means data that includes data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation or citizenship or immigration status; the processing of genetic or biometric data for the purpose of uniquely identifying an individual; personal data collected from a known child; or, precise geolocation data.	necessary for the disclosed purposes. **(ii)** Before processing sensitive information. In the case of processing sensitive data concerning a known child, without first obtaining consent from the child's parent or lawful guardian. **(iii)** Consent required for targeted advertising of consumers aged 13-16 years old. **A Data Processing Assessment is required** when processing activities that presents the sale of personal information, processing for purposes of profiling in certain case, processing of personal data, and processing involving heightened risk of harm to consumers.	rights (including appeals), details on data shared with third parties, categories of third parties involved, contact information, and opt-out methods for data sale or targeted advertising. Secure and reliable means for submitting rights requests should be established as described in the notice.	security or confidentiality of personal information maintained by a person doing business in New Hampshire. Any data breach must be notified to the relevant regulator. Prompt notification to consumer reporting agencies is, as well as notification to affected individuals as soon as possible after confirming a breach. Substitute notice may be given if the cost exceeds $5,000, more than 1,000 New Hampshire residents are affected, or if contact information is insufficient. It is mandatory to inform AG if a breach occurs.	demonstrating compliance, govern engagement with subcontractors, and allow for assessments by the controller or independent assessors.
Texas Data Privacy and Security Act (TDSPA)	Applicable to a person that: **(i)** Conducts business in Texas or produces a product or service consumed by the residents of Texas; **(ii)** Processes or engages in the sale of personal data; and **(iii)** Is	HIPPA, COPPA, Family Education Rights and Privacy Act, Farm Credit Act, GLBA, FCRA, Higher education institutions, Government organizations, Nonprofits, etc. Employment data is exempt. Shall not restrict the ability of controllers or processors to: conduct internal	"***Personal data***" refers to any information, which may include pseudonymous data and sensitive data, that is connected or reasonably capable of being connected to a known or identifiable individual. "***Publicly available information***" means information that is lawfully made available	"***Consent***," in relation to a consumer, refers to a clear and unambiguous agreement expressed through a freely given, specific, informed, and unambiguous act, indicating the consumer's agreement to process their personal data. This agreement can be provided through a	**Yes** Controllers must provide consumers with a clear and accessible privacy notice. It should include information on the categories of personal data processed, including any sensitive data, as well as the purpose of processing.	There is a requirement to notify data breaches pursuant to the Identity Theft Enforcement and Protection Act under Chapter 521 of Title 11 of the Business and Commerce Code ('Tex. Bus. & Com. Code'). **Breach of system security:** Unauthorised acquisition of computerized data that	**Yes** A DPA is needed, it must include clear instructions, purpose, data type, duration, rights, and obligations. The processor must ensure confidentiality, delete or return data as directed, provide compliance information, allow assessments, and engage compliant subcontractors.

	not classified as a small business according to the definition provided by the United States Small Business Administration. "***Sale of personal data***" is defined as *"the sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the controller to a third party."*	research, recall, repair technical errors, and perform internal operations aligned with consumer expectations. These activities should also be compatible with processing data to provide requested products or services or fulfill contractual obligations.	through 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 a consumer, or by a person to whom a consumer has disclosed the information, unless the consumer has restricted the information to a specific audience. *"**Sensitive Data**"* Means data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; Genetic or biometric data that is processed for the purpose of uniquely identifying an individual; Personal data collected from a known child; or Precise geolocation data.	written statement, including electronic means, or any other unambiguous affirmative action. Consent is required for: **(i)** Processing personal data for purposes beyond the disclosed purpose. **(ii)** Before processing sensitive information. In the case of processing sensitive data concerning a known child, without first obtaining consent from the child's parent or lawful guardian. **A Data Processing Assessment is required** when the processing activities presents heightened risk of harm including processing for purposes of targeted advertising, sale of personal information, certain case of processing for purposes of profiling.	Instructions on exercising consumer rights and appealing decisions should be provided. If personal data is shared with third parties, the notice should disclose the categories of data and third parties involved. Methods for submitting requests and opting out of data sale or targeted advertising should be explained.	compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data. businesses must notify the AG within 60 days of a breach involving 250+ residents. Prompt notification is required after law enforcement approval. Data Breach Submission Form	An independent assessment report may be provided. Liabilities of the controller and processor remain unchanged. The role of a processor depends on adherence to the controller's instructions.

USER RIGHTS

Consumer Right	CPA	CTDPA	UCPA	ICDPA	IDCPA	MCDPA	TIPA	NEW HAMPSHIRE	TDSPA
Right to Access	V	V	V	V	V	V	V	V	V
Right to confirm personal data is being processed	V	V	V	V	V	V	V	V	
Right to data portability	V	V	V	V	V	V	V	V	v
Right to delete	V	V	V	V	V	V	V	V	V
Right to correct	V	V	X	V	X	V	V	V	V
Right to opt-out of sale	V	V	V	V	V	V	V	V	V
Right to opt-out of targeted advertising	V	V	V	V	X[4]	V	X	V	V
Right to object to or opt-out of automated decision-making	V	X	X	V	X	V	X	V	V
Right to object to or opt-out of profiling	V	V	X	V	V	V	X	V	V
Opt-in required for processing of sensitive personal data	V	V	X[5]	V	X	V	X	V	V
Right to object to/restrict processing generally	X	X	X	X	X	X	X	X	X
Right to non-discrimination	V	V	V	V	V	V	V	V	V
Notice at collection requirement	V	X	X	V	V	V	V	V	V
Specific privacy policy content requirements	V	V	V	V	V	V	V	V	V
Purpose/use/retention limitations	V	V	X	V	V	V	V	V	V

[4] Although the consumer rights section of the law doesn't explicitly grant the right to opt out of targeted advertising, it does mandate that controllers involved in targeted advertising must offer transparent and easily noticeable disclosure options to allow users to opt out

[5] Although the consumer rights section of the law doesn't explicitly grant the right to opt out of targeted advertising, it does mandate that controllers involved in targeted advertising must offer transparent and easily noticeable disclosure options to allow users to opt out.

Method of Submitting a Request:

Under the most of the mew US State privacy regulations, the method must take into account the ways in which consumers **normally interact** with the controller, the need for secure and reliable communication relating to the request, and the ability of the controller to authenticate the identity of the consumer making the request. Controllers shall not require a consumer **to create a new account** in order to exercise consumer rights pursuant to this section but may require a consumer to use an existing account. A controller that processes personal data for purposes of **targeted advertising or the sale of personal data** shall provide a **clear and conspicuous method to exercise the right to opt out of the processing of personal data concerning the consumer**. The controller shall provide **the opt-out method** clearly and conspicuously **in any privacy notice**, **and** in a clear, conspicuous, and readily **accessible location outside the privacy notice**.

Exemptions for consumer rights under the CPA: de-identified data shall not be re-identified for a purpose of a request, if the controller is not able to reasonably associate the request with the personal data, or it would be unreasonably burdensome for the controller to associate the request with the personal data.

Time Line to Respond

Forty-five days after receipt of a consumer's request.

The period may be extended by an additional forty-five days, and the consumer must be informed of the extension and reasons within the initial forty-five-day timeframe.

In certain state the Consumer may appeal the decision, in which the controller shall respond within 45/60 days, and the consumer will have the option, similar to GDPR, to submit a complaint with the AG.

Therefore: add the appeal right to your privacy policy and make sure when responding to consumer requests, if you decline the request, make sure to inform the consumer of their right to appeal.

General Action Items

- Update the Privacy Policy to include state specifications.
- Update the DPA to include contractual requirements under these regulations.
- Ensure your CMP is compliant with notice and opt-out requirements.
- Make sure you have internal process to comply, respond and handle consumer requests.
- AdTech vendors, make sure you are part of the IAB Multi State Platform and use the GPP Signal.

Contact us

Adv. Hilla Shribman

Partner, Technology & Regulation Department

hillas@apm.law

Adv. Adi El-Rom

Partner, Technology & Regulation Department

adie@apm.law

Adv. Itamar Cohen

Partner, Technology and Regulation Practice

itamarc@apm.law

Adv. Gal Rezinovsky

Technology and Regulation Practice

galr@apm.law

Adv. Kobi Vinkrats

Technology and Regulation Practice

Kobiv@apm.law

Omer Mordel, Intern

omerm@apm.law

Adv. Efrat Katz

Technology and Regulation Practice

efratk@apm.law