A P M & C C

AMIT, POLLAK, MATALON

# US PRIVACY LAW HANDBOOK

APM & Co. Technology & Regulation Department

#### When will the acts come into effect?

- Colorado July 1<sup>st</sup>, 2023 with a 60-day cure period "grace" by AG until 31 December 2024.
- Connecticut July 1<sup>st</sup>, 2023 with a 60-day cure period "grace" by AG until 31 December 2024.
- Utah December 31<sup>st</sup>, 2023 with a 3-day cure period.
- Indiana January 1<sup>st</sup>, 2026
- lowa January 1<sup>st</sup>, 2026
- Montana October 1<sup>st</sup>, 2024
- Tennessee July 1<sup>st</sup>, 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. **lowa**: 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.



processing is required econtroller and cessor. The should include for processing,
processing is required e controller and cessor. The should include
is required controller and cessor. The should include
is required controller and cessor. The should include
controller and cessor. The should include
cessor. The should include
should include
for processing,
duration of
compliance
s, notification
ch, <u>opportunity</u>
a new sub-
and additional
such as data
or return,
nformation for
ng compliance,
h DPA, and the
audits and
controller and
re required to
technical
al measures.
ity Duties and
ontractors
e controller in
a DPA and
ng compliance.
-
niith niii

<sup>2</sup> 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.

<sup>3</sup> 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.

in Connecticut or produce products or produce products or services, identify and targeted towards Connecticut or 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 pampern transactions); OR (ii) 25,000 or more consumers and derive more than 25% of their gross revenue from the sale of performance of contract, and internal operations in process or profession, gross revenue from the sale of performance of contract and internal operations in process or processing and the process or processing and derive more than 25% of their gross revenue from the sale of performance of contract and device more consumers and derive more than 25% of their gross revenue from the sale of performance of contract and device more than 25% of their gross revenue from the sale of performance of contract and device more than 25% of their gross revenue from the sale of performance of contract and device more than 25% of their gross revenue from the sale of performance of contract and device more than 25% of their gross revenue from the sale of performance of contract and device more than 25% of their gross revenue from the sale of performance of contract and device more than 25% of their gross revenue from the sale of performance of contract and device more than 25% of their gross revenue from the sale of performance of contract and device more than 25% of their gross revenue from the sale of performance of contract and device more than 25% of their gross revenue from the sale of performance of contract and device more than 25% of their gross revenue from the sale of performance of contract and device more than 25% of their gross revenue from the sale of performance of contract and device more and device more than 25% of their gross revenue from the sale of performance of contract and device more than 25% of their gross revenue from the sale of performance of contract and device more than 25% of their gross revenue from the sale o			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.	
Data   Privacy Act   Conduct business   Conduct business   Correspondent   Privacy Act   Conduct business	Connecticut	Applicable to	•	"Personal data" means	"Consent" similar to	Yes	It is a requirement to	Yes
in Connecticut or products process, improving the cor services, identify and repair errors, provide the Connecticut or services and products, 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 pamer transactions); OR (ii) 25,000 or more consumers and derive more than 25% of their gross revenue from the sale of performance of contract and internal operations in personal data.  Inconnecticut or products or services, identify and tepair errors, provide the Connecticut or protection of fraud, during the prior calendar year, controlled or processed the personal data of: (ii) 25,000 or more consumers and derive more than 25% of their gross revenue from the sale of performance of contract and internal operations in personal data.  Inconnecticut or products, indentify and advallable individual. Information and internal operations in protection of fraud, during the prior calendar year, controlled or processed the personal data of: (ii) 21,25,000 or more consumers and derive more than 25% of their gross revenue from the sale of performance of contract and internal operations in performance of contract and inter	Data	people who:	or controller do <b>not</b> apply	any information that is	GDPR, consent means		notify data breaches	
produce products or services, identify and targeted towards residents, that, during the prior scontrolled or controlled or processed the personal data of: (i) at least 100,000 consumers (excluding data solely processed to 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.    produce products or services, identify and targeted towards to consumer and the process of processing, then the detail of the services, identify and targeted towards that, during the prior security incident, and adaptive action.    Publicly available information in formation in find the rights obtained upon an affirmative action.    Problicity available information in formation in find the rights and appealing information instructions for security consent: instructions for security and believe action.    Problicity available information in find the deal during the prior security in processed, purpose of processing, to accept the boltowing acceptance of th	Privacy Act	Conduct business	to personal data processed	linked or reasonably	"clear, affirmative,	A controller must	under §36a-701b of the	The contract should
or services targeted towards repair errors, provide the Connecticut services and products, residents, that, during the prior calendar year, controlled or processed the personal data of: personal data of: (i) at least 100,000 exemptions shall apply to consumers (lexcluding data solely processed the solely processed the solely processed the formation that is asolely processed the solely processed the formation that is asolely processed the formation that is asolely processed the solely processed the formation that is asolely processed the formation shall apply to consumers and derive more consumers and derive more than 25% of their gross revenue from the sale of personal data.  Information is the following does not constitute consent: and derive more than 25% of their gross revenue from the sale of personal data.  Information is the time of the services and products, residents, that, during the prior is calegories of possible privacy consider that includes: Consent is thall be obtained upon an affirmative action.  Information is means information that is constitute consent: acceptance of the personal data of: after through dark patterns. Consumer has lawfully made available through federal, state general, hover over, and any sale of data processing. The processor must assist the controller in meeting obligations, ensure data securely processor information of personal data dark patterns. Consent through dark patterns. The processor must assist the controller in meeting obligations, ensure data constitute consent: acceptance of the personal data for processor, may collect, process and retain information in that is a constitute acceptance of the personal data solely processor may collect, processor, may collect, processor, and retain information and processor processor may accessally upon an acquisition of electronic files, media, databases or constitute consent: acceptance of the personal data of the controller information information information withing acceptance of the personal data solely processor may accessin	(CTDPA)	in Connecticut or	for research, internal	linkable to an identified	freely given, specific,	provide consumers	General Statutes of	include instructions,
targeted towards Connecticut services and products, probable services and products, protection of fraud, during the prior calendar year, controlled or processed the personal data of processed the personal data of transactions) of a consumers (i) at least 100,000 exemptions shall apply to consumers (excluding data solely processed of processor, may collect, transactions); OR (iii) 25,000 or more consumers and derive more than 25% of their gross revenue from the sale of personal data.  The controller or performance of contract and internal operations in personal bata.  The controller or performance of contract and internal operations in personal data.  The controller or performance of contract and internal operations in which the consumer has leafly personal data.  The controller or performance of contract and internal operations in personal data.  The controller or performance of contract and internal operations in which the consumer has leafly personal data.  The controller or performance of contract and internal operations in which the consumer has leafly personal data.  The controller or performance of contract and internal operations in which the consumer has leafly personal data.  The following does not tonstitute consent: of the controller of the following acquisition of electronic of the constroller in meeting obligations of both and the rights and appealing obligations of both personal data of the controller in meeting information that is lawfully made available the through federal, state municipal government records widely distributed media, and a controller in through federal, state municipal government trecords widely distributed media, and a controller in through federal state municipal government treasant information and the rights and appealing information when access to the personal data information and information a		produce products	process, improving the	or identifiable individual.	informed, and	with a clear and	Connecticut.	purpose of processing,
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 or than 25% of their gross revenue from the sale of personal data or than 25% of their gross revenue from the sale of personal data or the personal data or than 25% of their gross revenue from the sale of personal data or the prior calendar year, controlled or processed the personal data or consumers and derive more than 25% of their gross revenue from the sale of personal data or the prior calendar year, controlled acceptance of affirmation.  Services and products, protection of fraud, incident, protection of fraud, incident, protection of fraud, during the prior calendar year, controlled acceptance of affirmative action.  "Publicly available information.  "Publicly available information or personal data or complying with federal information in that is lawfully made available through federal, widely dark patterns.  (ii) at least 100,000 consumer requests as well.  (excluding data solely processed for personal data or contract, etc. These exemptions shall apply to consumer requests as well.  The following does not constitute consent: of personal data or computerised data, obligations, of both of personal data or complurised accepts of of processing, information in that is lawfully made available through dark patterns.  Consent to processed, product recall, repair errors, performance of contract and internal operations in which the consumer has lead to the controller and any sale of data or the following:  Before processing controller or personal data for through dark patterns.  Consent to process or general, thore over, before with cutoffied and any sale of data or the following:  Before processing controller or targeted or through dark patterns.  Consent to processing sent with third parties with the cont		or services	services, identify and	It does not include de-	unambiguous".	accessible privacy		type of data processing,
residents, that, during the prior security incident, safeguard consumer rights, controlled or processed the personal data of: consumers (i) at least 100,000 exemptions shall apply to consumers of 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.  The following does not constitute consent: and derive more than 25% of their gross revenue from the sale of personal data.  The following does not constitute consent: and the personal data of: does not consumer secured by examptions in when the consumer has least and derive more than 25% of their gross revenue from the sale of personal data.  The following does not constitute consent: and the consumer has laws, taking steps in accordance with customer accordance with customer consumers and development of the services, product recall, repair errors, and internal operations in which the consumer has which the consumer has least of personal data of: the controller, or processor, may collect, process and retain gross revenue from the sale of personal data.  The following does not constitute consent: acceptance of the privacy policy in general, hover over, agreement through decisions, categories of withdraw within 15- days of notice.  The following does not constitute consent: nate of the controller in meeting decisions, categories of opersonal data and and and and and and and and and an		targeted towards	repair errors, provide the	identified data or	Consent shall be	notice that includes:	Breach of security:	duration, and the rights
during the prior calendar year, controlled or processed the personal data of: (i) at least 100,000 consumers (excluding data solely processed for for payment transactions); QR (ii) 25,000 or more consumers and derive more than 25% of their gross revenue from the sale of personal data.  In during the prior calendar year, safeguard consumer rights, controlled or processing tinformation in that is information in that is information in that is a reasonable expectation in personal data.  In during the prior calendar year, safeguard consumer rights, controlled or processed, the personal information in means information that is acceptance of the privacy policy in gement, hover over, distributed media, and a solely processed for processor may collect, process and retain gross revenue from the sale of personal data.  In during the prior calendar year, safeguard consumer rights, combroiled information in means information that is information that is acceptance of the privacy policy in gement, hover over, distributed media, and a consumer rate with third parties with third parties with the personal information or by any other method or technology that renders the personal information or by any other method or technology that renders the personal information or by any other method or technology that renders the personal information or by any other method or technology that renders the personal information or by any other method or technology that renders the personal information or by any other method or technology that renders the personal information or by any other method or technology that renders the personal information or by any other method or technology that renders and any sale of data and any sale of da		Connecticut	services and products,	publicly available	obtained upon an	categories of	unauthorised access to	and obligations of both
calendar year, controlled or controlled or processed the personal data of: accordance with customer consumers (excluding data solely processed to transactions); OR more consumers and derive more consumers and derive more and derive more than 25% of their gross revenue from the sale of personal data.  The following does not constitute consent: information means in personal data of: acceptance of the personal data of: acceptance of the privacy policy in distributed media, and a solely processed to the personal data of: acceptance of the privacy policy in distributed media, and a solely processed to though federal, state municipal government consumers (excluding data solely processed to the personal data of: acceptance of the privacy policy in distributed media, and a solely processed to though federal, state municipal government consumers (excluding data solely processed to though federal, state municipal government consumers (excluding data solely processed to though federal, state municipal government consumers (excluding data solely processor, may collect, process and retain personal Data for internal research and development of the services, product than 25% of their gross revenue from the sale of personal data.  The following does not constitute constant in formation when access to to the personal data information when access of processing seneral, hover over, agreement through distributed media, and a controller name at acceptance of the privacy policy in gifts and appealing information when access to the personal data information when access to the personal data information when access to the personal data information when access the privacy policy in gifts and appealing information when access the privacy policy in general, hover over, agreement through dark patterns, shared with third secured by encryption or by any other method or technology that rende		residents, that,	•	information.	affirmative action.	personal data		•
controlled or processed the personal data of: (i) at least 100,000 consumers (excluding data solely processed transactions); OR (ii) 25,000 or more consumers and derive more consumers and derive more than 25% of their gross revenue from the sale of personal data.  The controller, or more consumers and derive more than 25% of their gross revenue from the sale of personal data.  The controller, or more consumers and derive more than 25% of their gross revenue from the sale of personal data.  The controller, or more consumers and derive more than 25% of their gross revenue from the sale of personal data.  The controller, or more consumers and derive more than 25% of their gross revenue from the sale of personal data.  The controller, or more consumers and device more than 25% of their gross revenue from the sale of personal data.  The controller, or more consumers and device more than 25% of their gross revenue from the sale of personal data.  The controller, or processor, may collect, process and retain personal bears to believe a consumer has lawfully made available through federal, state municipal government records widely dark patterns.  Consent transactions for exercising consumer rights and appealing decisions, categories of the personal data shared with third parties with dark patterns.  Consent transactions for exercising consumer rights and appealing decisions, categories of the personal data shared with third parties with dark patterns.  Consent transactions for exercising consumer rights and appealing decisions, categories of the personal data shared with third parties with dark patterns.  Consent transactions for exercising consumer rights and appealing decisions, categories of the personal information when access to the personal data shared with third parties with dark patterns.  Consent is required for to the personal data on through dark patterns.  Consent is required for to the personal data on the decisions, categories of third partiers.  Consent is required for to the personal data on through dar		during the prior				processed, purpose	acquisition of electronic	
processed the personal data of: accordance with customer (i) at least 100,000 exemptions shall apply to 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.    Personal data of: accordance with customer ocotract, etc. These through federal, state municipal government records widely distributed media, and a controller, or processor, may collect, processed the personal data.    Indicate the personal data of: accordance with customer ocotract, etc. These through federal, state municipal government records widely distributed media, and a controller has a reasonable basis to believe a consumer has gross revenue from the sale of personal data.    Indicate the personal data of: accordance with customer accordance with customer accordance with customer through federal, state municipal government accordance with customer available through federal, state municipal government accordance with customer in accordance with customer accordance with customer contract, etc. These through federal, state municipal government 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 following:   Before processing sensitive data. In the case of processing sensitive data information when access to the personal data information and processor remain liable.   Consent is required for the following:   Determining roles depends and any sale of data or targeted individuals without unreasonable delay, but no later than 60 days and any sale of data i		calendar year,		· ·	The following does not	- 1 0/		l e
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.  In the sale of personal data of: (ii) at least 100,000 contract, etc. These through federal, state records widely distributed media, and a solely processed for payment transactions); OR (iii) 25,000 or more consumers and derive more than 25% of their gross revenue from the sale of personal data.  Information when access to to the personal data of personal data of personal data of personal data of through federal, state municipal government and derive media, and a solely processed for payment through dark patterns.  Consent can be withdraw within 15- days of notice.  Information when access to to the personal information has not been shared with third secured by encryption or by any other method or the consumer has lawfully made available through dark patterns.  Consent can be withdraw within 15- days of notice.  Information when access to to the personal data of payment through dark patterns.  Consent is required for the following:  Before processing sensitive data. In the gross revenue from the sale of personal data.  Information when access to to the personal data of procesure by any other method or the parties, categories of third parties, attending the patterns.  Consent is required for the following:  Before processing sensitive data. In the case of processing sensitive data. In the following:  Before processing sensitive data. In the sensitive data and internal operations in when acces to the decisions, categories of therwith third secured by encryption or the with third secured by encryption or the with third secured by encryption or the winders of payment through dark patterns.  Consent is required for the following:  Before processing sensitive dat							•	_
(i) at least contract, etc. These exemptions shall apply to consumers (excluding data solely processed for payment transactions); OR (ii) 25,000 or more consumers and derive more consumers and derive more than 25% of their gross revenue from the sale of personal data.  (ii) at least contract, etc. These exemptions shall apply to consumer requests as well.  (iii) 25,000 or more consumers and development of the services, product from the sale of personal data.  (iv) 25,000 or more consumers and development of the services, product from the sale of personal data.  (iv) 25,000 or more consumers and development of the services, product from the sale of personal data.  (iv) 25,000 or more consumers and development of the services, product from the sale of personal data.  (iv) 25,000 or more consumers and development of the services, product from the sale of personal data.  (iv) 25,000 or more consumers and development of the services, product from the sale of personal data.  (iv) 25,000 or more consumers and development of the services, product from the sale of personal data.  (iv) 25,000 or more consumers and development of the services, product from the sale of personal data.  (iv) 25,000 or more consumers and development of the services, product from the sale of personal data.  (iv) 25,000 or more consumers and retain processor, may collect, personal blassis to believe a consumer has lawfully made available to the general public.  (iv) 25,000 or more consumers and development of the services, product from the sale of personal data.  (iv) 25,000 or more consumers and development of the services, product from the sale of personal data and any sale of data or targeted and any sale of data or targeted advertising.  (iv) 25,000 or more consumers and development of the services, product or easonable beautiful personal data that cannot reasonable beautiful personal data that cannot		•				_	•	, ,
transactions); OR (ii) 25,000 or more consumers and derive more than 25% of their gross revenue from the sale of personal data.  In the controller, or payment transactions of the services, product from the sale of personal data.  In the controller has a consumer has for payment transactions of the services and derive more than 25% of their gross revenue from the sale of personal data.  In the controller, or payment transactions); OR (iii) 25,000 or more consumers and derive more than 25% of their gross revenue from the sale of personal data.  In the controller, or processor, may collect, process, and retain to believe a consumer has and derive more than 25% of their gross revenue from the sale of personal data.  In the controller, or processor, may collect, process, and retain to believe a consumer has and derive more than 25% of their gross revenue from the sale of personal data.  In the controller, or processor, may collect, process, and retain to believe a consumer has and the transactions); OR (iii) 25,000 or more consumers and derive more than 25% of their gross revenue from the sale of personal data.  In the controller has a without within 15-days of notice.  In the controller has a consumer has and a consumer has and retain believe a consumer has and the processor, may collect, process, and retain believe a consumer has and retain believe a consumer has and the processor, and retain believe a consumer has and the processor, may collect, process, and retain believe a consumer has and the processor, and retain to believe a consumer has and the processor, and retain believe a consumer has and treating to the personal data and a controller.  In the controller has a without within 15-third parties, categories of the without and any sale of data and any sale of d		•		•				, , ,
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.  Consumer seculding data solely processed transactions and derive more than 25% of their gross revenue from the sale of personal data.  Consumer swidely distributed media, and a controller has a processor, may collect, transactions); OR (iii) 25,000 or more consumers and derive more than 25% of their gross revenue from the sale of personal data.  Consent can be withdraw within 15- days of notice.  Consent is required for the following:  Before processing sensitive data. In the gross revenue from the sale of personal data.  Consent can be withdraw within 15- days of notice.  Consent is required for the following:  Before processing sensitive data. In the general public.  Consent can be withdraw within 15- days of notice.  Consent is required for the following:  Before processing sensitive data. In the general public asse of processing sensitive data in the mans data that cannot reasonably be used to personal data.  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. In the personal individuals without case of processing sensitive data in the case of processing sensitive data in the case of processing sensitive data in the data in the case of processing sensitive data in the consumer has reasonable expectation to the following:  Consent can be withdraw within 15- third parties with whom data is shared, and any sale of data or transactions.  Consent is required for the following:  Before processing sentitive data in the case of processing sensitive data. In the case of processing sensitive data in the data in the case of processing sensitive data. In the consumer has reasonable expectation which the consumer has data that cannot reasonable delay, but no later than 60 days after the breach discovery.		` '	,			_	' '	subcontractors, and allow
(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.  (excluding data solely processed for payment transactions); OR (iii) 25,000 or more consumers and derive more than 25% of their gross revenue from the sale of personal data.  (iii) 25,000 or more consumers and derive more than 25% of their gross revenue from the sale of personal data.  (iii) 25,000 or more consumers and derive more than 25% of their gross revenue from the sale of personal data.  (iii) 25,000 or more consumers and development than 25% of their gross revenue from the sale of personal data.  (iv) 25,000 or more consumers and development than 25% of their gross revenue from the sale of personal data.  (iv) 25,000 or more consumers and development than 25% of their gross revenue from the sale of personal data.  (iv) 25,000 or more consumers and development than 25% of their gross revenue from the sale of personal data.  (iv) 25,000 or more consumers and development of the services, product resonable basis to believe a consumer has to the general public.  (iv) 25,000 or more consumers and derive more than 25% of their gross revenue from the sale of personal data.  (iv) 25,000 or more consumers and development of the consumer has consumer has to the general public.  (iv) 25,000 or more consumers and development of the services, product research and development to the general public.  (iv) 25,000 or more consumers and derive more transactions, and any sale of data or targeted to the following:  (iv) 26,000 or more consumers and derive more transactions and any sale of data or targeted individuals without unreasonable delay, but no later than 60 days after the breach discovery.  (iv) 26,000 or more consumers and any sale of data or targeted individuals without unreasonable delay, but no later than 60 days after the breach discovery.		•						assessments.
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.  The controller, or processor, may collect, process and retain transactions); OR (iii) 25,000 or more consumers and derive more than 25% of their gross revenue from the sale of personal data.  The controller has a reasonable basis to believe a consumer has lawfully made available to the general public.  The controller has a reasonable basis to believe a consumer has lawfully made available to the general public.  The controller, or processor, may collect, process and retain believe a consumer has lawfully made available to the general public.  The controller has a reasonable basis to believe a consumer has lawfully made available to the general public.  The notice shall include an active email address for how the consumer has reasonable expectation which the consumer has reasonable expectation in dividual.  The notice shall include an active email address for how to contact the controller.  The notice shall include an active email address for how to contact the controller.  The personal information unreadable or unusable.  Notifying affected individuals without unreasonable delay, but no later than 60 days advertising.  The processor, may collect, process and retain believe a consumer has lawfully made available to the general public.  The notice shall include an active email address for how to contact the controller.			consumer requests as well.	I	•			
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.    The payment transactions); OR (iii) 25,000 or more consumers and development than 25% of their gross revenue from the sale of personal data.    The notice shall the personal information and any sale of data or targeted advertising.    The notice shall to the general public on adherence to instructions, and non-compliance may lead to enforcement actions.    The notice shall to concerning a known reasonable delay, but reasonable expectation		,	l	· ·		<u> </u>		
transactions); OR (ii) 25,000 or more consumers and derive more than 25% of their gross revenue from the sale of personal data.  Transactions); OR (ii) 25,000 or more consumers and development than 25% of their gross revenue from the sale of personal data.  Transactions); OR (iii) 25,000 or more consumers and development than 25% of their gross revenue from the sale of personal data.  Transactions); OR (iii) 25,000 or more consumers and development of the services, product than 25% of their gross revenue from the sale of personal data.  Transactions); OR (iii) 25,000 or more consumers and development of the general public.  The notice shall include an active email address for how the consumer has reasonable expectation to the general public.  The notice shall include an active email address for how to contact the consumer than 60 days after the breach discovery.  The notice shall include an active email address for how to contact the consumer than 60 days after the breach discovery.  The notice shall include an active email address for how to contact the consumer than 60 days after the breach discovery.			•			•		•
(ii) 25,000 or more consumers and derive more than 25% of their gross revenue from the sale of personal data.  (iii) 25,000 or more consumers and development of the services, product from the sale of personal data.  (iii) 25,000 or more consumers and development of the services, product than 25% of their gross revenue from the sale of personal data.  (iii) 25,000 or more consumers and development of the services, product than 25% of their gross revenue from the sale of personal data.  (iii) 25,000 or more consumers and development of the general public.  (iii) 25,000 or more consumers and development of the services, product the general public.  (iii) 25,000 or more consumers and development of the services, product than 25% of their gross revenue from the sale of personal data.  (iii) 25,000 or more consumers and development of the services, product than 25% of their gross revenue from the sale of personal data.  (iii) 25,000 or more consumers and development of the services, product than 25% of their gross revenue from the sale of personal data.  (iii) 25,000 or more consumers and development of the services, product than 25% of their gross revenue from the sale of performance of contract and internal operations in which the consumer has reasonably be used to individual.  (iii) 25,000 or targeted advertising.  (iii) 25,000 or targeted for the following:  (iii) 25,000 or targeted for the following:  (iii) 25,000 or targeted advertising.  (iii) 25,000 or targeted advertising.  (iii) 25,000 or targeted advertising.  (iii) 25,000 or targeted for the following:  (iii) 25,000 or targeted for the following:  (iii) 25,000 or targeted advertising.  (iii) 25,000 or targeted advertising.  (iii) 25,000 or targeted for the following:  (iii) 25,000 or targeted for the following:  (iii) 25,000 or targeted for the following:  (iii) 25,000 or targeted advertising.  (iii) 2		1 1			days of notice.	•	•	
more consumers and derive more than 25% of their gross revenue from the sale of personal data.  The following:  The following:  The following:  The following:  The notice shall include an active personal data.  The notice shall include an active email address for how the consumer has reasonable expectation  The notice shall include an active email address for how to contact the concerning a known reasonable expectation  The notice shall include an active email address for how to contact the concerning a known to contact the discovery.  The notice shall include an active email address for how to contact the concerning a known to controller.		-	F			<u> </u>	unreadable or unusable.	
and derive more than 25% of their gross revenue from the sale of personal data.  In the services, product recall, repair errors, performance of contract and internal operations in reasonable expectation  Individuals without unreasonable delay, but no later than 60 days after the breach discovery.  Individuals without unreasonable delay, but no later than 60 days after the breach discovery.  Individuals without unreasonable delay, but no later than 60 days after the breach discovery.						_		-
than 25% of their gross revenue from the sale of personal data.  The notice shall include an active email address for how personable expectation which the consumer has reasonable expectation.  The notice shall include an active email address for how to contract the concerning a known concerning a known to controller.  The notice shall include an active email address for how after the breach discovery.  Confidentiality Duties.			•	to the general public.		advertising.		•
gross revenue from the sale of performance of contract personal data.    performance of contract from the sale of personal data.   performance of contract from the sale of personal data.   performance of contract from the sale of personal data.   performance of contract from the sale of personal data from the sale of personal data.   performance of contract from the sale of personal data from the sal				"D-id-wife-d Data"	, ,	The section shall		enforcement actions.
from the sale of personal data.  The sale of personal data and internal operations in personably be used to personal data.  The sale of personal data and internal operations in personably be used to personably be used to concerning a known to contact the discovery.  The sale of personal data and internal operations in personably be used to concerning a known to contact the discovery.  The sale of personal data and internal operations in infer information or link to and individual.  The sale of personal data and internal operations in infer information or link to and individual.  The sale of personal data and internal operations in infer information or link to and individual.  The sale of personal data and internal operations in infer information or link to and individual.			•	•			• •	Caufidautialitu Dutiaa
personal data. which the consumer has reasonable expectation to and individual. concerning a known to contact the discovery.		0	<u>'</u>		-		-	Confidentiality Duties.
reasonable expectation to and individual. child, without first controller.			•	-				
		personal data.					discovery.	
I NOTE OF DESCRIPTION OF THE PROPERTY OF THE P		"Sale of personal	such use.	to and marvidual.	obtaining consent from	controller.	The covered entity that	
data   is defined   the child's parent or   owns the personal data,			Judii uje.				•	

<sup>1</sup> 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.

	(ii) Derive over	operations, providing the	"Sensitive Data": race or	Conducting a DPA is		personal information by	Additionally, if the
	50% of gross	services, retain the email	ethnicity; religion;	not required.		an employee or agent of	processor engages any
	revenue from the	address for the	health; sexual	•		the person possessing	subcontractors, there must
	sale of personal	suppression list, etc.	orientation;			unencrypted	be a written contract in
	data and control		citizenship; genetic or			computerised data	place requiring them to
	or process					unless the personal	uphold the same
	personal data of		biometric data used to			information is used for an	obligations regarding the
	25,000 or more		identify a person; and			unlawful purpose or	personal data as the
	consumers.		precise geolocation.			disclosed in an	processor.
						unauthorised manner.	
	" <b>Sale</b> ," " <b>sell</b> ," or					The covered entity that	
	" <b>sold</b> " refers to					owns the personal data,	
	"the exchange of					is required to notify,	
	personal data by					including any service	
	a controller to a					provider they use are	
	third party in					required to notify the	
	return for					owner.	
	monetary						
	consideration."					Notification of a breach	
						should be made in the	
	Actual money.					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.	
In all aux -	Amalian bl - t -	LUDDA CODDA F 'I	Dononoul destrill f	((Canaan#) : -#:	Voc	Exemption apply.	Vea
<u>Indiana</u>	Applicable to a	HIPPA, COPPA, Family	"Personal data" refers to	"Consent" is defined as	Yes.	There is a requirement to	Yes
<u>Consumer</u>	person who	Education Rights and	information that is	a <u>clear affirmative</u> act	Controllors	notify data breaches	The DDA must be bigding
Protection	conducts	Privacy Act, Driver Privacy	connected or reasonably	that signifies a	Controllers must	under § 24-4.9-1 et seq.	The DPA must be binding
Act (ICDPA)	business in the	Act, Farm Credit Act, GLBA,	capable of being	consumer's <u>freely</u>	provide consumers	of Article 4.9 of Title 24 of	and include instructions for
	state of Indiana	FCRA, Higher education	connected to a known or	given, specific,	with a clear and	the Indiana Code.	processing personal data,
	or produce	institutions, Government	identifiable individual,	informed, and	accessible privacy		details about the nature
	products or	organizations, Nonprofits.	does not include data	<u>unambiguous</u>	notice that includes		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 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 that operations 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 disclosed information; unless the consumer has restricted the information to a specific audience.

"Sensitive Data": information revealing racial or ethnic origin, religious beliefs, a mental 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.

<u>required</u> to <u>conduct</u> <u>and document DPIAs:</u> processing for <u>targeted</u> <u>advertising</u>, substantial injuries to consumers; or processing sensitive data, or in the event of heightened risk. personal data processed, purpose processing, instructions exercising consumer rights, and how they appeal, may categories of personal data shared with third parties, and categories of third parties involved. If a controller sells personal data or uses for targeted advertising, they must clearly disclose such activities and provide opt-out or preference management information for

consumers.

the categories of

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.

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

individual; Personal data collected from a known

			the information to a			Office of the Attorney	
			specific audience.			General ('AG').	
			"Sensitive Data" means			Exemptions apply.	
			racial or ethnic origin,				
			genetic or biometric,				
			precise location, child				
			data, etc.				
Montana	Applicable for	HIPPA, COPPA, Family	"Personal data" refers to	"Consent" means a	Yes.	There is a requirement to	Yes.
Consumer	persons that	Education Rights and	any information that is	clear affirmative act		notify breaches under	
Data	conduct business	Privacy Act, Driver Privacy	connected or reasonably	signifying a consumer's	Controllers must	§30-14-1704 of Part 17 of	The DPA between the
Privacy Act	in Montana or	Act, Farm Credit Act, GLBA,	capable of being	freely given, specific,	provide consumers	Chapter 14 of Title 30 of	controller and the
(MCDPA)	market	FCRA, Higher education	connected to a known or	informed, and	with an accessible	the Montana Code	processor is necessary to
<del></del>	commercial	institutions, Government	identifiable individual.	unambiguous	and clear privacy	Annotated 2017.	govern the processing of
	products or	organizations, Nonprofits.	The term excludes	agreement to allow the	notice that includes:		personal data on behalf of
	services that are	, ,	deidentified data and	processing of personal	categories of	Breach of the security of	the controller. The DPA
	targeted to		publicly available	data relating to the	personal data	the data system:	must be binding and
	Montana	Employment data is	information.	consumer. The term	processed, purpose	Unauthorized acquisition	include clear instructions
	residents and:	exempt.		may include a written	of processing,	of computerized data	for data processing,
	(i) Control or	·	"Publicly available	statement, a statement	categories of	that materially	specifying the purpose,
	process the	Shall not restrict the ability	<i>information</i> " means	by electronic means, or	personal data shared	compromises the	duration, and types of data
	personal data of	of controllers or processors	information that: is	any other unambiguous	with third parties (if	security, confidentiality,	involved. It should also
	at least 50,000	to: collect, use, and retain	lawfully made available	affirmative action.	applicable),	or integrity of personal	establish confidentiality
	consumers,	personal data internally	through federal, state, or		categories of third	information maintained	obligations, require the
	excluding data	without restrictions. This	municipal government	Consent is required for	parties involved,	by the person or business	return or deletion of data
	solely processed	includes conducting	records or widely	the following:	contact information,	and causes or is	at the controller's request,
	for payment	research for product	distributed media; or a	(i) For the processing of	and instructions for	reasonably believed to	and enable the controller
	transactions; or	development,	controller has a	personal data for	exercising consumer	cause loss or injury to a	to access information to
	(ii) Control or	improvement, repair,	reasonable basis to	purposes that are not	rights and appealing	Montana resident.	verify compliance. The DPA
	process the	recalls, fixing technical	believe a consumer has	reasonably necessary	decisions.		should address
	personal data of	errors, and performing	lawfully made available	to or compatible with		The covered entity that	subcontractors'
	at least 25,000	internal operations aligned	to the public.	the disclosed purposes		owns the personal data,	obligations, and the
	consumers and	with consumer		for which the personal		is required to notify,	processor must cooperate
	derive more than	expectations.	"Sensitive Data" means	data is processed as		including any service	with assessments of their
	25% of gross		racial or ethnic origin,	disclosed to the		provider they use are	data protection measures.
	revenue from the		health, genetic or	consumer unless the		required to notify the	Overall, the DPA ensures
	sale of personal		biometric, child data,	controller obtains the		owner.	proper data handling and
	data.		Precise geolocation data,	consumer's consent.			protection between the
	"Sale of personal		etc.			Montana residents must	controller and processor.
	data" is defined			(ii) Before processing		be notified if their	
	as "the exchange			sensitive data; and (iii)		unencrypted personal	
	of personal data			for targeted advertising		information is acquired	
	for monetary or			5		by an unauthorized	

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

			reasonable basis to	from the child's parent		made within 45 days of	
	"Sale of personal		believe is lawfully made	or lawful guardian		discovering the breach.	
	information" is		available to the general	_		_	
	defined as "the		public through widely	A Data Processing			
	exchange of		distributed media, by the	Assessment is required		Encryption exempts the	
	personal		consumer, or by a person	when processing		need for notification,	
	information for		to whom the consumer	activities that presents		unless the encryption key	
	valuable		has disclosed the	the sale of personal		is accessed. Information	
	monetary		information, unless the	information, processing		holders with their own	
	consideration by		consumer has restricted	for purposes of		notification procedures	
	the controller to		the information to a	profiling in certain case,		are considered	
	a third party."		specific audience.	processing of personal		compliant. GLBA and	
	, ,		·	data, and processing		HIPAA entities are	
			"Sensitive Data" includes	involving heightened		exempt from the	
			data revealing racial or	risk of harm to		requirements.	
			ethnic origin, religious	consumers.			
			beliefs, mental or			Notice to AG not	
			physical health diagnosis,			required.	
			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.				
New	Applicable	HIPPA, COPPA, Family	"Personal data" means	" <b>Consent</b> " means a	Yes	There is a requirement	Yes
<u>Hampshire</u>	persons that	Education Rights and	any information that is	clear affirmative act		to notify data breaches	
	conduct business	Privacy Act, Farm Credit	linked or reasonably	signifying a consumer's	Controllers must	pursuant to the <u>New</u>	The DPA should govern the
	in New	Act, GLBA, FCRA, Higher	linkable to an identified	freely given, specific,	provide consumers	Hampshire right to	processor's data processing
	Hampshire or	education institutions,	or identifiable individual.	informed and	with an accessible,	privacy act under §359-	procedures and clearly
	persons that	Government organizations,	"Publicly available	unambiguous	clear, and meaningful	C:1 et seq. of Title XXXI	outline instructions,
	produce products	_	<i>information</i> " means				responsibilities, and
	or services that		information that is	processing of personal	should include	Revised Statutes ('N.H.	obligations. The contract
	are targeted to	Employment data is	lawfully made available	data relating to the	categories of	Rev. Stat. Ann.').	must ensure
	the residents of	exempt.	through federal, state,	consumer.	personal data	,	confidentiality, require the
	New Hampshire.		municipal government		processed, purpose	Security breach:	deletion or return of
		Shall not restrict the ability	records, or widely	Consent is required for:	of processing,	Unauthorized acquisition	personal data, enable the
		of controllers or processors	distributed media, and a	(i) Processing personal	instructions for	of computerized data	controller to access
		to: conduct internal	•	data beyond what is	exercising consumer	that compromises the	necessary information for
				1 / 40 / 10 / 10			TO THE CONTRACT OF THE CONTRAC

		research, recall, repair	reasonable basis to	necessary for the	rights (including	security or confidentiality	demonstrating compliance,
		technical errors, and	believe a consumer has	disclosed purposes.	appeals), details on	of personal information	govern engagement with
		perform internal	lawfully made available	(ii) Before processing	data shared with third	maintained by a person	subcontractors, and allow
		operations aligned with	to the general public.	sensitive information.	parties, categories of	doing business in New	for assessments by the
		consumer expectations.		In the case of	third parties involved,	Hampshire.	controller or independent
		These activities should also	"Sensitive Data" means	processing sensitive	contact information,		assessors.
		be compatible with	data that includes data	data concerning a	and opt-out methods	Any data breach must be	
		processing data to provide	revealing racial or ethnic	known child, without	for data sale or	notified to the relevant	
		requested products or	origin, religious beliefs,	first obtaining consent	targeted advertising.	regulator. Prompt	
		services or fulfill	mental or physical health	from the child's parent	Secure and reliable	notification to consumer	
		contractual obligations.	condition or diagnosis,	or lawful guardian.	means for submitting	reporting agencies is, as	
			sex life, sexual	(iii) Consent required	rights requests	well as notification to	
			orientation or citizenship	for targeted advertising	should be established	affected individuals as	
			or immigration status;	of consumers aged 13-	as described in the	soon as possible after	
			the processing of genetic	16 years old.	notice.	confirming a breach.	
			or biometric data for the			Substitute notice may be	
			purpose of uniquely	A Data Processing		given if the cost exceeds	
			identifying an individual;	Assessment is required		\$5,000, more than 1,000	
			personal data collected	when processing		New Hampshire	
			from a known child; or,	activities that presents		residents are affected, or	
			precise geolocation data.	the <u>sale</u> of personal		if contact information is	
				information, processing		insufficient.	
				for purposes of			
				profiling in certain case,			
				processing of personal		It is mandatory to inform	
				data, and processing		AG if a breach occurs.	
				involving heightened			
				risk of harm to			
				consumers.			
Texas Data	Applicable to a	HIPPA, COPPA, Family	"Personal data" refers to	"Consent," in relation	Yes	There is a requirement	Yes
Privacy and	person that:	Education Rights and	any information, which	to a consumer, refers to		to notify data breaches	
Security Act	(i) Conducts	Privacy Act, Farm Credit	may include	a clear and	Controllers must	pursuant to the <u>Identity</u>	A DPA is needed, it must
(TDSPA)	business in Texas	Act, GLBA, FCRA, Higher	pseudonymous data and	<u>unambiguous</u>	provide consumers	Theft Enforcement and	include clear instructions,
	or produces a	education institutions,	sensitive data, that is	agreement expressed	with a clear and	Protection Act under	purpose, data type,
	product or	Government organizations,	connected or reasonably	through a freely given,	accessible privacy	Chapter 521 of Title 11	duration, rights, and
	service	Nonprofits, etc.	capable of being	specific, informed, and	notice. It should	of the Business and	obligations. The processor
	consumed by the		connected to a known or	unambiguous act,	include information	Commerce Code ('Tex.	must ensure
	residents of	Employment data is	identifiable individual.	indicating the	on the categories of	Bus. & Com. Code').	confidentiality, delete or
	Texas; (ii)	exempt.	W= 444	consumer's agreement	personal data		return data as directed,
	Processes or	<b>2</b> 1 11	"Publicly available	to process their	processed, including	Breach of system	provide compliance
	engages in the	Shall not restrict the ability	<i>information</i> " means	personal data. This	any sensitive data, as	security: Unauthorised	information, allow
	sale of personal	of controllers or processors	information that is	agreement can be	well as the purpose	acquisition of	assessments, and engage
	data; and <b>(iii)</b> Is	to: conduct internal	lawfully made available	provided through a	of processing.	computerized data that	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 compatible be with processing data to provide requested products or services fulfill contractual obligations.

through government records, or information that a business has a reasonable basis 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 physical health diagnosis, sexual orientation, or citizenship 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 personal 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.

<u>Data Breach Submission</u> <u>Form</u> 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	СРА	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	Х	V	Х	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 <sup>4</sup>	V	X	V	V
Right to object to or opt-out of automated decision-making	V	X	X	V	Х	V	X	V	V
Right to object to or opt-out of profiling	V	V	X	V	V	V	Х	V	V
Opt-in required for processing of sensitive personal data	V	V	<b>X</b> <sup>5</sup>	V	Х	V	X	V	V
Right to object to/restrict processing generally	Х	х	Х	Х	Х	Х	Х	X	Х
Right to non-discrimination	V	V	V	V	V	V	V	V	V
Notice at collection requirement	V	Х	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

<sup>&</sup>lt;sup>4</sup> 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

<sup>&</sup>lt;sup>5</sup> 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**, <u>and</u> 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



omerm@apm.law



Adv. Efrat Katz

Technology and Regulation Practice efratk@apm.law