

CONSUMER PERSONAL DATA - PRIVATE SECTOR

- *Applies* to legal entities that conduct business targeted to Washington residents and:
 - Control or process personal data of more than 100,000 consumers during a calendar year; or
 - Derive over 25 percent of gross revenue from the sale of personal data and process or control the personal data of over 25,000 consumers
- *Does not apply* to:
 - state agencies, local governments, or tribes
 - nonprofit corporations
 - institutions of higher education
 - municipal corporations
 - personal data governed by certain state and federal regulations
 - employment records
- Provides consumers with rights regarding their personal data:
 - Access
 - Correction
 - Deletion
 - Data portability
 - Opt-out of the processing of personal data for the purposes of targeted advertising, the sale of personal data, and profiling in furtherance of decisions that produce legal effects
- Specifies controller responsibilities of:
 - Transparency
 - Purpose specification
 - Data minimization
 - Avoid secondary use
 - Security
 - Nondiscrimination
 - Antiretaliation
 - Sensitive data
 - Nonwaiver of consumer rights
- Requires data protection assessments for the following activities:
 - Processing for targeted advertising
 - Sale of personal data
 - Processing for purposes of profiling where reasonably foreseeable risks are present
 - Processing of sensitive data
 - Any processing activities that present heightened risk of harm to consumers
- Specifies limitations for when the obligations imposed on controllers or processors under this chapter do not restrict a controller or processor, i.e., complying with federal, state, or local laws
- Authorizes sole Attorney General (AG) enforcement under the Consumer Protection Act (CPA)
 - Provides a 30-day cure period
 - Prescribes penalties of up to \$7,500 per violation if violation continues after cure
- Requires the AG to submit a report by July 1, 2022, evaluating the liability and enforcement provisions
- Preempts local regulations regarding the processing of personal data, except for those in effect as of July 1, 2020
- Provides an effective date of 120 days after enactment

DATA PROCESSED FOR A PUBLIC HEALTH EMERGENCY - PRIVATE AND PUBLIC SECTOR

BILL SECTION	PRIVATE SECTOR	PUBLIC SECTOR
SCOPE	<p>Regulates covered data processed for a covered process</p> <p>Covered data includes personal data and one or more of the following: specific geolocation data, proximity data, or personal health data.</p> <p>Covered purpose means processing of covered data for automated contact tracing purposes related to a state of emergency declared by the governor pursuant to current law</p>	Same as PRIVATE SECTOR provisions
PROHIBITIONS	<p>Regarding covered data, it is unlawful to:</p> <ul style="list-style-type: none"> • Process data unless an individual is provided notice and the individual provides consent • Disclose data to law enforcement • Sell data • Share covered data unless such sharing is governed by a contract 	Same as PRIVATE SECTOR provisions
CONSUMER RIGHTS	<ul style="list-style-type: none"> • Confirm processing data and access data • Opt-out of processing • Correction • Deletion 	Provisions do not apply to PUBLIC SECTOR
CONTROLLER RESPONSIBILITIES	<ul style="list-style-type: none"> • Comply with a request to exercise a right • Provide a privacy notice • Limit collection of data to what is required • Secure covered data • Delete or deidentify covered data when it is no longer needed for a covered purpose • Nondiscrimination 	<ul style="list-style-type: none"> • Similar to PRIVATE SECTOR provisions • <u>Does not</u> include provision related to comply with a request to exercise a right (Consumer Rights do not apply to PUBLIC SECTOR)
LIMITATIONS	<ul style="list-style-type: none"> • Specifies exemptions for complying with current law and research 	Same as PRIVATE SECTOR provisions
ENFORCEMENT	<ul style="list-style-type: none"> • Authorizes sole AG enforcement under the CPA • Provides a 30-day cure period; prescribes penalties of up to \$7,500 per violation if violation continues after notifying an individual of cure 	<ul style="list-style-type: none"> • Specifies that any individual injured by a violation of this chapter may institute a civil action to recover damages • Provides that any controller that violates this chapter may be enjoined
PREEMPTION	Preempts local regulations regarding the processing of covered data, except for those in effect as of July 1, 2020	Provisions do not apply to PUBLIC SECTOR
EFFECTIVE DATE	Immediately	Same as PRIVATE SECTOR provisions

Bill Section	2SSB 6281 Management and oversight of personal data (2020) <i>Senator Carlyle</i>	California Consumer Protection Act (CCPA)	Consumer Privacy Rights Act (CPRA)	Washington Privacy Act 2021 <i>Senator Carlyle</i>
PERSONAL DATA PRIVACY REGULATIONS - PRIVATE SECTOR				
Jurisdictional Scope	<p>Applies to legal entities that conduct business or produce products that are targeted to WA residents and:</p> <ul style="list-style-type: none"> Control data for over 100,000 consumers during a calendar year; or Derive over 50% of revenue from the sale of data and process personal data of over 25,000 consumers <p><u>Exemptions:</u> Specified entities and data:</p> <ul style="list-style-type: none"> State agencies, local governments, or tribes; Municipal corporations; Personal data regulated by certain federal and state regulations such as HIPAA, FCRA, GLBA, DPPA, FERPA, and COPPA parental consent Employment records 	<p>For profit businesses that collect and control California resident personal information and:</p> <ul style="list-style-type: none"> Has gross annual revenues over \$25 million; Control information of 50,000 or more CA residents, households, or devices; or Derive 50% or more of annual revenues from selling CA resident data <p><u>Exemptions:</u> Similar to 2SSB 6281</p>	<p>For profit businesses that collect and control CA resident personal information (PI) and:</p> <ul style="list-style-type: none"> As of January 1, of the calendar year, had gross revenues over \$25 million in the preceding calendar year; Annually buys, sells, or shares PI of over 100,000 consumers or households; or Derives 50% or more of revenue from selling or sharing consumer's PI <p><u>Exemptions:</u></p> <ul style="list-style-type: none"> PI regulated by federal and state regulations such as HIPAA, FCRA, GLBA, DPPA, and vehicle information for warranty purposes PI collected for job applications and employment records (expires) 	<p>Applies to legal entities that conduct business or produce products that are targeted to WA residents and:</p> <ul style="list-style-type: none"> Control data for over 100,000 consumers during a calendar year; or Derive over 25% of revenue from the sale of data and process personal data of over 25,000 consumers <p><u>Exemptions:</u> Same as 2SSB 6281 with the addition of:</p> <ul style="list-style-type: none"> Institutions of higher education Nonprofit organizations

Bill Section	2SSB 6281 Management and oversight of personal data (2020) <i>Senator Carlyle</i>	California Consumer Protection Act (CCPA)	Consumer Privacy Rights Act (CPRA)	Washington Privacy Act 2021 <i>Senator Carlyle</i>
Responsibility Roles	<ul style="list-style-type: none"> • Specifies controllers obligations and contract requirements • Requires processors to follow controller instructions • Prescribes processors assistance requirements and responsibilities 	Similar to 2SSB 6281	Similar to 2SSB 6281	Same as 2SSB 6281
Consumer Rights	<ul style="list-style-type: none"> • Access • Correction • Deletion • Data portability • Opt out of the processing of personal data for the purposes of targeted advertising, the sale of personal data, or to profiling in furtherance of decisions that have legal effects • Requires controllers to establish an internal appeals process 	<ul style="list-style-type: none"> • Request what personal data a business has about them, source, purpose and whether it is being disclosed or sold • Delete personal data with certain exceptions • Opt out to the sale of personal data by using a link titled “Do Not Sell My Personal Information” on the business home page 	<ul style="list-style-type: none"> • Access • Correction • Delete - business must notify third parties it shared data • Know what PI is sold or shared and to whom • Opt-out of sale or sharing • Limit use and disclosure of sensitive PI • Exercise rights through self-serve tools and without being penalized 	Same as 2SSB 6281
Responsibilities of Controllers	<ul style="list-style-type: none"> • Transparency • Purpose specification • Data minimization • Avoid secondary use • Security • Sensitive data • Nondiscrimination 	<ul style="list-style-type: none"> • Requires a privacy notice • Requires businesses to have a prominent opt out link on website home page 	<ul style="list-style-type: none"> • Similar to 2SSB 6281, i.e., disclosure of categories of data collected, purpose, and retention policies • Prohibits retaliation for exercising any right 	Similar to 2SSB 6281

Bill Section	2SSB 6281 Management and oversight of personal data (2020) <i>Senator Carlyle</i>	California Consumer Protection Act (CCPA)	Consumer Privacy Rights Act (CPRA)	Washington Privacy Act 2021 <i>Senator Carlyle</i>
Data Protection Assessment (DPA)	<ul style="list-style-type: none"> Specifies DPA scope and requirements Provides that DPAs conducted pursuant to other laws may qualify for compliance 	-	Requires business to submit risk assessments to the California Privacy Protection Agency (agency established in CPRA)	Same as 2SSB 6281
Compliance	Authorizes the attorney general (AG) to request a DPA relevant to an investigation; AG may evaluate compliance with controller responsibilities and other laws	Authorizes the AG to monitor compliance	Authorizes the AG to monitor compliance	Same as 2SSB 6281
Deidentified Data and Pseudonymous Data	Requires controllers or processors that use deidentified data to exercise oversight to monitor compliance with any contractual commitments	Reference in definitions	References in definitions and AG rulemaking	Same as 2SSB 6281
Limitations and Applicability	Specifies that the obligations imposed on controllers and processors do not restrict their ability to, amongst other things, comply with current laws and regulations	Similar to 2SSB 6281	Similar to 2SSB 6281	Same as 2SSB 6281
Preemption	Preempts local regulations regarding the processing of personal data by controller or processors	Preempts city, county, or local agency regulations regarding the collection and sale of consumers' personal information by a business	Preempts all regulations by a city, county, city and county, municipality, or local agency regarding the collection and sale of consumer's PI by a business	<ul style="list-style-type: none"> Same as 2SSB 6281 Adds exemption for local regulations in effect as of July 1, 2020
Liability	<ul style="list-style-type: none"> Prohibits use of chapter as basis for a private right of action (PRA) Allocates liability according to principles of comparative fault 	-	-	Same as 2SSB 6281

Bill Section	2SSB 6281 Management and oversight of personal data (2020) <i>Senator Carlyle</i>	California Consumer Protection Act (CCPA)	Consumer Privacy Rights Act (CPRA)	Washington Privacy Act 2021 <i>Senator Carlyle</i>
Enforcement	<ul style="list-style-type: none"> Provides sole AG enforcement Prescribes penalties of \$7,500 each violation 	<ul style="list-style-type: none"> Provides AG enforcement Prescribes penalties of \$2,500 each violation and \$7,500 each intentional violation Authorizes PRA for certain unauthorized access and exfiltration, theft, or disclosure of a consumer's nonencrypted PI 	<ul style="list-style-type: none"> Creates the California Privacy Protection Agency Adds to AG authority Maintain CCPA penalties Prescribes penalties of \$7,500 for each violation related to minors Authorizes PRA for unauthorized access and disclosure of nonencrypted PI 	<ul style="list-style-type: none"> Provides sole AG enforcement under the Consumer Protection Act (CPA) Provides a 30-day cure period; prescribes penalties of up to \$7,500 per violation if violation continues after notifying a consumer of cure
Facial Recognition (FR) Private Sector	<p>Provides regulatory framework, including:</p> <ul style="list-style-type: none"> Independent testing Meaningful human review prior to making decisions with legal effect Consent prior to enrolling an image Prohibits disclosure to law enforcement, exceptions apply 	-	-	-
Reports	Requires the AG to evaluate the liability and enforcement	-	-	-
Effective Date	July 31, 2021	January 1, 2020	<ul style="list-style-type: none"> CPRA applies to data collected after January 1, 2022 CCPA remains in effect until January 1, 2023 	120 days after enactment

2SSB 6281, CCPA, and CPRA do not include provisions related to data privacy regarding a public health emergency.

Washington Privacy Act 2021 (DRAFT)

Senator Carlyle

Bill Sections	DATA PRIVACY REGARDING PUBLIC HEALTH EMERGENCY PRIVATE SECTOR	DATA PRIVACY REGARDING PUBLIC HEALTH EMERGENCY PUBLIC SECTOR
Scope	Applies to controllers and processors that process covered data for a covered purpose . Covered data - Personal data and one or more of the following: specific geolocation data, proximity data, or personal health data Covered purpose - Processing of covered data concerning an individual for automated contact tracing related to a state of emergency declared by the governor pursuant to current law	Same as DATA PRIVACY REGARDING PUBLIC HEALTH EMERGENCY - PRIVATE SECTOR <u>Exempts</u> current public health contact tracing processes
Prohibitions	Regarding processing of covered data for a covered purpose, it is unlawful to: <ul style="list-style-type: none"> • Process unless provide a privacy notice and obtain consent • Disclose data to law enforcement • Sell covered data • Share data unless governed by a contract 	Same as DATA PRIVACY REGARDING PUBLIC HEALTH EMERGENCY - PRIVATE SECTOR
Consumer Rights	<ul style="list-style-type: none"> • Opt-out of processing • Access • Correct inaccurate data • Deletion 	<u>Does not apply</u> to PUBLIC SECTOR
Responsibility Roles	Same as 2SSB 6281	Similar to 2SSB 6281
Responsibilities of Controllers	<ul style="list-style-type: none"> • Transparency • Purpose specification • Data minimization • Avoid secondary use • Security • Deletion 	Same as DATA PRIVACY REGARDING PUBLIC HEALTH EMERGENCY - PRIVATE SECTOR
Limitations and Applicability	Specifies that the obligations do not restrict ability: <ul style="list-style-type: none"> • to comply with current laws and regulations; or • process deidentified data for research in the public interest 	Same as DATA PRIVACY REGARDING PUBLIC HEALTH EMERGENCY - PRIVATE SECTOR
Enforcement	<ul style="list-style-type: none"> • Provides sole AG enforcement under the CPA • Provides a 30-day cure period; prescribes penalties of up to \$7,500 per violation if violation continues after cure 	<ul style="list-style-type: none"> • Specifies that any individual injured by a violation of this chapter may institute a civil action • Provides that a controller that violates this chapter may be enjoined
Preemption	Same as 2SSB 6281 Adds exemption for local regulations in effect as of July 1, 2020	<u>Does not apply</u> to PUBLIC SECTOR
Effective data	Immediately	Immediately

Comparison of Federal COVID-related Privacy Legislation and the Washington Privacy Act 2021

	Provision	COVID-19 Consumer Data Protection Act of 2020 <i>Senator Wicker [R-MS]</i>	Public Health Emergency Privacy Act <i>Senator Blumenthal [D-CT]</i>	Exposure Notification Privacy Act <i>Senator Cantwell [D-WA]</i>	Washington Privacy Act 2021 <i>Senator Carlyle</i>
1	Applies to private sector	X	X	X	X
2	Applies to public sector		X		X
3	Covered data	Geolocation, proximity, and health data, and persistent identifiers	Geolocation, proximity, diagnosis, and demographic data and contact logs	Data collected with an automated exposure notification service	Personal data and geolocation, proximity, or personal health data
4	Covered purpose	Contact tracing and social distance compliance related to COVID-19	COVID-19 public health emergency	Digitally notifying exposure to infectious disease	Automated contact tracing for an infectious disease directly related to a state of emergency
5	Collaborate with public health authority			X	
6	Data Minimization	X	X	X	X
7	Privacy policies	X	X	X	X
8	Avoid secondary use		X	X	X
9	Security	X	X	X	X
10	Non-discrimination		X	X	X
11	Prohibitions	X	X	X	X
12	Affirmative consent	X	X	X	X
13	Right to revoke consent/opt-out	X	X		X (private sector only)
14	Right to access				X (private sector only)
15	Right to correct	Report inaccuracies	X		X (private sector only)
16	Right to delete			X	X (private sector only)
17	Retention limitation	X	X	X	X
18	Exemptions		X	X	X
19	Preemption	X			X (private sector only)
20	Platform responsibility			X	
21	Reporting requirements	X	X	X	
22	Enforcement	FTC and state AG	FTC and state AG	FTC and state AG	state AG
23	Private right of action		X	X	X (public sector only, current law)
24	Covers non-COVID data				X (private sector only)

Automated Contact Tracing Information

Prepared for Senator Reuven Carlyle

RESOURCES

[Responsible Data Use Playbook for Digital Contact Tracing](#), FPF and BrightHive, July 21, 2020

The playbook provides a series of considerations to assist stakeholders in setting up a digital contact tracing initiative to track and manage the spread of COVID-19, while addressing privacy concerns raised by these technologies in an ethical, responsible manner.

[Use of the Apple | Google exposure notification framework \(A|G ENF\)](#), June 2020

Public Health Informatics Institute provides a white paper to help state and local public health officials learn about the A|G ENF and decide whether to build and deploy a statewide app for uses to receive exposure alerts for enhanced COVID-19 contact tracing.

[COVID-19 contact tracing tools](#), TechCrunch, June 5, 2020

Demonstration videos of 15 contact tracing tools sorted into three broad categories:

- (1) contact-tracing/exposure-notification applications using Google/Apple API
- (2) contact-tracing/exposure-notification applications not using Google/Apple API
- (3) personal-symptom-tracking applications

[Digital Contact Tracing Technology](#), Congressional Research Service, May 29, 2020

Overview and considerations for the implementation of digital contact tracing technology.

[Key aspects of location data](#), Future of Privacy Forum (FPF), May 22, 2020

Infographic outlines how location data is generated from mobile devices, who has access to it, and factors to consider in evaluating privacy risks.

[MIT Technology Review: COVID Tracing Tracker Project](#), May 7, 2020

A database to capture details of every significant automated contact tracing effort around the world. [Database - read-only \(Last updated on July 9, 2020\)](#)

STATE LEGISLATION

In 2020, legislation related to contact tracing and privacy have been introduced in at least eight states. Kansas enacted legislation and in New York legislation has been sent to the governor.

[Broad list of all contact tracing bills](#), NCSL, June 15, 2020



RECENT PUBLICATIONS

- o [Data privacy laws collide with contact tracing efforts; privacy is prevailing](#), Thomson Reuters Regulatory Intelligence, July 21, 2020
- o [Security flaws found in South Korea quarantine app](#), The New York Times, July 21, 2020
- o [Contact Tracing Apps Aren't Going to Solve the Pandemic](#), Governing, June 15, 2020
- o [Apple and Google impact on COVID-19 app development in Europe](#), Politico EU, May 16, 2020