



Front Burner Privacy Compliance Issues for 2022

Gretchen A. Ramos, CIPP/E/US, CIPM
Global Co-Chair Data, Privacy & Cybersecurity Group
415.655.1319 | ramosg@gtlaw.com

Agenda



1. CPRA, VCDPA, & CPA

- Comparison of the Three Laws
- New Provisions & How They Impact Compliance
- Compliance Plan

2. On the Horizon in 2022

- State Privacy Legislation
- India - Personal Data Protection Bill
- Quebec - Bill 64
- Privacy Shield 2.0
- United Kingdom Developments
- ePrivacy Regulation

3. Questions

A low-angle, upward-looking perspective of several modern skyscrapers. The buildings are constructed from glass and steel, with their facades reflecting the sky. They converge towards the top of the frame, creating a strong sense of height and scale. The sky is a clear, vibrant blue, dotted with soft, white cumulus clouds. The overall composition is symmetrical and dynamic, emphasizing the architectural grandeur of the urban environment.

New State Privacy Laws

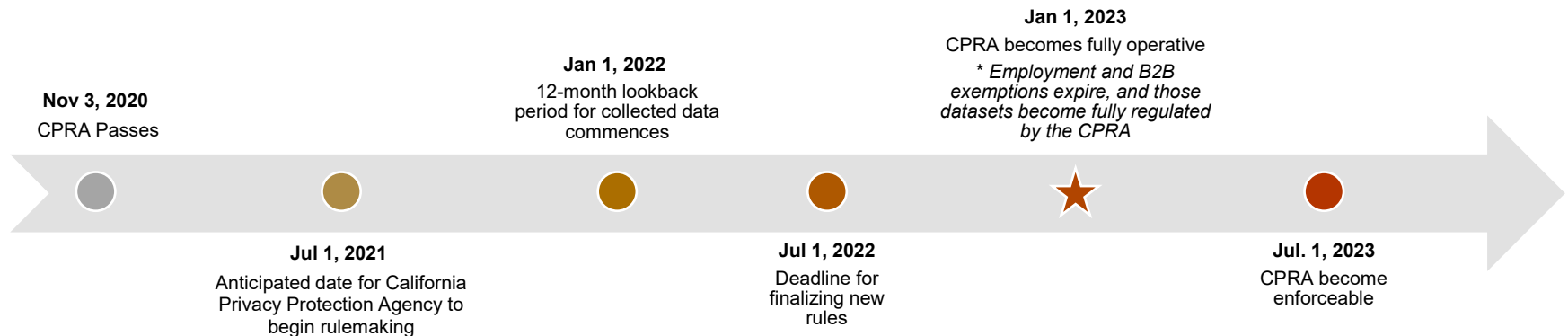
CPRA, VCDPA & CPA

California, Leading the Charge...

Background

- The California Privacy Rights Act of 2020 (“CPRA”) is “Phase 2” for data privacy compliance in California.
- CPRA significantly amends the California Consumer Privacy Act (“CCPA”) and creates new rights and imposes additional obligations on business.
- The CCPA will remain in full force and effect until the CPRA becomes effective on Jan. 1, 2023.
- A new California agency called the California Privacy Protection Agency (CPPA) will be created and will promulgate new regulations by July 1, 2022; which will become enforceable on July 1, 2023.

CPRA Timeline



How Does the CPRA Modify the CCPA?



Benefits to Businesses

- Trade Secrets Exempt. Establishes an exemption from disclosure for trade secrets.
- Publicly Available Information Exempt and Expanded. Expands the exemption for information that is “publicly available.”
- HR & B2B Exemption Deferred. Defers employee data and some B2B data from 2022 (current enforcement date) until 1.1.23.

How Does the CPRA Modify the CCPA?

Burdens on Businesses

- Retention Periods & Data Minimization. Prohibits businesses from retaining PI for longer than “reasonably necessary.” Businesses must also inform consumers of the length of time they retain each category of PI.
- Right of Correction. Allows consumers to request that a business correct any inaccurate PI it maintains about them.
- Right to Opt-Out of Behavioral Advertising. Allows consumers to “opt out” of all online behavioral advertising regardless of whether a company “sells” information to an AdTech company.
- Right to Object to the Use/Disclosure of Sensitive Information. Allows consumers to limit a business’s use and/or disclosure of “sensitive personal information,” a new category and definition. Businesses that collect “sensitive personal information” must display a new opt-out link on their homepages.
- Right to Opt-Out of Automated Decision Making & Profiling. Businesses may have to allow consumers to opt-out of automated decision-making technology
- New Contracting Requirements. Requires businesses to enter into contracts extending the CPRA requirements to these entities’ handling of such PI, and requires service providers to have similar contracts in place with any sub-service providers.
- Security Audits. Requires businesses to perform a “cybersecurity audit” annually if the use of PI presents a “significant risk to consumers’ privacy or security.”
- Privacy Risk Assessments. Requires businesses to submit a risk assessment “on a regular basis” to the California Privacy Protection Agency.

CPRA Individual Rights

- ❖ **Right to Correction.** Consumers may request any correction of their PI held by a business if that information is inaccurate. ✓ **New**
- ❖ **Right to Opt Out of Behavioral Advertising.** Consumers may opt out of the sharing of their PI with cross-context behavioral advertising companies. ✓ **New**
- ❖ **Right to Opt Out of Use of Sensitive PI.** Consumers may limit the use and disclosure of sensitive PI for certain “secondary” purposes, including prohibiting businesses from disclosing sensitive PI to third parties, subject to certain exemptions. ✓ **New**
- ❖ **Right to Opt Out of Automated Decision-Making Technology.** Consumers may opt out of automated decision-making technology, including “profiling,” in connection with decisions related to a consumer’s work performance, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. ✓ **New**
- ❖ **Right to Access Information About Automated Decision Making.** The CPRA authorizes regulations allowing consumers to make access requests seeking meaningful information about the logic involved in the decision-making processes and a description of the likely outcome based on that process. ✓ **New**
- ❖ **Right to Access.** Consumers may request access to a copy of specific information, including (i) categories and specific pieces of PI collected; (ii) categories of sources from which PI is collected; (iii) purpose for collecting or selling PI, and (iv) categories of third parties with whom the business shares PI for the last 12 months. ! **Modified**
- ❖ **Right to Delete.** Businesses are required to delete (upon request) any PI that the business has collected “from the consumer” if an exception does not apply. Businesses must direct service providers to delete the PI from their records. notify third parties to delete any consumer PI bought or received, subject to certain exceptions. ! **Modified**
- ❖ **Opt-In Rights for Minors.** Businesses cannot share or sell PI of consumers under 16 without express authorization. As with the opt-out right, businesses must wait 12 months before asking a minor for consent to sell or share his or her PI after the minor has declined to provide it. ! **Modified**
- ❖ **Right to Opt Out of Sale & Right to Nondiscrimination.** Remain the same.

Comparison of State Privacy Laws

		GDPR	CCPA	CPRA (eff. 1.1.23)	VCDPA (eff. 1.1.23)	CPA (eff. 7.1.23)
Ability to Process Data	Permissible Purpose	✓			✓ (Consent for sensitive data)	✓ (Consent for sensitive data)
	Data Minimization	✓		✓	✓ (Only extends to collection)	✓ (Only extends to collection)
Individual Rights	Right to be Informed (aka Notice to Data Subjects)	✓	✓	✓	✓	✓
	Right to Access	✓	✓	✓	✓	✓
	Right to Correction (aka Right to Rectification)	✓		✓	✓	✓
	Right to Deletion (aka Right to Be Forgotten)	✓	✓	✓	✓	✓
	Right to Opt-Out of Behavioral Advertising	✓*		✓	✓	✓
	Right to Opt-Out of Sale	✓*	✓	✓	✓	✓
	Right to Object to Use of Sensitive Information	✓*		✓		
	Right to Nondiscrimination	✓*	✓	✓	✓	✓
	Financial Incentive Disclosure		✓	✓		
Accountability & Governance	Documentation and Recordkeeping	✓		✓		
	Privacy Risk Assessment	✓		✓	✓	✓
Security	Appropriate Data Security to Safeguard Information	✓	✓	✓	✓	✓
	Breach Notification	✓	✓ (Related statute)	✓ (Related statute)	✓ (Related statute)	✓ (Related statute)
Transfers to Third Parties	Contractual Requirements in Service Provider Agreements	✓		✓	✓	✓

* As part of larger right to object to legit. interest or withdraw consent.

Key Differences in State Privacy Laws

- ✓ Scope - Who Is Subject to the Law
- ✓ Cure Period
- ✓ Enforcement/Fines
- ✓ Contracting Requirements
- ✓ Opt-Out Rights
- ✓ Sensitive Data Requirements

Scope

CPRA (uses business/ service provider/ contractor, third party)

Applies to:

1. For-profit legal entity that collects consumers' PI and that determines the purposes and means of processing, that does business in the State of California, and that satisfies one or more of the following thresholds:
 - (A) As of January 1 of the calendar year, had annual gross revenues in excess of twenty-five million dollars **(\$25,000,000)** in the preceding calendar year or
 - (B) Alone or in combination, annually **buys, sells, or shares the personal information of 100,000 or more consumers or households** or
 - (C) **Derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information.**
2. Any entity that **controls or is controlled by a business**, as defined in paragraph (1), and that shares **common branding** with the business and with whom the **business shares consumers' personal information.**
3. A **joint venture or partnership** composed of businesses in which each business has at least a 40 percent interest.
4. A person that does business in California, that is not covered by paragraph (1), (2), or (3) and that **voluntarily certifies to the California Privacy Protection Agency that it is in compliance with, and agrees to be bound by, this title.**

VCDPA (GDPR terminology – controller / processor)

Applies to persons that conduct business in the Commonwealth or produce products or services that are targeted to residents of the Commonwealth and that

- (i) during a calendar year, control or process personal data of at least **100,000 consumers or**
- (ii) control or process personal data of at least **25,000 consumers and derive over 50 percent of gross revenue from the sale of personal data.**

CPA (GDPR terminology – controller / processor)

Applies to “controller” that:

- (a) conducts business in Colorado or produces or delivers commercial products or services that are intentionally targeted to residents of Colorado; and
- (b) satisfies one or both of the following thresholds:
 - (i) controls or processes the personal data of one hundred thousand **(100,000) consumers** or more during a calendar year; or
 - (ii) **derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of twenty-five thousand (25,000) consumers or more.**

Entity Exemptions

CPRA	VCDPA	CPA
Non-profits exempt	Non-profits exempt	No exemption for non-profits
Exempts personal information subject to GLBA, CalFIPA, FCRA	Financial Institutions subject to GLBA	Financial Institutions subject to GLBA
Health care providers governed by CMIA, and CEs governed by HIPAA	Entities regulated by HIPAA	Includes broad exemptions for HIPAA-regulated data and certain other data maintained by covered entities, business associates, and other health care entities
Exempts medical information governed by the CMIA and PHI collected by CA or BA governed by HIPAA		
Data regulated by FERPA, To the extent education institution is not-for-profit, exempt based on business definition	Certain higher education institutions	State institutions of higher education

Human Resource & B2B

✓ *California – In Scope*

- ✓ CCPA's HR and B2B exemptions expire on 1.1.23 when the CPRA takes effect.

✓ *Virginia - Exempt*

- ✓ "consumer" definition excludes persons acting in "commercial or employment context"
- ✓ exempts data maintained about applicants, employees, contractors, and emergency contacts and beneficiaries

✓ *Colorado - Exempt*

- ✓ "consumer" definition excludes persons acting in a "commercial or employment context"
- ✓ general exemption for "data maintained for employment records purposes"

Non-Compliance Consequences

	CPRA	VCDPA	CPA
Cure Period	CCPA's 30 day cure period eliminated CPPA may offer cured period	AG must provide 30 day cure period prior to initiating enforcement action	AG must provide 60 day cure period (if cure is possible) before initiating enforcement action Cure period expires 1.1.25
Fines	\$2,500 per violation \$7,500 per intentional violation or violation involving consumer under 16	\$7,500 per violation	\$20,000 per violation under the Colorado Consumer Protection Act
Enforcement	California AG & California Privacy Protection Agency (CPPA)	Virginia AG	Colorado AG & Colorado District Attorneys

Opt-Out Rights

California (CPRA). Consumers can opt-out of (1) the “sale” of personal information and (2) “sharing” of personal information. “Sharing” is defined to include sharing personal information with a third party “for cross-context behavioral advertising, whether or not for monetary or other valuable consideration.”

Virginia (VCDPA). Consumers can opt-out of: (1) targeted advertising; (2) the “sale” of personal data; and (3) profiling in furtherance of decisions that produce legal or similarly significant effects.

- “Targeted advertising” is defined to include displaying ads based on personal data obtained from consumer activities over time and across non-affiliated websites or applications.
 - “Sale” is defined to include the exchange of personal data for monetary consideration.”
 - “Profiling” is defined to include automated processing of personal data to analyze or predict consumer activities or characteristics. “Legal or similarly significant effects” include, among other things, decisions that impact financial services, housing, employment, and health care.
- Colorado (CPA). Consumers can opt-out of: (1) targeted advertising; (2) the “sale” of personal data; and (3) profiling in furtherance of decisions that produce legal or similarly significant effects.
- Follows the VCDPA’s definitions for targeted advertising and profiling in furtherance of decisions that produce legal or similar significant effects.
 - Follows the CCPA/CPRA definition for “sale” (i.e., it covers transfers of personal data for “other valuable consideration”).

Sensitive Data Requirements

- California (CPRA).
 - Consumers have the right to limit the use of “sensitive personal information” (e.g., government identification numbers, precise geolocation data, biometric data) to certain business purposes (e.g., purposes necessary to provide a service requested by the consumer). If a business is processing sensitive personal information for purposes other than the core purposes permitted by the CPRA, consumers have a right to stop such processing.
- Virginia (VCDPA).
 - Controllers must obtain opt-in consumer consent to process “sensitive data” (e.g., data revealing racial or ethnic origin, health data, precise geolocation data, biometric data, data of a known child). Parental consent is required to process the data of a consumer under 13 years of age.
- Colorado (CPA).
 - Controllers must obtain VCDPA’s opt-in consumer consent to process “sensitive data” (e.g., data revealing racial or ethnic origin, health data, biometric data, data of a known child). Parental consent is required to process the data of a consumer under 13 years of age (data regulated by COPPA is completely exempt from the requirements of the CPA).

Contracting

California

- General set of contract requirements that businesses must implement with (1) third parties to which the business sells or shares personal information and (2) contractors and service providers to which the business discloses personal information for business purposes.
- Among other things, contracts must prohibit the recipient from selling or sharing the personal information or retaining, using, or disclosing personal information other than for specified purposes.

Virginia & Colorado

- Similar to Article 28, GDPR data processing agreements.
- Contracts between controllers and processors must be in writing and set forth (i) the processing instructions including the nature and purpose of the processing; (ii) the type of personal data and duration of the processing; and (iii) obligations to delete or return all personal data at the end of the services period.



Compliance Strategy

Compliance Checklist


It will take most businesses at least 12 months to become substantially compliant with the state privacy laws.

- **Step 1: Scope** - Determine if you are a covered business/ controller under the state privacy laws.
- **Step 2: Team** - Identify the members of the team that will lead the compliance project.
- **Step 3: Gap Assessment** - Undertake an initial assessment of your data protection program to identify gaps in compliance and develop a detailed work plan based on that assessment.
- **Step 4: Data Inventory** - Create or update your data inventory, so that you have a complete understanding of how your organization is processing and sharing personal information, be sure to identify sensitive personal information.
- **Step 5: Contracting** - Identify review and reach out to your vendors, services providers, processors to put in place compliant data processing addendums.
- **Step 6: Website Compliance** - Review all digital advertising on the website and otherwise to ensure that it structured in compliance with the applicable laws.
- **Step 7: Rights Request** - Review, revise and update your consumer rights requests procedure to address new requirements under CPRA, VCDPA and CPA.
- **Step 8: PIA** - If your organization engages in high-risk processing activities perform and document a privacy impact assessment.
- **Step 9: Procedures** - Review, update and revise all internal privacy policies and procedures to make sure they are compliant with the new state laws.
- **Step 10: Privacy Policy** - Review and update website Privacy Policy.
- **Step 11: Training** - Update training materials, implement procedures for training and conduct training.

CRPA Compliance Steps

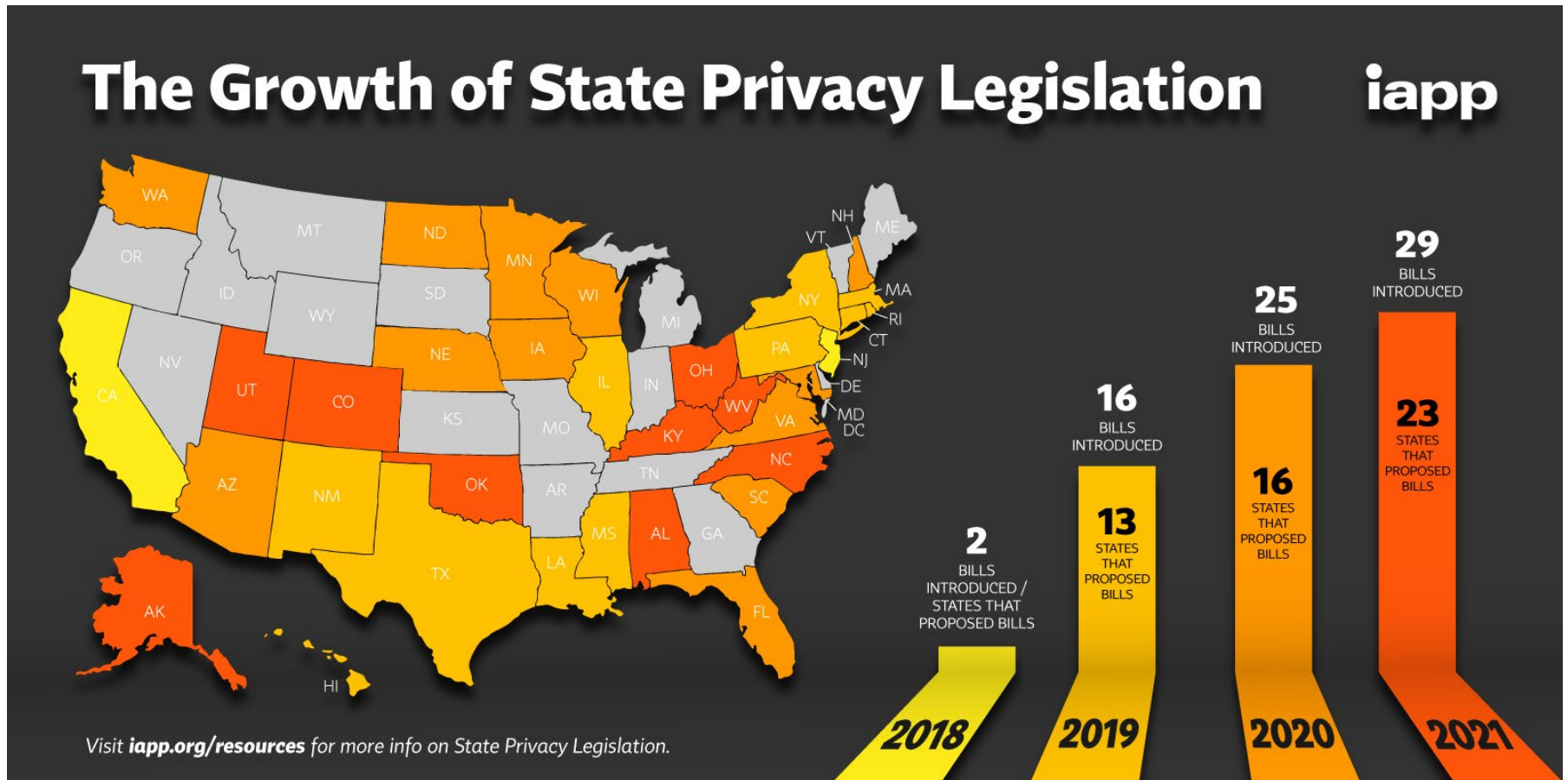
HR Data

- Revise (or develop) workforce disclosures to include new definitions and rights.
- Develop workforce request workflows for rights to access, receive, correct, and delete personal information.
- Put in place contractual provisions with workforce vendors including diligence and contractual indemnity.

A low-angle, upward-looking perspective of several modern skyscrapers. The buildings are characterized by repetitive horizontal window patterns and are arranged in a way that creates a sense of height and scale. The sky is a clear, vibrant blue, punctuated by soft, white cumulus clouds. The overall composition is symmetrical and dynamic, emphasizing architectural grandeur.

On the Horizon 2022

More State Privacy Legislation?



Active Privacy Bills



- Pending Legislation
 - Massachusetts Information Privacy Act
 - New York Privacy Act, Digital Fairness Act
 - Ohio Personal Privacy Act
 - Minnesota Consumer Data Privacy Act
 - North Carolina Consumer Privacy Act
 - Pennsylvania, HB 1126



India's *Draft* Personal Data Protection Bill

- Effective Date: Final version not issued, draft bill provides companies 18 months from enactment date to come into compliance.
- Broad Territorial Scope: Applies to companies (a) processing data within the territory of India or (b) that have a connection with any business carried on or a connection with any activity involving the profiling of data within the territory of India.
- Fines: Range from 2%-4% of the worldwide turnover or 5-15 crores rupees whichever is higher (appr. \$675k - \$2M)
- Legal Bases for Processing: Six legal bases, similar to GDPR; separate bases for processing sensitive data.
 - However, trade union memberships, racial or ethnic origin and philosophical beliefs are not considered sensitive personal data.
- Overlap with GDPR: Individual rights, breach notification to supervisory authority, definition of personal data, DPIAs, record of processing activities.
- Localization: Data fiduciaries (controllers) transferring data outside of India are required to maintain a copy of the data within India.
- International Transfers: Subject to adequacy decisions, SCC approved by Authority, necessity as determined by Authority, data subject's consent.

ePrivacy Regulation



- Purpose:
 - To create rules for electronic communications and protect the privacy of end users, the confidentiality of their communications and the integrity of their devices.
 - Covers not only personal data but also metadata and confidentiality requirements, and will apply to instant messaging apps, Voice over Internet Protocol (VoIP) platforms, and machine-to-machine communication.
- Impact: Increased privacy protection for EEA data when they are transmitted electronically that is uniformly enforced across EU member states. Will impact most companies as it will apply to digital marketing/cookies.
- Being Finalized: Will replace the existing ePrivacy and Electronic Communications Directive 2002/58 and could be finalized in 2022.
- Grace Period: Will apply 24 months from the date the Regulation enters into force.
- Fines: Will be in line with GDPR - 4%/2% of global annual revenue or €20/10 million, whichever is higher.

United Kingdom Data Protection Regime

“Now that we have left the EU, we have the freedom to create a bold new data regime: one that unleashes data’s power across the economy and society for the benefit of British citizens and British businesses whilst maintaining high standards of data protection.”

Department for Digital, Culture Media & Sport –
Data: A new direction, 10 Sept 2021.

- Potential to significantly alter the data protection landscape in the UK.
- Seeking to make changes to establish a “pro-growth and innovation friendly” data protection regime that is more practical and “business friendly”.
- More risk-based approach and a shift away from a “one size fits all” approach to compliance with data regulations, which should reduce burdens on business.



Cross-Border Transfers

- **EEA**

- Further guidance and perhaps SA decisions on supplementary measures and transfer impact assessments under the new EU SCCs.
- Perhaps Privacy Shield 2.0 finalized.

- **United Kingdom**

- Publication of UK International Data Transfer Agreement (<https://ico.org.uk/media/about-the-ico/consultations/2620396/intl-data-transfer-agreement-202100804.pdf>), and UK Addendum to the EU SCCs (<https://ico.org.uk/media/about-the-ico/consultations/2620398/draft-ico-addendum-to-com-scc-20210805.pdf>).

- **Others** – Japan, Quebec, Brazil

APPI Amendments

Most recent APPI Amendments enacted June 2020, and effective **April 2022**.



Changes Include

Enhanced Data Subject Rights – added right to deletion, stop processing, stop transfers, access to records of transfers

PIC must inform data subjects of the details of the transfer to a third party in a foreign country.

Data breach notifications are mandatory where breach would result in violation to individual's rights.

PPC will have authority to order foreign business to take necessary measures and can publish when business fails to do so.

New obligations for transferring data to third parties of internationally.

Impact

Privacy notices will need to be updated.

Privacy notice will need to be updated.

Incident response plan will need to be updated.

Impact on brand if not in compliance.

Contracting provisions, and privacy notice will need to be updated.

Quebec Bill 64 – the Act

- **Effective Data.** Will come into effect in three stages over three years, with most provisions coming into effect in Sept. 2023.
- **Scope.** Applies to those “carrying on an enterprise” within Quebec and the Commission d'accès à l'information (“CAI”), which is Quebec’s privacy regulator, regularly exerts jurisdiction (under the old privacy law and other privacy laws) over entities that operate completely outside of Quebec.
- **Penalties.** Administrative penalties for breaches would be \$50,000 per individual says Bernier, and for corporations up to \$10 million, or 2 per cent of global revenues, whichever is higher. Criminal penalties are even greater: 4 per cent of an organization’s gross global revenue in its financial year before the one in which the organization is sentenced, or \$25 million, whichever figure is higher, and \$100,000 per individual.
- **Privacy Impact Assessments.** Requires entities to conduct mandatory Privacy Impact Assessments (“PIA”) in three scenarios: (1) acquisition, development, and redesign of any information systems or electronic services involving PI; (2) transfers of PI to somewhere outside of Quebec; and (3) communications of PI without consent for study, research, or statistical purposes.

A low-angle, upward-looking perspective of several modern skyscrapers. The buildings are characterized by repetitive horizontal window patterns and are arranged in a way that creates a sense of height and scale. The sky is a clear, vibrant blue, punctuated by a few wispy white clouds. The overall composition is symmetrical and geometric, emphasizing the architectural lines of the buildings.

Questions