# Canadian Federal Privacy Law Reform:
## Initial Comments and Insights on the Proposed New Private Sector Privacy Statute - the *Consumer Protection Privacy Act*

**Adam Kardash**
Chair, Privacy and Data Management
Osler, Hoskin & Harcourt LLP
National Lead, AccessPrivacy

OSLER

# Background – Key Features of New Privacy Legislative Reform Proposal

Bill C-11, referred to as the *Digital Charter Implementation Act, 2020*, proposes to enact The *Consumer Privacy Protection Act* ("CPPA") and *Personal Information and Data Protection Tribunal Act.*("DPTA").

The CPPA would replace the privacy regime under the privacy provisions under *Personal Information Protection and Electronic Documents Act* ("PIPEDA").

The DPTA would establish a new Personal Information and Data Protection Tribunal (Tribunal).

Similar to PIPEDA, the CPPA's proposed statutory framework is largely grounded within the following key features:

- a balancing of the interests of individuals and organizations;
- rules generally drafted in principles-based, technologically neutral fashion; and
- an accountability model.

Compared to Bill 64 (Quebec's proposed reform to its private sector privacy law), the CPPA's rules are far less prescriptive, less stringent, less onerous, and considerably more flexible, proportionate and—critically—appear generally interoperable with Canadian provincial private sector privacy laws and foreign privacy regimes (including the GDPR).

# Background – Key Features of New Privacy Legislative Reform Proposal

**Key new features of the CPPA**

- An enforcement regime with potentially severe financial penalties, a private right of action, order making power for the Privacy Commissioner of Canada.
  - The Tribunal (not the Commissioner) would have the ability to impose penalties.
  - Inclusion of rights of appeal, procedural fairness provisions.
- A re-enforcement of consent (especially express consent) as the primary authority for organizations to process personal information, and more prescriptive consent requirements.
- Clarifications and additional "exceptions to consent" authorities for use and disclosures of personal information, including for standard business practices.
- Provisions relating to "de-identified" data.
- Strengthened and more prescriptive accountability requirements.
- Clarification of the obligations of service providers.
- Statutory recognition of "codes of practice" and certification programs.
- New statutory rights (right of disposal, data mobility rights).
- Provisions for automated decision making systems.

# Background – Key Features of New Privacy Legislative Reform Proposal - Continued

## Status of Bill C-11

- Bill is at first reading, and no announcement yet of public consultation or hearing process.
- CPPA silent on transitional period for compliance, after statute comes into force.

# New Enforcement Regime - Monetary Penalties & Fines

- Maximum penalty of the ***higher of*** $10 million or 3% of gross global revenues. (s. 94(4))
  - Fines on conviction for indictable offence may be up to higher of $25 million or 5%. (s. 125(a))
- Penalties may only be imposed by Tribunal for certain contraventions (s. 93(1)), including:
  - collecting personal information beyond that which is necessary for purposes identified and recorded by an organization (s. 13)
  - using or disclosing personal information for a secondary purpose without consent (s. 14(1))
  - contravening the "refusal to deal" provision (s. 15(5))
  - obtaining consent through false or misleading information, or using deceptive practices (s. 16)
  - contravening the retention and disposal requirements (s. 53, and 55(1) and (3))
  - contravening the safeguarding requirements (s. 57(1))
  - failing to report breach of security safeguards (s. 58(1))
  - failing to notify affected individuals of breach of security safeguards (s. 58(3))
- Certain ***knowing*** contraventions may be prosecuted as offences in court (s. 125), including:
  - failing to report breach of security safeguards or notify affected individuals (s. 58)
  - failing to provide Commissioner with access to breach records (s. 60(1))
  - failing to retain personal information that is subject of personal information request (s. 69)
  - using de-identified information to identify an individual (s. 75)
  - retaliating against a whistleblower (s. 124)
  - obstructing an investigation, inquiry or audit (s. 125)

# New Enforcement Regime - Monetary Penalties

- Factors to be considered by Commissioner in making recommendation (s. 93(2)):
  - nature and scope of contravention
  - voluntary compensation
  - history of compliance
  - any other relevant factor
- Commissioner recommends penalties after inquiry; new Tribunal decides whether to impose. (s. 94(1))
  - In deciding, Tribunal may also consider ability to pay, effect of penalty on carrying on business and financial benefit obtained from contravention. (s. 94(5))
- Decision ***not* to recommend** monetary penalties may be appealed to Tribunal by complainant. (s. 100)

# New Enforcement Regime - Private Right of Action & Order-Making Powers

- Private right of action. (s. 106)
  - After a final finding of contravention or a conviction, affected individuals may sue for "**damages for loss or injury...suffered as a result**". (s. 106(1))
  - Claims may be brought in either Federal Court or provincial superior courts. (s. 106(4))
  - Two-year limitation period running from final finding or conviction. (s. 106(3))
- Order-making powers
  - Following an inquiry, Commissioner may **order an organization to comply and to publicize corrective measures.** (s. 92(2))
  - During an investigation, inquiry or audit, Commissioner may make any **interim order** considered appropriate (s. 98(1)(d)) and may make **information preservation orders.** (s. 98(1)(e))
  - Compliance orders **may be appealed** to Tribunal. (s. 100)
  - Interim orders may be appealed to Tribunal, but only with leave. (s. 101)

# New Enforcement Regime - Inquiries and Appeals

- Inquiries. (ss. 88, 89 and 90)
  - Inquiries may follow investigations or be conducted into suspected non-compliance with compliance agreements. (s. 88, s. 89)
  - Findings, compliance orders and recommendations for penalties made after an inquiry. (s. 92)
  - Inquiry must be **informal and expeditious**, subject to **fairness and natural justice**; rules of evidence do not bind Commissioner. (s. 90(1))
  - Both organization and complainant entitled to **opportunity to be heard**. (s. 90(3))
  - Commissioner may define inquiry procedure, which must be made public. (s. 91)
  - Inquiry to be completed **within 1 year of complaint**, subject to single 1 year extension. (s. 92(4))
- Appeals to Personal Information and Data Protection Tribunal
  - Findings and orders made after an inquiry may be appealed to new Tribunal. (s. 100)
  - Tribunal's standard of review of Commissioner's decision is same as appellate court. (s. 102(2))
  - Tribunal may award costs. (DPTA, s. 20)

# Balancing of interests – Adjustments

- The preamble provision to the CPPA—which informs the interpretation of the statutory requirements under the statute—has been adjusted with an emphasis on the "protection of personal information" as follows (comparison relative to the preamble to PIPEDA):
  - The purpose of this ~~Part~~Act is to establish~~,~~ — in an era in which ~~technology increasingly facilitates~~data is constantly flowing across borders and geographical boundaries and significant economic activity relies on the analysis, circulation and exchange of personal information~~,~~ — rules to govern the ~~collection, use and disclosure~~ protection of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.
- CPPA (Section 12(1) restates includes the overarching "reasonable and appropriate" provision whereby organization may only:

  "collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances" (Currently, s. 5(3) of PIPEDA)

# Reasonable & Appropriate Provisions

- Mandatory factors to consider under subsection 12(2) in determining whether purposes are appropriate include:

  (a) the **sensitivity** of the personal information;

  (b) whether the purposes represent **legitimate business needs** of the organization;

  (c) the **effectiveness** of the collection, use or disclosure in meeting the organization's legitimate business needs;

  (d) whether there are **less intrusive means** of achieving those purposes at a **comparable cost** and with **comparable benefits**; and

  (e) whether the individual's **loss of privacy** is **proportionate to the benefits** in light of any measures, technical or otherwise, implemented by the organization to mitigate **the impacts of the loss of privacy** on the individual.

- These sections codify principles set out in *Eastmond v. Canadian Pacific Railway*, 2004 FC 852 (CanLII), affirmed by the Federal Court of Appeal) in *Turner v. Telus Communications Inc* (2005 FC 1601), and have long been used by the OPC as elements of the test for determining the "reasonability" and appropriateness of the purposes of a given collection, use and disclosure.

# Purpose Identification and Data Minimization

- Organizations must **identify** and **record** the purposes associated with personal information that they collect, used or disclose **at or before the time of collection**, or before using or disclosing for a new purpose. (s. 12(3) and (4))
- The "appropriate provisions" flow to the CPPA's "limitation of collection" requirement, as organizations may only collect the personal information **that is necessary** for the determined and recorded purposes. (s. 13)
  - The concept of "necessary" has been interpreted as akin to "required", and a higher standard than "mere reasonableness"
  - Operationalizing this principle within complex data ecosystems, AI contexts, etc. may prove very challenging
- If an organization contravenes the limitation of collection requirements at s. 13, penalties may be imposed by the Tribunal and the organization could be liable for a fine of up to the higher of $10 million or 3% of gross global revenues. (s.94(4))

# Accountability Provisions

The CPPA sets out provisions that clarify the concept of an "accountable organization" and several provisions relating to "demonstrable" accountability.

- Background - Similar to PIPEDA, CPPA provides that organizations are "accountable" for personal information under its control.
- CPPA clarifies that personal information is under the control of an organization (i.e. the accountable organization) that **decides to collect it and that determines the purposes** for its collection, use or disclosure, regardless of whether the information is collected, used or disclosed by the organization itself" or by a service provider. (s. 7(2))

# Accountability Provisions

- CPPA requires organizations to implement a **privacy management program**, which must:
  - include **policies, practices and procedures** that are put in place to fulfil the organization's obligations under the Act (s. 9(1)), and
  - **take into account the volume and sensitivity** of personal information under the organization's control. (s. 9(2))
    - Appears to codify joint OPC, PIPA BC and PIPA Alberta 2012 guidance - *Getting Accountability Right with a Privacy Management Program.*
- Upon request of the Commissioner (i.e. no reasonable grounds necessary), organizations are required to **provide the Commissioner with access to their policies, practices and procedures** that are included in its privacy management program. (s. 10)
  - The Commissioner cannot use policies, practice and procedures obtained via Section 10 to initiate a complaint or audit. (s. 110)

# Service Providers - Concept Clarifications

CPPA clarifies that the concept of a "service provider" and the scope of statutory requirements imposed on service providers.

- A "service provider" is "an organization … that provides services for or on behalf of another organization to assist the other organization in fulfilling its purposes." (s. 2)
- The definition is non-exhaustive and includes a parent corporation, subsidiary, affiliate, contractor or subcontractor providing such services for or on behalf of another organization. (s.2)
- An organization that would fall outside the scope of a service provider concept if it
  - collects, uses or discloses personal information other than for "any purpose other than the purposes for which the information was transferred" by an accountable organization, (s. 11 (2)) or
  - determines the purposes for its collection, use or, disclosure. (s. 7 (2))

# Service Providers - Concept Clarifications

**Scope of Statutory Requirements**

- Service providers must
  - comply with statutory safeguarding requirements (s. 57); and
  - notify an accountable organization about a breach of security safeguards involving personal information under the organization's control as soon as feasible in the event of a security breach. (s. 61)
- Service providers are expressly not subject to the CPPA's provisions relating to accountability, consent, retention, accuracy, rights of access, transparency, data portability and and other Part 1 requirements in respect of personal information that is transferred to it under the control of the "accountable organization". (s. 11(2))
- However, a service provider that collects, uses or discloses personal information for any other purpose would effectively be deemed an "accountable entity" and would be subject to Part 1. (s. 11(2))

**Service Providers and Consent**

- CPPA clarifies that organizations may transfer an individual's personal information to a service provider without the consent to whom the personal information relates. (s. 19)

# Service Provider - Concept Clarifications

Service Providers and Disposal of Personal Information

- Where an accountable organization disposes (permanently and irreversible deletes) personal information, it must, as soon as feasible, inform any service provider to which it has transferred the information of the individual's request and obtain a confirmation from the service provider that the information has been disposed of. (s. 55(3))

# Accountability Frameworks – Codes of Practice and Certifications

CPPA provides statutory recognition of **codes of practice** and related **certification programs**.

- Allows for the establishment of voluntary accountability frameworks that may be very helpful for personal information processing in complex data ecosystems, sectoral information sharing arrangements, AI and other complex analytics, business models, etc.
- Codes of practice need to provide for "**substantially the same or greater protection of personal information as some or all of the protection provided**" under the Act. (s. 76(2))
- **Criteria for codes and certification programs** to be set out in regulations. (s. 76(3))
- Organizations would **apply to the Commissioner for approval** of a code or program, and Commissioner has to make public his/her decision. (s. 76(2) and 79)
- Compliance with a code does **not relieve an organization of its obligations under the Act**. (s. 80)
- Certification programs run by entities will include **independent verification mechanisms** and **disciplinary measures** for non-compliance with the code. (s. 77(1)(d) and (e))

# Accountability Frameworks – Codes of Practice and Certifications - Continued

- The Commissioner's powers include:
  - Cooperating with an entity that operates a program for the exercise of the Commissioner's powers and duties. (s. 81(b))
  - **Revoking an approval.** (s.81(e))
  - **Discretionary power to decline to investigate a complaint** when it "raises an issue in respect of which a certification program that was approved by the Commissioner… applies and the organization is certified under that program." ( s. 83(1)(d))
- Commissioner **cannot** recommend a penalty if an organization is in compliance with an approved code or certification program (s. 93(3)), **BUT** the **private right of action** would still be available (s. 106) for this contravention.

# De-Identification

CPPA includes several technical provisions involving the process of de-identification of personal information, and the use and disclosure of de-identified data.

- The term "**de-identify"** is defined in the statute as a:

  > "means to **modify** personal information — **or create** information from personal information — **by using technical processes** to ensure that the information **does not identify** an individual or could not be used in **reasonably foreseeable circumstances**, alone or in combination with other information, **to identify an individual**." (s. 2)

- Based on wording in definition and the use of the term in other provisions:
  - Concept of "de-identified data" appears generally consistent with the definition of that term proposed by the Canadian Anonymization Network (CANON), but it is unclear whether sufficiently "de-identified" data is still "personal information" for the purposes of the CPPA.
  - The scope of the CPPA (s. 6(1)) contemplates rules protecting "personal information", but in certain circumstances, the statute regulates the use or disclosure of "de-identified" data (i.e. not PI).

# De-Identification

**Requirements for De-Identification Process:**

- In the course of the de-identification process, organizations are obligated to ensure that any **technical and administrative measures** applied to the information are **proportionate to the purpose** for which the information is de-identified **and the sensitivity** of the personal information. (s.74)

**Authorized Uses of De-identified Data:**

The CPPA incorporates the concept of "de-identifying" data as a condition in circumstances for organization to use or disclose personal information without consent. See:

- Exception to consent for use of personal information for research and Development. (s. 21)
- Exception to consent for disclosures for Prospective Business Transactions. (s. 22)
- Exception to consent for disclosures for Socially Beneficial Purposes. (s. 39)

**Key Issue**:

Data that is not "personal information" (i.e. "de-identified data") is not generally subject to the consent or any other requirements under the CPPA, and organizations would not need any exception to consent authority for the subsequent use or disclosure.

Unclear why data that is sufficiently "de-identified" (and is no longer "personal information") would even need to be included in the above exceptions to consent.

# De-Identification

**Authority to De-Identify:**

- The CPPA helpful clarifies that organizations are legally authorized under the statute to de-identify data without obtaining the consent of the individual to whom the personal information relates. (s. 20)

**Prohibitions on Re-identification:**

- Very broad prohibition under CPPA from using de-identified information - alone or in combination with other information - to identify an individual, except in order to conduct testing of the effectiveness of security safeguards that the organization has put in place to protect the information. (s. 75)
  - Additional carve-outs to prohibition required to address the array of circumstances where re-identification is wholly legitimate and appropriate
- *Knowingly* using de-identified information in contravention of s. 75 may be prosecuted as an offence in court and the organization could be liable for a fine of up to the higher of $25 million or 5% of gross global revenues. (s.125)

# Authority to Process Personal Information - Consent

Under the CPPA (and similar to PIPEDA), organizations may not collect, use or disclose personal information without a legal authority set out under the Act. (s 15(1))

Two classes of legal authorities for processing: (i) consent or (ii) an exception to consent. Key new features of the CPPA's consent authority for processing are as follows:

<u>Primacy of Consent as Authority for Processing</u>

Drafting suggests a **clear intention to re-enforce the primacy of consent** as the authority for processing of personal information (despite widespread acknowledgement of the increasing challenges faced by organizations obtaining valid consent in dynamic, constantly evolving data environment).

- Distinct from GDPR, where consent is just one of multiple lawful bases for processing of personal information

# Authority to Process Personal Information – Consent - Continued

## Form of Consent

The CPPA provides that express consent is the default form of consent. Specifically, when an organization relies on consent as an authority for processing, the organization **must generally obtain an express form of consent**. (s. 15(4))

An **implied form of consent** may only be relied upon if the **organization establishes that it is appropriate to rely on an individual's implied consent**, taking into account the reasonable expectations of the individual and the sensitivity of the personal information that is to be collected, used or disclosed. (s. 15(4))

# Authority to Process Personal Information - Consent

Valid Consent

The CPPA provides prescriptive information requirements for a valid consent.

The information must be **provided** in **plain language** at or before the time the individual seeks the consent.

The information must include the following content (which is more prescriptive than the definition of "valid consent" under Section 6.1 of PIPEDA):

(a) the **purposes for the collection, use or disclosure** of the personal information determined by the organization and recorded under the Act's "appropriate purposes" provisions (in 12(3) or (4));

(b) **the way in which the personal information is to be collected, used or disclosed**;

(c) any **reasonably foreseeable consequences** of the collection, use or disclosure of the personal information;

(d) the **specific type of personal information** that is to be collected, used or disclosed; and

(e) the **names of any third parties or types of third parties** to which the organization may disclose the personal information.

Requirements upon withdrawal of consent

- Upon receiving notice of withdrawal of consent from the individual, an organization must **inform the individual of the consequences of the withdrawal** of their consent, and **"as soon as feasible after that" cease the collection, use or disclosure** the applicable personal information. (Section 17(2))

If an organization contravenes the consent requirements in s. 14, s. 15(5) or s. 16 of the Act penalties may be imposed by the Tribunal and the organization could be liable for a fine of up to the higher of $10 million or 3% of gross global revenues. (s.94(4))

# Authority to Process - Exceptions to Consent for Standard Business Operations

CPPA helpfully clarifies and expands the circumstances where organizations may collect and/or use personal information without consent in the course of standard business operations.

- No consent required for organizations to **transfer personal information to their third party service providers**. (s.19)
- No consent required for the process of **de-identifying personal information**. (s. 20)
- No consent required for the collection and use (**but not disclosure**) of personal information for a broad range of standard "business activities" including an activity:
  - **i. necessary to provide or deliver a product or service** that the **individual has requested** from the organization
  - ii. carried out in the **exercise of due diligence to prevent or reduce the organization's commercial risk**;
  - **iii. necessary for the organization's information, system or network security**;
  - iv. necessary for the **safety of a product or service** that the organization provides or delivers;
  - v. in the course of which **obtaining the individual's consent would be impracticable** because the organization **does not have a direct relationship** with the individual; (s. 18(2))

  **provided that** in the course of any activity:
    - the collection or use is something a **reasonable person would expect**; and
    - the collection or use **is not used to influence the individual's behaviour or decisions**. (18(1))

# Exceptions to Consent – Business transactions

- Background:
  - PIPEDA contains a helpful (and widely used) exception to consent for parties to disclose personal information in connection with prospective and completed business transaction as long as certain requirements are met (including notice to impacted individuals upon completion of the transaction).
- CPPA contains a similar "business transaction" provision but it has been amended very restrictively to require that personal information be de-identified before it is used or disclosed in connection with a prospective transaction (and remain de-identified until the transaction is complete).

# Exceptions to Consent – Use and Disclosure for Research Purposes

The CPPA provides organizations with an exception to consent for the use of personal information for the broad concept of "internal research and development purposes", but only on the very **restrictive condition** that the i**nformation be "de-identified" prior to the use** for such purpose. (s. 21)

- Many wholly R&D activities that legitimately require the processing of personal information (including standard customer research, AI and other complex analytics) will fall outside the scope of this exception to consent authority.

The CPPA maintains (and clarifies a technical drafting issue in) PIPEDA's exception to consent for disclosure of personal information for "statistical purposes or scholarly study or research purposes**,** provided that:

- those purposes cannot be achieved without disclosing the information;
- it is impracticable to obtain consent; and
- the organization informs the commissioner before the disclosure. (s. 35)

# Exceptions to Consent – Disclosures for Socially Beneficial Purposes

The CPPA includes as a new exception for consent for disclosures for "socially beneficial purposes" (aka "Data for Good").

- Organization may disclose personal information without consent if the information is
  - **De-identified** before the disclosure;
  - Made to an **government institution, post-secondary institution, health institution, or library**; and
  - Made for a **socially beneficial purpose**
    - a purpose related to "health, the provision or improvement of public amenities or infrastructure, the protection of the environment" or purpose set out in regulations. (s. 39)
- Excludes "Data for Good" disclosures to private sector entities

# Exceptions to Consent – Collection and disclosure for fraud detection

- CPPA contains a new "fraud exception" that helpfully **clarifies a technical drafting issue** under PIPEDA's exception to consent for fraud detection and suppression.
  - PIPEDA provides an exception to the consent requirement for the **disclosure** of personal information to another organization where it is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud. However, PIPEDA does **not** contain an express corresponding exception to the consent requirement for the **collection** of personal information for these purposes.

- THe CPPA clarifies that the exception to consent applies to **both** the **disclosure and corresponding collection** of personal information for the purposes of detecting, suppressing or preventing fraud. (s. 27(2))

# Transparency

The CPPA requires organizations to make information that explains its policies and practices readily available in "**plain language**." (s. 62)

- PIPEDA required information to be available in a form that is "generally understandable."

The CPPA supplements PIPEDA's transparency requirements by setting out several new content requirements when organizations make such information available:

- A general account of **any automated decision systems** that could have **a significant impact** on individuals.
- **How the organization applies consent exceptions** to its practices.
- Whether or not the organization **transfers or discloses information internationally or interprovincially** that may have **reasonably foreseeable privacy implications**.
- How individuals may make **a request for the disposal** (permanent and irreversible deletion) of their information. (s. 62)

# Automated Decision Systems and Algorithmic Transparency

CPPA introduces requirements related to "automated decision system," defined as:

- "any technology that assists or replaces the judgement of human decision-makers using techniques such as **rules-based systems**, **regression analysis**, **predictive analytics**, **machine learning**, **deep learning** and **neural nets**." (s. 2)

New requirements include:

- Openness: Organizations must make available a **general account of the organization's use of any automated decision system** to make predictions, recommendations or decisions about individuals **that could have significant impacts** on them. (s. 62(2)(c))
- Access: With respect to access to personal information, organizations have an explicit obligation to, **upon request**, **provide individuals with an explanation of any prediction, recommendation or decision made by an automated decision system**, and of **how the personal information that was used** to make the prediction, recommendation or decision was obtained. This information must be provided in **plain language**. (s. 63(3) and 66(1))

There is no express right to object to automated decisions.

# Breaches of Security Safeguards

- The CPPA contains a similar mandatory breach notification requirement (s. 58) as under PIPEDA.
- The CPPA clarifies that **service providers** are required to notify the **organization that controls the personal information** of a breach of security safeguards. (s. 61)
- The **content requirements** for the report to the Commissioner and notice to affected individuals have not yet been prescribed.
- If an organization contravenes the breach notification requirements at s. 58, or the safeguarding requirements as s. 57(1), penalties may be imposed by the Tribunal and the organization could be liable for a fine of up to the higher of $10 million or 3% of gross global revenues. (s. 94(4))
- If an organization *knowingly* contravenes the breach notification requirements at s. 58 or breach recording requirements at s.60(1), the contravention may be prosecuted as an offence in court and the organization could be liable for a fine of up to the higher of $25 million or 5% of gross global revenues. (s.125)

# Right of Disposal of Personal Information

- The CPPA provides a new statutory right of disposal of personal information.
  - Specifically, **upon request of an individual, an organization must dispose** of that individual's personal information. (s. 55 (1))
- Key requirements/features of the right of disposal include the following:
  - The standard for a valid "disposal" of personal is very high, as the disposal must result in the "**permanent and irreversible deletion** of personal information". (s. 2)
  - Based on wording, the right of disposal is **not restricted to just personal information "online**".
  - The **disposal must take place "as soon as feasible"** after the request.
  - **Must inform any service provide**r as soon as feasible about the individual's request, and obtain a confirmation of the individual's request from the service provider. (s. 55(3))

# Right of Disposal of Personal Information - Continued

  - **No requirement to dispose in certain circumstances** - where the information would result in the disposal of personal information about another individual and the information is not severable, or there are legislative requirements or reasonable terms of a contract that prevent it from doing so. (s. 55(1)).
- Where an organization refuses an individual's request, an organization must inform the individual in writing and set out the reasons and any recourse the individual may have to challenge compliance.
- If an organization contravenes the retention and disposal requirements at s. 53, or s. 55(1), or s. 55(3), penalties may be imposed by the Tribunal and the organization could be liable for a fine of up to the higher of $10 million or 3% of gross global revenues. (s.94(4))

# Right of Data Mobility

The CPPA introduces a concept of data mobility rights.

- Upon request of an individual, an organization must disclose the personal information that it has collected from the individual to an organization designated by the individual. (s. 72)

- Key requirements for data mobility rights include:
  - The data mobility disclosure must take place "**as soon as feasible**"
  - Both organizations must be subject to a "**data mobility framework"** provided under the **regulations** of the Act (s. 72)

# Data Mobility Frameworks

Key details about the **nature, scope and requirements of data mobility rights will be set out in regulations** that may include:

- data mobility frameworks that provide
  - **safeguards** to enable the secure disclosure and subsequent collection of the personal information (s. 120(a)), and
  - **parameters for the technical means for ensuring interoperability** in respect of the disclosure and collection of that information. (s. 120(a))

- requirements that **specify organizations that are subject to the data mobility framework** (s. 120 (b)), and

- requirements that provide for **exceptions to the data mobility disclosure requirement**, including exceptions related to the protection of proprietary or confidential commercial information. (s. 120(c))

# What's Next?

Stay current with AccessPrivacy:

- Sign up for **e-news blasts** for updates featuring **key developments involving the CPPA** and other Canadian privacy legislative reform.
- Register for our **complimentary Monthly Privacy Calls**:
  - Next call is Wednesday, November 25 with an in-depth analysis of key features of the CPPA
- Track developments and gain insight on Canadian privacy legislative reform by subscribing to the **AccessPrivacy Knowledge Portal.**

**Visit www.accessprivacy.com to find out more.**

Thank you for attending!