# Data Protection Laws in US & Canada

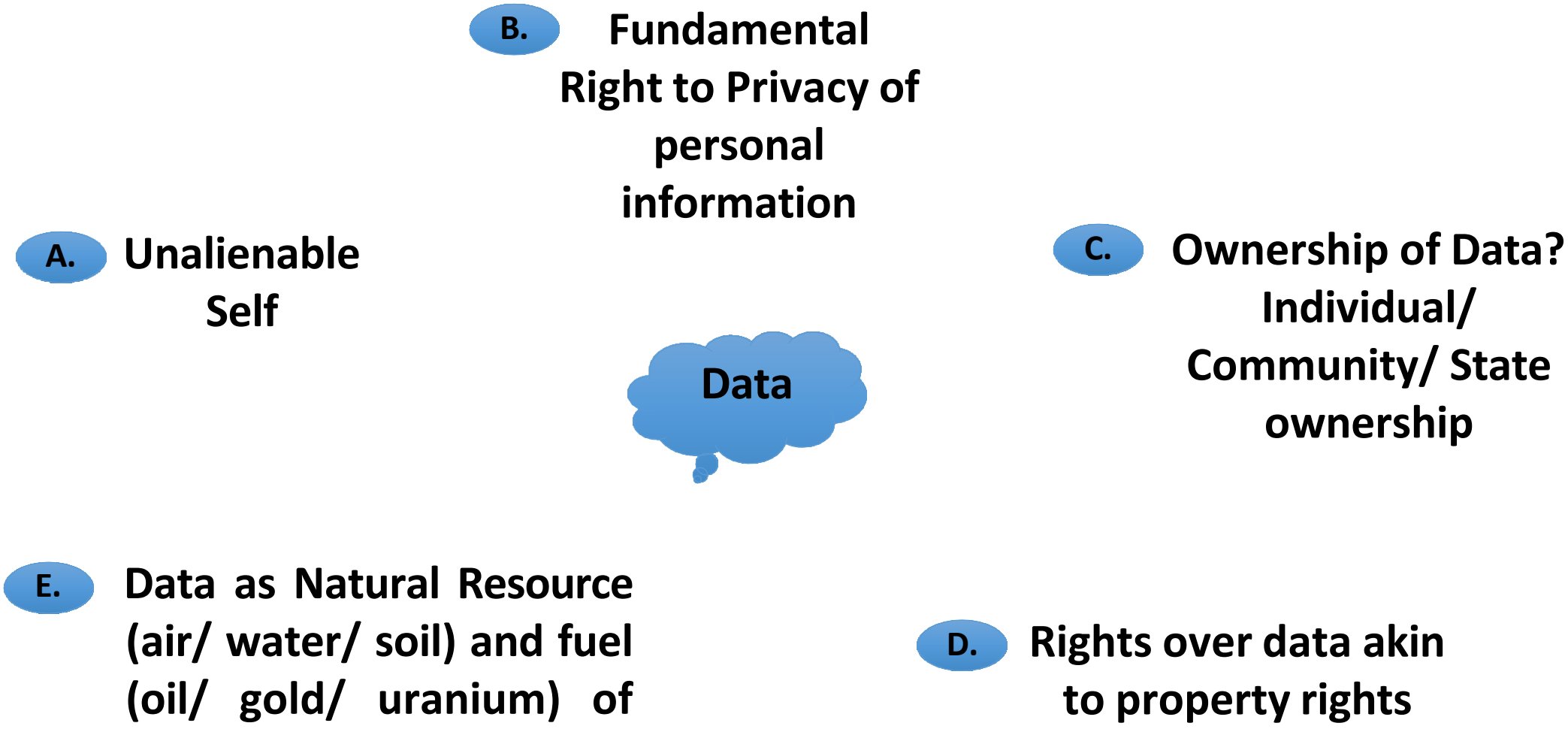
## NALSAR

06-12-23

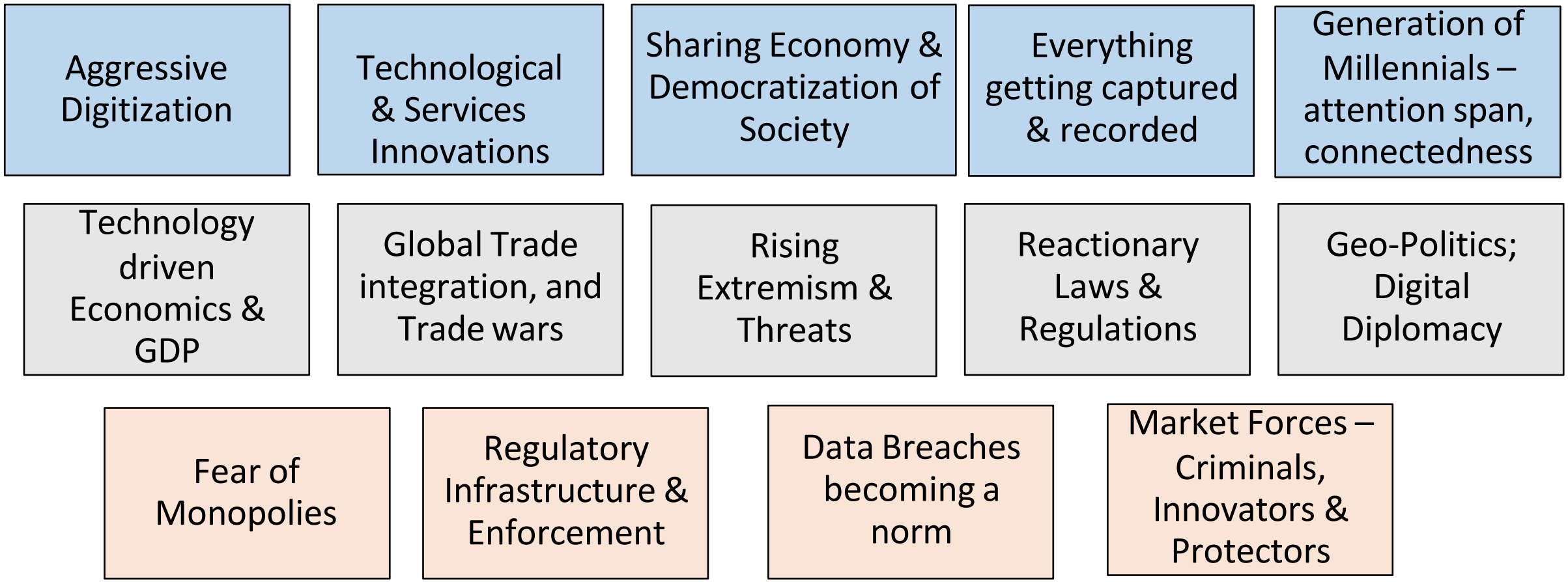
RAHUL SHARMA

FOUNDER – THE PERSPECTIVE

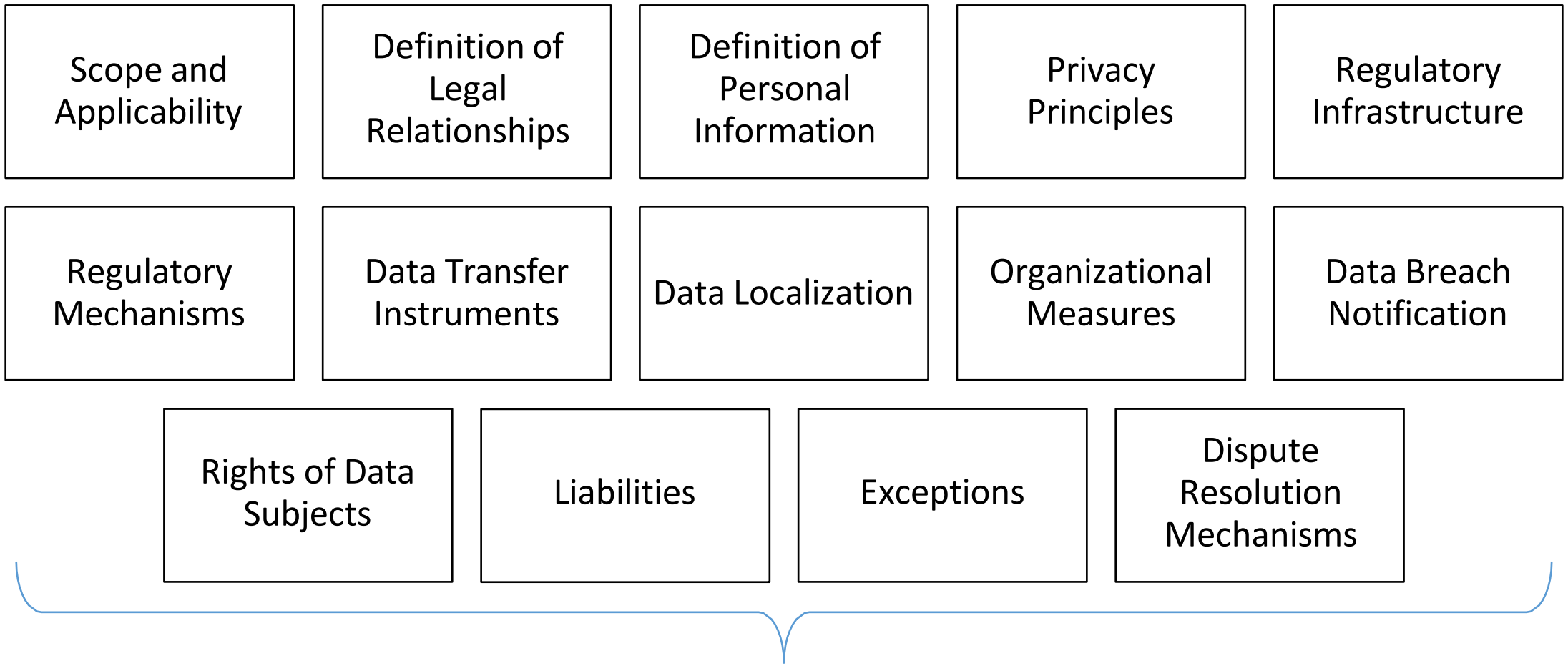
FOUNDER - DIRECTOR- GRADE ACE


B.
Fundamental Right to Privacy of personal information
A.
Unalienable Self
Data
C.
Ownership of Data? Individual/ Community/ State ownership
E.
Data as Natural Resource (air/ water/ soil) and fuel (oil/ gold/ uranium) of digital economy
D.
Rights over data akin to property rights

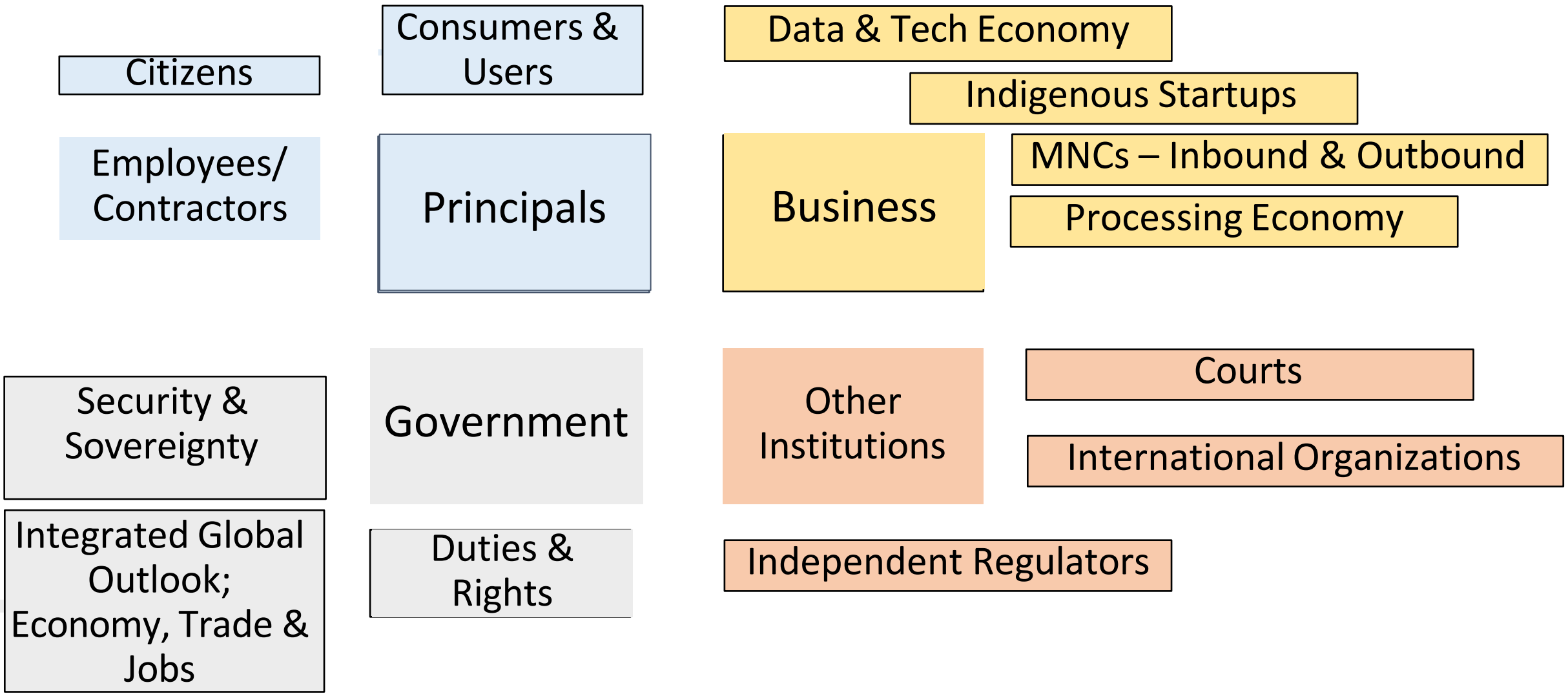
# Context of Data Ecosystem



# Components of Data Protection Law



# Stakeholders' Perspective(s)



# Privacy risks include, but not limited to:

- failure to have the appropriate legal authority to collect, use or disclose personal information;
- excessive collection of PII (loss of operational control);
- unauthorized access to PII (loss of confidentiality);
- unauthorized modification of the PII (loss of integrity);
- loss, theft or unauthorized removal of the PII (loss of availability);
- unauthorized or inappropriate linking of PII;
- failure to keep information appropriately secure;
- retention of personal information for longer than necessary;
- processing of PII without the knowledge or consent of the PII principal (unless such processing is provided for in the relevant legislation or regulation); and
- sharing or repurposing PII with third parties without the explicit informed consent of the data subject

# Privacy Assessment Typical Solutions

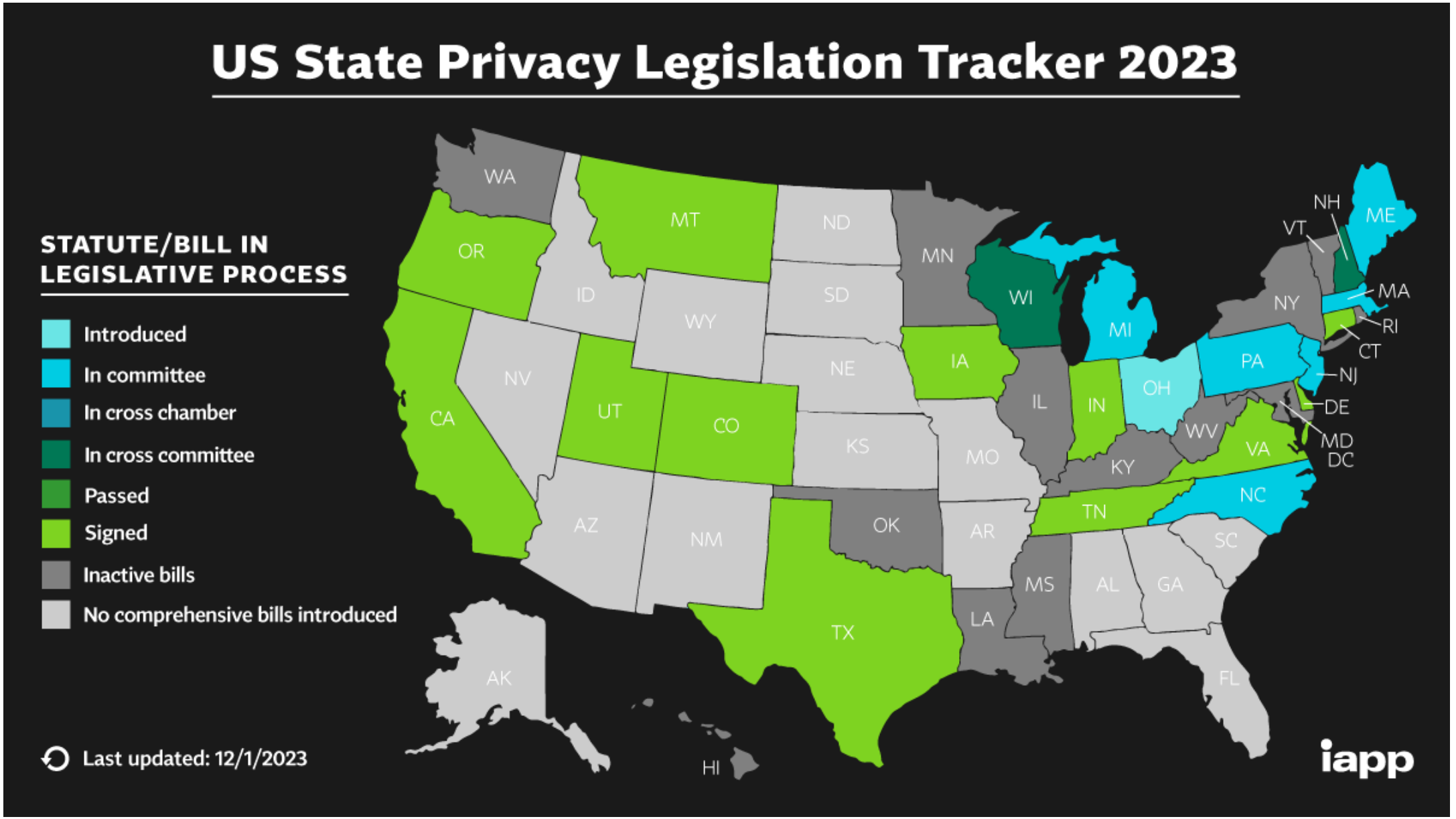
- deciding not to collect, use or disclose particular types of personal information;
- creating retention periods that only keep information for as long as necessary and planning the secure disposal of information;
- implementing appropriate technological, procedural and physical security measures;
- ensuring that staff are properly trained and are aware of the potential privacy impact and appropriate privacy-protective measures to be followed;
- developing ways to safely anonymize and/or de-identify the information, where possible;
- producing guidance for staff on how to use new programs, processes and systems, and how and when it is appropriate to collect, use, access, disclose and dispose of personal information;
- taking steps to ensure that individuals are fully aware of how their information is used and that they can contact the institution for assistance, if necessary;
- selecting third parties that will provide a greater degree of security and ensuring that agreements are in place to protect the personal information in the custody of the third parties; and
- producing information sharing agreements that clarify what information will be shared, how it will be shared and with whom it will be shared

# US Federal Data Protection Framework

- Gramm-Leach-Bliley Act
- Federal Trade Commission Act (Enforcement of Unfair and Deceptive Trade Practices)
- Fair Credit Reporting Act/FACTA
- Family Educational Rights and Privacy Act (FERPA)
- SEC disclosure requirements
- Federal Sector Requirements
  - Federal Information Security Management Act
  - OMB's Breach Notification Policy
  - Veterans Affairs Information Security Act
- Children's Online Privacy Protection Act
- HIPAA/HITECH
- Pending federal bills American Data Privacy Protection Act (ADPPA)
- Consumer health privacy laws – Washington, Nevada, Connecticut
- State Data Protection Laws….

| 2021 PROPOSED FEDERAL LEGISLATION | |
|---|---|
| Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA) Act (S.2499) | Consumer Data Privacy and Security Act of 2021 (S.1494) |

Data Privacy Law Tracker US




**Source: IAPP**

# State Data Privacy Law Tracker US

| | Legislation Name | Type | Commencement |
|---|---|---|---|
| US Legislation | California Privacy Rights Act (CPRA) | US state law | January 1, 2023 |
| | Virginia Consumer Data Protection Act (VCDPA) | US state law | January 1, 2023 |
| | Colorado Privacy Act (CPA) | US state law | July 1, 2023 |
| | Connecticut Data Privacy Act (CTDPA) | US state law | July 1, 2023 |
| | Utah Consumer Privacy Act (UCPA) | US state law | December 31, 2023 |
| | Delaware Personal Data Privacy Act (DPDPA) | US state law | Jan 1, 2025 |
| | Indiana Consumer Data Protection Act (ICDPA) | US state law | January 1, 2026 |
| | Iowa Consumer Data Protection Act (ICDPA) | US state law | January 1, 2025 |
| | Montana Consumer Data Privacy Act (MCDPA) | US state law | October 1, 2024 |
| | Oregon Consumer Privacy Act (OCPA) | US state law | July 1, 2024 |
| | Tennessee Information Protection Act (TIPA) – NIST* | US state law | July 1, 2025 |
| | Texas Data Privacy and Security Act (TDPSA) | US state law | July 1, 2024 |

# Data Privacy Law Tracker - Canada

| | Legislation Name | Type | Commencement |
|---|---|---|---|
| Canadian Legislation | Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) – CPPA* | Canadian federal law | April 13, 2000 |
| | Personal Information Protection Act Alberta (PIPA Alberta) | Canadian provincial law | January 1, 2004 |
| | Personal Information Protection Act British Columbia (PIPA BC) | Canadian provincial law | January 1, 2004 |
| | Quebec's Protection of Personal Information in the Private Sector Act (Private Sector Act) and Protection of Personal Information in the Public Sector Act (Public Sector Act) are both amended by the Privacy Legislation Modernisation Act (Law 25) | Canadian provincial law | September 22, 2022 (Law 25 commences in stages) |

# Summary Snapshot

| Consumer Right | PIPEDA | CCPA | CPRA | CDPA | GDPR | CPA |
|---|---|---|---|---|---|---|
| Right to access | × | ✓ | ✓ | ✓ | ✓ | ✓ |
| Right to confirm personal data is being processed | × | Implied | Implied | ✓ | ✓ | ✓ |
| Right to data portability | × | ✓ | ✓ | ✓ | ✓ | ✓ |
| Right to delete ~ | × | ✓ | ✓ | ✓ | ✓ | ✓ |
| Right to correct inaccuracies/right of rectification | × | × | ✓ | ✓ | ✓ | ✓ |
| Notice and transparency requirements | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Right to opt-out of sales | ✓* | ✓***** | ✓***** | ✓**** | ✓** | ✓***** |
| Right to opt-out of targeted advertising (CO and VA) / cross-context behavioral advertising sharing (CA) | × | ×*** | ✓ | ✓ | ✓ | ✓ |
| Right to object to or opt-out of automated decision-making ~ ~ | × | × | ✓ | ✓ | ✓ | ✓ |
| Opt-in or opt-out for processing of "sensitive" personal data? – "sensitive is defined differently under CPRA, CDPA and CPA | × | × | Opt-out† | Opt-in | Opt-in†† | Opt-in† |
| Right to object to/restrict processing generally | × | × | × | × | ✓ | × |
| Right to non-discrimination | × | ✓ | ✓ | Limited | Implied | Limited |
| Purpose / Use / Retention Limitations | × | Implied | ✓ | ✓ | ✓ | ✓ |
| Applies to both consumers and in HR and B-to-B contacts | × | + | ++ | × | ✓ | × |
| Privacy and security impact assessments sometimes required | × | × | ✓ | ✓ | ✓ | ✓ |
| Obligation to maintain reasonable security | × | ✓ | ✓ | ✓ | ✓ | ✓ |

Grade Ace

# US & Canadian Privacy Requirements: Definition of Personal Information

| | Legislation | Definition of personal information |
|---|---|---|
| US Legislation | CPRA | Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household |
| | VCDPA | Any information that is linked or reasonably linkable to an identified or identifiable natural person |
| | CPA | Materially similar to VCDPA<br><br>Information that is linked or reasonably linkable to an identified or identifiable individual |
| | CTDPA | Identical to CPA |
| | UCPA | Identical to CPA |
| Canadian Legislation | PIPEDA | Information about an identifiable individual |
| | PIPA Alberta | Identical to PIPEDA |
| | PIPA BC | Information about an identifiable individual and includes employee personal information but does not include contact information or work product information |
| | Law 25 | Any information which relates to a natural person and allows that person to be identified |

# US & Canadian Privacy Requirements: Definition of Sensitive Information

| | Legislation | Definition of sensitive information |
|---|---|---|
| US Legislation | CPRA | Personal information revealing government-issued identifiers, finances, geolocation, race, religion, union membership, communications, genetics, biometrics, health, and sexual orientation |
| | VCDPA | Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health, sexual orientation, or citizenship or immigration status; processing of genetic or biometric data for the purpose of uniquely identifying a natural person; personal data from a known child; or specific geolocation data |
| | CPA | Largely similar to VCDPA, with the exclusion of geolocation data<br><br>Personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status; genetic or biometric data that may be processed for the purpose of uniquely identifying an individual; or personal data from a known child |
| | CTDPA | Materially similar to VCDPA<br><br>Personal data that includes data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation or citizenship or immigration status; the processing of genetic or biometric data for the purpose of uniquely identifying an individual; personal data collected from a known child; or precise geolocation data |
| | UCPA | Similar to VCDPA, but with an exception to what constitutes sensitive information<br>Personal data that reveals an individual's racial or ethnic origin; an individual's religious beliefs; an individual's sexual orientation; an individual's citizenship or immigration status; or information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional; the processing of genetic personal data or biometric data, if the processing is for the purpose of identifying a specific individual; or specific geolocation data.<br>It does not include personal data that reveals an individual's racial or ethnic origin, if the personal data are processed by a video communication |
| Canadian Legislation | PIPEDA | Not specifically defined but the sensitivity of some types of data has been recognised in case law and by the Office of the Privacy Commissioner. For example, medical information, health, biometric information (in most cases), Health and financial data, ethnic and racial origins, political opinions, genetic and biometric data, an individual's sex life or sexual orientation, and religious/philosophical beliefs ( are all generally sensitive) |
| | PIPA Alberta | No definition |
| | PIPA BC | No definition |
| | Law 25 | Information that entails a high level of reasonable expectation of privacy |

# US & Canadian Privacy Requirements: Definition of Sensitive Information

| | | Racial or ethnic origin | Religious Beliefs | Union Membership | Health Data | Sexual Orientation | Citizenship Status | Genetic or Biometric Information | Children's Data | Geolocation | Government ID | Facial Information | Private Communication |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| US Legislation | CPRA | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | X | ✓ | ✓ | ✓ | ✓ |
| | VCDPA | ✓ | ✓ | X | ✓ | ✓ | ✓ | X | ✓ | ✓ | X | X | X |
| | CPA | ✓ | ✓ | X | ✓ | ✓ | ✓ | ✓ | ✓ | X | X | X | X |
| | CTDPA | ✓ | ✓ | X | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | X | X | X |
| | UCPA | ✓ | ✓ | X | ✓ | ✓ | ✓ | ✓ | X | ✓ | X | X | X |

# US & Canadian Privacy Requirements: Processing Requirements

| | Legislation | Processing requirements / principles |
|---|---|---|
| US Legislation | CPRA | (i) Identifying Purposes<br>(ii) Limiting Use, Disclosure, and Retention<br>(iii) Limiting Collection<br>(iv) Safeguards<br>(v) Transparency<br>(vi) Consent (in certain circumstances) |
| | VCDPA | Identical to CPRA |
| | CPA | Identical to CPRA |
| | CTDPA | Identical to CPRA |
| | UCPA | Identical to CPRA |
| Canadian Legislation | PIPEDA | Identical to CPRA, but it additionally requires (vii) accountability, (viii) accuracy, (ix) individual access, and (x) challenging compliance |
| | PIPA Alberta | Identical to PIPEDA |
| | PIPA BC | Identical to PIPEDA |
| | Law 25 | Identical to PIPEDA. However, the principle of openness and challenging compliance have not been included. It should be noted that express consent and more safeguards are required when processing sensitive data. |

Grade Ace

# US & Canadian Privacy Requirements: Individual Rights

| | USA | | | | | CANADA | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Consumer Rights** | CPRA | VCDPA | CPA | CTCPA | UTCPA | PIPEDA | PIPA Alberta | PIPA BC | Law 25 |
| Right to know/ information | ✓ | ✓ | ✓ | ✓ | ✓ | X | ✓ | ✓ | ✓ |
| Right to access | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Right to rectify | ✓ | ✓ | ✓ | ✓ | X | ✓ | ✓ | ✓ | ✓ |
| Right to delete | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Right to data portability | ✓ | ✓ | ✓ | ✓ | ✓ | X | X | X | ✓ |
| Right to appeal | X | ✓ | ✓ | ✓ | X | X | X | X | X |
| Right to reject ADM and profiling | ✓ | ✓ | ✓ | ✓ | ✓ | X | X | X | ✓ |
| Right not to be discriminated | ✓ | ✓ | ✓ | ✓ | ✓ | X | X | X | X |

# US & Canadian Privacy Requirements: DPIAs and PIAs

| | Legislation | Definition of personal information |
|---|---|---|
| US Legislation | CPRA | DPIAs are required when there is a “significant risk” to consumers |
| | VCDPA | DPIAs are required when a processing activity poses a “heightened risk of harm” to consumers |
| | CPA | Identical to VCDPA |
| | CTDPA | Identical to VCDPA |
| | UCPA | DPIAs are not required |
| Canadian Legislation | PIPEDA | Data Privacy Impact Assessments are not defined or required; however, organisations may complete them to fulfil their requirements under the Fair Information Principles. OPC guidance recommends performing PIAs prior to introducing or materially changing products, services or information systems. |
| | PIPA Alberta | Identical to PIPEDA |
| | PIPA BC | Identical to PIPEDA |
| | Law 25 | As of September 2023, PIAs will be required when:<br>(i) Upgrading, acquiring, or developing the firm’s IT systems or digital products;<br>(ii) Transferring covered data outside Quebec; and<br>(iii) Disclosing covered data in connection with research purposes and without the individual’s consent. |

Grade Ace

# Requirements towards PIA/ Risk assessments

| | USA | | | | | CANADA | | | |
|---|---|---|---|---|---|---|---|---|---|
| | CALIFORNIA | VIRGINIA | COLORADO | CONNECTICUT | UTAH | PIPEDA | ALBERTA | BRITISH COLUMBIA | QUEBEC |
| **PIAs** | CPRA | VCDPA | CPA | CTCPA | UTCPA | | PIPA Alberta | PIPA BC | Law 25 |
| **Are PIAs required?** | Regular risk assessment | ✓ | | | X | X | X | X* | ✓ |
| | | | | | | | | | |
| **What information is required?** | | | | | | | | | |
| Context of the processing | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ |
| Benefits of the processing | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ |
| Potential risks to data subjects | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ |
| Safeguards to mitigate the risks | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ |
| | | | | | | | | | |

*In Canada (aside from Quebec) PIAs are not mandatory but strongly endorsed by the Privacy Commissionaires (X)

# US & Canadian Privacy Requirements: Cybersecurity

| | Legislation | Security requirements |
|---|---|---|
| US Legislation | CPRA | Organisations must:<br>• Provide reasonable cybersecurity safeguards to all categories of personal information<br>• Conduct annual cybersecurity audits and make regulatory filings of risk assessments if the presents a significant risk to consumers' privacy or security<br>• Require contractual clauses and other safeguards to address supply chain security and privacy risks when they transfer, share or otherwise disclose personal information to their vendors and other third parties |
| | VCDPA | Data controllers must establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue |
| | CPA | Identical to VCDPA |
| | CTDPA | Identical to VCDPA |
| | UCPA | Materially similar to VCDPA<br>A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices designed to:<br>• protect the confidentiality and integrity of personal data; and<br>• reduce reasonably foreseeable risks of harm to consumers relating to the processing personal data.<br>Considering the controller's business size, scope, and type, a controller shall use data security practices that are appropriate for the volume and nature of the personal data at issue |
| Canadian Legislation | PIPEDA | No particular security safeguards are specified. However, the Fair Information Principle 7 requires organisations to protect personal information in a manner that is appropriate given its degree of sensitivity. OPC guidance suggestions to fulfil this principle include: technological tools (i.e., encryption), physical measures (i.e., locked filing cabinets), and organisational controls (i.e., limit who has access) |
| | PIPA Alberta | No mention of specific security safeguards. It is only stated that an organisation must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorised access, collection, use, disclosure, copying, modification, disposal or destruction |
| | PIPA BC | Materially similar to PIPA Alberta; however, it also recognises making reasonable security arrangements against additional risks that are similar to those listed in the legislation |
| | Law 25 | No mention of specific security safeguards. However, it is acknowledged that fines may be imposed for failing to implement the security measures necessary to protect personal information |

# DPIA Legal Requirements - US

Grade Ace

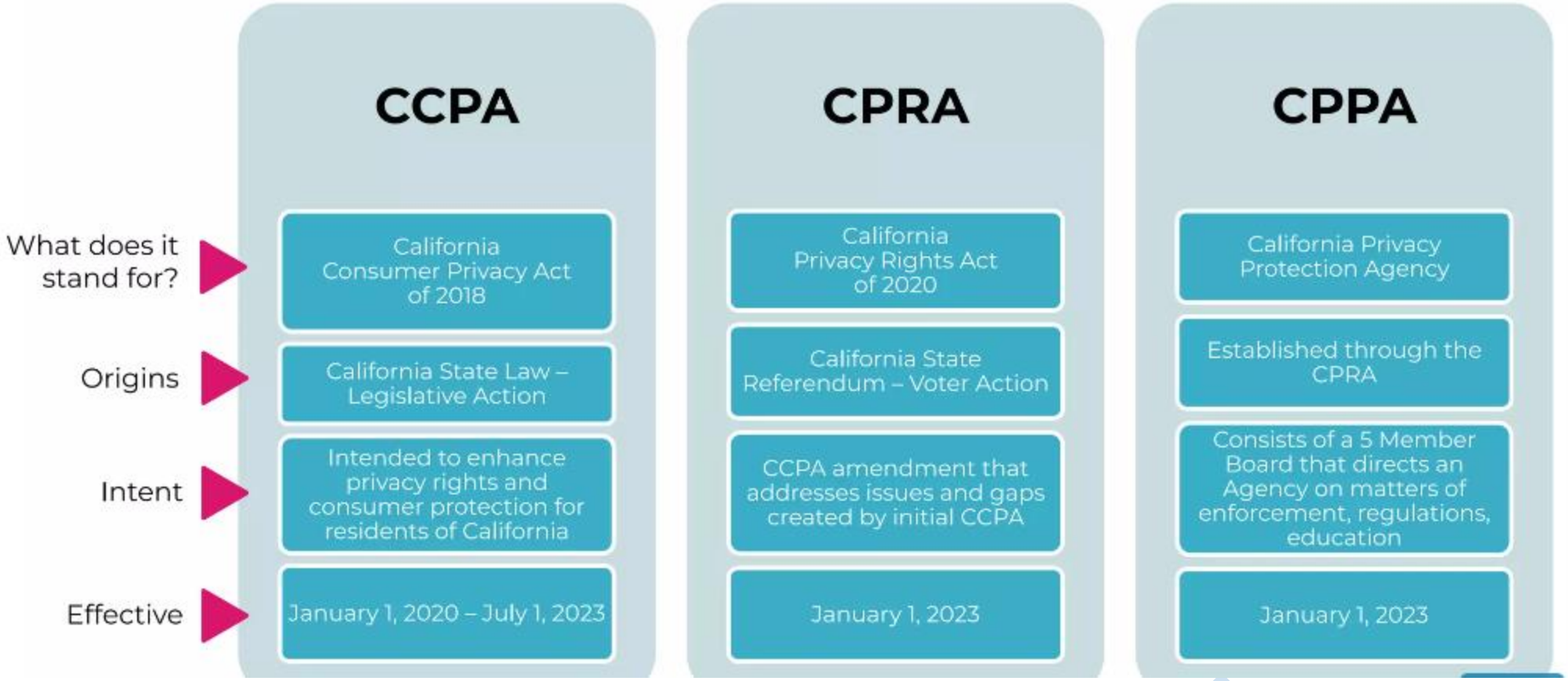
| Factors Required in a DPIA | CPRA | Colorado CPA 2023 | Conn. CTDPA'23 | Virginia VCDPA'23 |
|---|---|---|---|---|
| Explain benefits from processing. The DPIA should identify and weigh the benefits that may flow, directly or indirectly, from the proposed processing to either the organization, the data subject, other stakeholders, or the public. | CPRA does not directly require that companies create a DPIA, it empowers the CPPA to issue regulations that might require companies to submit to the agency a risk assessment with respect to certain forms of processing activities | ✓ | ✓ | ✓ |
| Explain risks from processing. The DPIA should identify and weigh the potential risks to the rights of the consumer associated with the proposed processing. | | ✓ | ✓ | ✓ |
| Describe risk mitigations taken. The DPIA should describe any safeguards that the organization has taken to mitigate potential risks. | | ✓ | ✓ | ✓ |
| Use of de-identification. To the extent that de-identification strategies have been utilized to mitigate risks, those strategies should be indicated. | | ✓ | ✓ | ✓ |

# DPIA Legal Requirements – US

Grade Ace

| Factors Required in a DPIA | CPRA | Colorado CPA 2023 | Conn. CTDPA'23 | Virginia VCDPA'23 |
|---|---|---|---|---|
| Reasonable expectations of data subject. The DPIA should consider whether the proposed processing aligns with the reasonable expectations of data subjects. | | ✓ | ✓ | ✓ |
| Compliance with other aspects of state privacy law. The DPIA should consider whether the processing complies with other requirements imposed upon controllers under the state privacy laws. | | ✓ | ✓ | Attorney General can evaluate the DPIA for compliance with all requirements within §59.1-574 |

# CCPA, CPRA, and CPPA Overview



**How is a 'business' defined?**

The CPRA defines a "business" as:

- a for-profit legal entity:
  - that collects consumers' personal information on its own or by others on its behalf
  - that alone or jointly with others determines the purposes and means of the processing
  - that "does business" in California
  - and satisfies at least one of the following thresholds:

    i. has annual gross revenues in excess of $25 million

    ii. annually buys, receives, sells, or shares the personal information of 50,000 or more consumers, households, or devices

    iii.derives 50% or more of its annual revenues from selling consumers' personal information

**What does 'sharing' personal information mean?**

The CPRA defines "sharing" as renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.

# Obligations

**What are the principal obligations of a contractor?**

A contractor must:

- use personal information only to perform services on behalf of a business as specified in a contract
- comply with the terms of the contract
- implement security safeguards
- not combine personal information received from a given business with any personal information received from others
- notify the business regarding their use of subcontractors, and those subcontractors must be contractually bound to the same terms as the contractors.

**What rights do consumers have?**

The CCPA creates six specific rights for consumers:

1. the **right to know** (request disclosure of) personal information collected by the business about the consumer, from whom it was collected, why it was collected, and, if sold, to whom;

2. the **right to delete** personal information collected from the consumer;

3. the **right to opt-out** of the sale of personal information (if applicable);

4. the **right to opt-in** to the sale of personal information of consumers under the age of 16 (if applicable);

5. the **right to non-discriminatory treatment** for exercising any rights; and

6. the **right to initiate a private cause of action** for data breaches.

The CPRA creates two additional rights:

7. the **right to correct** inaccurate personal information; and

8. the **right to limit use and disclosure** of sensitive personal information.

**What are the consequences for non-compliance?**

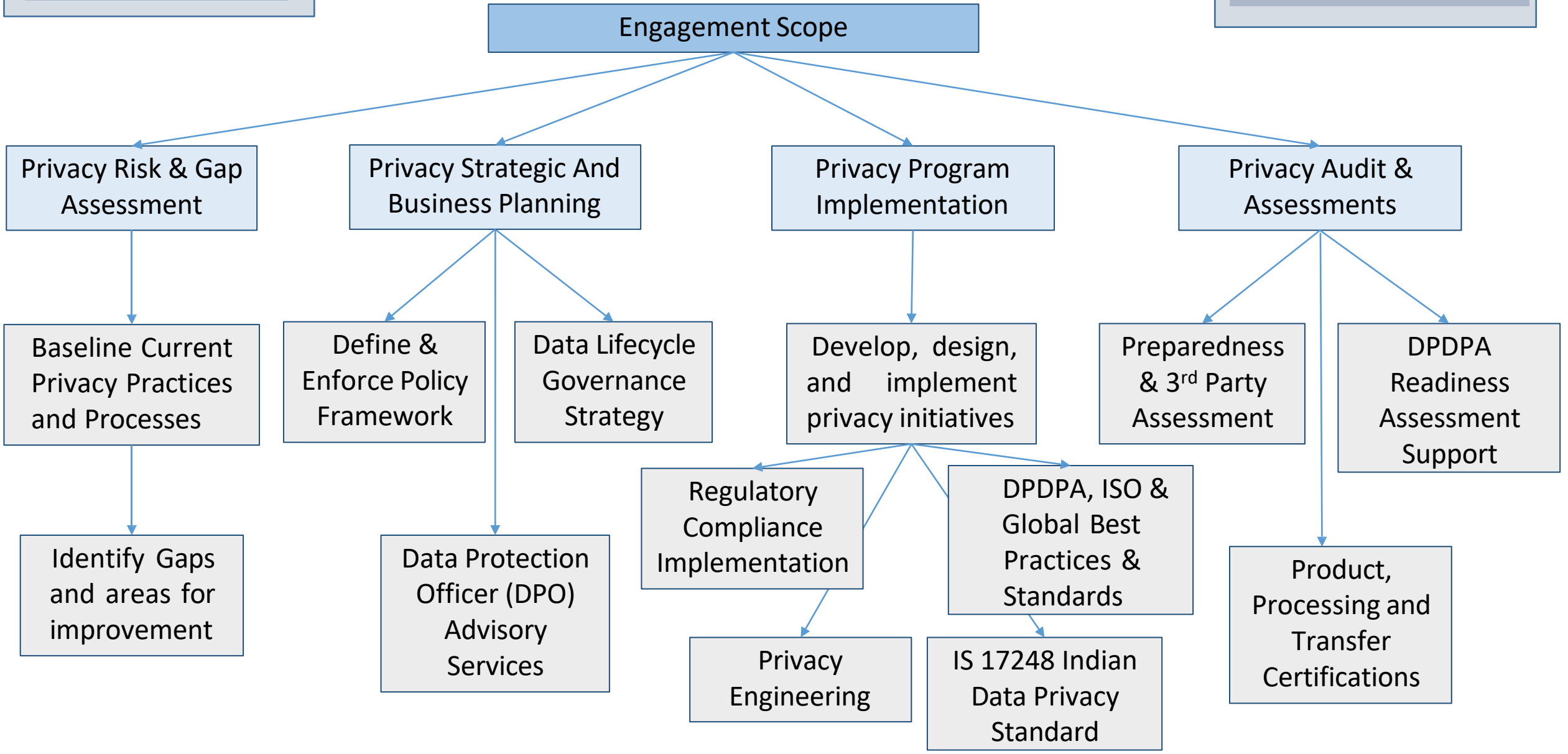
The CCPA provides for the following options for imposing liability in the event of non-compliance:

- Civil Penalties – In actions by the California Attorney General, businesses can face penalties of up to $7,500 per intentional violation or $2,500 per unintentional violation (but there is an opportunity to cure any alleged violation within 30 days after receiving notice of the alleged violation).
- Damages – In actions brought by consumers for security breach violations, consumers may recover statutory damages not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater. In actions for statutory damages, consumers must first provide businesses with written notice and an opportunity to cure.
- Non-Monetary Relief – In actions brought by consumers for security breach violations, consumers may seek injunctive or declaratory relief, as well as any other relief the court deems proper.
- Businesses may also be subject to an injunction in actions brought by the Attorney General.

# Privacy - Data Protection Offerings

**The Perspective™**

**Grade Ace™ Pvt Ltd**



Grade Ace

# Thank You

Rahul Sharma
Founder Director- Grade Ace
ThePerspective.Rahul@protonmail.ch
9711156157

Linkedin: https://www.linkedin.com/in/rahulsharma86/

Twitter: @wisdom_stoic