CANON Canadian Anonymization Network

The Hon. François-Philippe Champagne
Minister of Innovation, Science and Industry
Government of Canada
Francois-Philippe.Champagne@parl.gc.ca

December 7, 2022

Proposed amendments to the de-identification and anonymization provisions in the *Digital Charter Implementation Act, 2022* (Bill C-27)

Dear Minister Champagne,

On behalf of the Canadian Anonymization Network (CANON), we are pleased to provide proposed amendments to the de-identification and anonymization provisions in the *Digital Charter Implementation Act, 2022* (Bill C-27).

By way of background, CANON is a not-for-profit organization whose members consist of large data custodians from across the public, private, and health sectors. One of CANON's core publicly-stated objectives is to advocate for balanced legislative and policy standards for anonymization that enable innovative and beneficial uses of data, while reasonably protecting against foreseeable privacy risks.

In August 2022, CANON struck a Working Group to consider the provisions in Bill C-27 that relate to concepts of "de-identified" and "anonymized" data. For your consideration, the attached document consists of the Working Group's comments and proposed targeted amendments to the relevant definitions and associated provisions related to the concepts of "de-identified" and "anonymized" data in the draft legislation.

The attached document incorporates additional comments received from the broader CANON Steering Committee and reflects input from stakeholders across all sectors in connection with a consultation (which included a digital roundtable discussion with over 100 participants) that CANON commenced on October 3, 2022.

CANON appreciates the opportunity to provide our comments on Bill C-27, and we look forward to our continued dialogue on this critically important legislative reform initiative.

Yours sincerely,

Adam Kardash, on behalf of the Canadian Anonymization Network

December 7, 2022

CANON Canadian Anonymization Network

Proposed amendments to de-identification and anonymization provisions in the *Digital Charter Implementation Act, 2022* (Bill C-27)

The Canadian Anonymization Network (CANON) is a not-for-profit organization whose members comprise large data custodians from across the public, private, and health sectors. One of CANON's core publicly-stated objectives is to advocate for balanced legislative and policy standards for anonymization that enable innovative and beneficial uses of data, while reasonably protecting against foreseeable privacy risks.

In August 2022, CANON struck a Working Group[1] to review the Government of Canada's Bill C-27, which is currently in its second reading in the House of Commons. This document consists of the Working Group's proposed targeted amendments to the relevant definitions and associated provisions related to the concepts of "de-identified" and "anonymized" data in Bill C-27, and it incorporates additional comments received from the broader CANON Steering Committee and stakeholders across all sectors (including a foreign data protection authority) as part of a consultation that CANON commenced on October 3, 2022. This document also incorporates various comments received in the course of a workshop that CANON conducted on November 3, 2022, which was attended by over 100 participants.

CANON intends to submit a version of this document to the parliamentary committee that is ultimately struck to study Bill C-27 and will seek to appear as a witness.

***

Note: The balance of this document sets out each of the provisions in Bill C-27 that incorporates the concepts of "de-identified" and/or "anonymized" data. The text highlighted in green below reflects the amendments that have been proposed in Bill C-27 to the original text of the *Consumer Privacy Protection Act* (the "**CPPA**") as introduced in Bill C-11. The text in purple indicates CANON's suggested amendments to Bill C-27.

[1] **Adam Kardash**, Partner and Chair of the Privacy and Data Management Group at Osler, Hoskin & Harcourt LLP, National Lead of AccessPrivacy by Osler; **Suzanne Morin**, VP Enterprise Conduct, Data Ethics and Chief Privacy Officer at Sun Life; **Holly Shonaman**, Assistant General Counsel, Financial Crimes and Data Protection at RBC; **Lorraine Krugel**, Director, Privacy and Data at the Canadian Bankers Association; **Jordan Prokopy**, Partner and National Privacy Practice Leader at PwC Canada; **Faeron Trehearne,** Chief Legal Officer and Corporate Secretary at Moneris; **Sarah Nasrullah**, Legal Counsel (Privacy) at Bell; **Katelyn Smith**, Associate in the Privacy and Data Management Group at Osler, Hoskin & Harcourt LLP; **Catherine Hart**, Associate in the Privacy and Data Management Group at Osler, Hoskin & Harcourt LLP.

Part 1 – CPPA: Anonymization

Section 2(1)

anonymize means to irreversibly and permanently modify personal information, in accordance with generally accepted best practices, to ensure that no individual can be identified from the information, whether directly or indirectly, by any means. (*anonymiser*)

CANON Proposed Amendment:

anonymize means to irreversibly and permanently modify personal information, in accordance with generally accepted best practices, to ensure that there is no reasonably foreseeable risk in the circumstances that an individual can be identified from the information, whether directly or indirectly, by any means. (*anonymiser*)

CANON Comment:

The current definition of "anonymize" sets an extremely high and practically unworkable threshold for the circumstances in which information would no longer be deemed to be "identifiable". CANON's proposed amendment would align the CPPA's concept of "anonymized" data with the standard for anonymization within legislative schemes across Canadian jurisdictions, in particular Quebec's private sector privacy law (*Act respecting the protection of personal information in the private sector*, as amended by Bill 64, at s. 23 [in force September 2023]) and Ontario's health privacy law (*Personal Health Information Protection Act*, *2004* at s. 2 [definition of "de-identify" in English, corresponding to "anonymiser" in French] ("**PHIPA**")).

Quebec's private sector privacy law, as amended by Bill 64, provides:

> For the purposes of this Act, information concerning a natural person is anonymized if it is, at all times, reasonably foreseeable in the circumstances that it irreversibly no longer allows the person to be identified directly or indirectly. Information anonymized under this Act must be anonymized according to generally accepted best practices and according to the criteria and terms determined by regulation. (s.23) [our emphasis]

For its part, PHIPA includes the following definition:

> "de-identify", in relation to the personal health information of an individual, means to remove any information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual, and "de-identification" has a corresponding meaning; ("anonymiser") [our emphasis]

Further, CANON's proposed amendment aligns with Canadian jurisprudence on the scope of the concept of "personal information". In essence, Canadian jurisprudence provides that information will be deemed to be about an "identifiable individual" where there is a "serious possibility" that an individual could be identified through the use of that information, alone or in combination with other available information. (*Gordon v. Canada (Minister of Health),* 2008 FC 258; see also Canada *(Information Commissioner) v. Canada (Transportation Accident*

Investigation and Safety Board), 2006 FCA 157; see also the OPC's *Interpretation Bulletin: Personal Information* (2013)).

As a final comment, there was considerable discussion on whether to delete the phrase "irreversibly and permanently", which qualifies the term "modify" in the definition of "anonymize". The concern with this phrase (and, in particular, "irreversibly") is that it does not appear logically aligned with the concept of there being "no reasonably foreseeable risk in the circumstances" that is proposed in the revisions set out above (and which aligns with PHIPA and Quebec's Bill 64). Further, inclusion of the phrase "irreversibly and permanently" suggests that these terms have two distinct and operative meanings. Presumably, if information has been modified "irreversibly", that modification is permanent, and vice versa. Notably, the definition of "anonymize" under Quebec's Bill 64 includes the term "irreversibly" only, whereas the equivalent definition under PHIPA does not contain either concept. For drafting clarity, it would be preferable to take the same approach as PHIPA and remove the terms "irreversibly and permanently", which do not appear to be necessary qualifiers. However, for the purposes of this document, a decision was ultimately made not to delete this phrase, as the modification of personal information to create anonymized data is qualified by (1) "generally accepted best practices", and (2) the proposed inclusion of the phrase "no reasonably foreseeable risk in the circumstances" (as also contained in PHIPA and Quebec's Bill 64).

Section 2(1)

~~*disposal*~~***dispose*** means ~~the permanent~~ to permanently and ~~irreversible deletion of~~ irreversibly delete personal information~~. (~~ or to anonymize it. (*retrait*).

CANON Comment:

No amendments recommended. However, as noted in our commentary above under the definition of "anonymize", concerns were expressed regarding the redundancy of the terms "permanently" and "irreversibly".

Section 6(5)

For greater certainty

6(5) For greater certainty, this Act does not apply in respect of personal information that has been anonymized.

CANON Comment:

No amendments recommended.

Part 2 – CPPA: De-identification

Section 2(1)

de-identify means to modify personal information ~~— or create information from personal information — by using technical processes to ensure~~ so that ~~the information does not identify~~ an individual ~~or could not~~ cannot be ~~used in reasonably foreseeable circumstances, alone or in combination with other information, to identify an~~ directly identified from it, though a risk of the individual~~. (~~ being identified remains. (*dépersonnaliser*).

CANON Comment:

No amendments recommended. However, we note that concerns have been raised about the final clause ("though a risk of the individual being identified remains") on the basis that it is superfluous. Simply put, given the definition of "anonymize" (with the proposed revisions above), there would appear to be no need to include an express reference to the risk of "de-identified" data being re-identified.

In addition, and consistent with our comment under s. 74 below, certain stakeholders expressed concern regarding a lack of clarity with respect to the relationship between s. 74 and the definition of "de-identify". Notably, unlike the term "anonymize", the definition of "de-identify" does not expressly contemplate the manner in which personal information must be de-identified. However, when an organization "de-identifies" personal information, the de-identification process would have to comply with s. 74, which requires a proportionate implementation of the technical and administrative measures applied in the circumstances. For ease of reference and to ensure the qualifying language in s. 74 is more clearly brought to the attention of the reader, we recommend moving s. 74 up to become a subsection of s. 2.

Section 2(3)

Interpretation — de-identified information

(3) For the purposes of this Act, other than sections 20 and 21, subsections 22(1) and 39(1), sections 55 and 56, subsection 63(1) and sections 71, 72, 74, 75 and 116, personal information that has been de-identified is considered to be personal information.

CANON Comment:

No amendments recommended. However, questions were raised as to the necessity of this provision, and significant concerns were expressed regarding the highly technical drafting and corresponding likelihood that this provision will create considerable uncertainty for organizations.

Section 20

De-identification of personal information

20 An organization may use an individual's personal information without their knowledge or consent to de-identify the information.

CANON Proposed Amendment:

20 An organization may use an individual's personal information without their knowledge or consent to de-identify or anonymize the information.

CANON Comment:

Although the CPPA is clear that its provisions do not apply in respect of personal information once anonymized (s. 6(5)), there is currently no corresponding exception to consent for the use of personal information to anonymize it, as there is to de-identify it. This proposed revision is consistent with the spirit and intent of s. 20 and serves to remove any uncertainty regarding the lawful authority to "anonymize" personal information without consent.

Section 21

Research, analysis and development

21 An organization may use an individual's personal information without their knowledge or consent for the organization's internal research, analysis and development purposes, if the information is de-identified before it is used.

CANON Comment:

This provision was discussed extensively and concerns were raised as to whether the requirement for personal information to be de-identified in all cases prior to conducting research, analysis and development would impose unintended adverse consequences for organizations who may legitimately require personal information (including direct identifiers) in certain cases in order to conduct the particular research or analysis in question (e.g., in artificial intelligence applications). One of the suggested approaches to "future proof" this provision was to revise the language to contemplate a carveout for those presumably limited circumstances where direct identifiers are required (i.e., consistent with the approach taken under s. 22 (Prospective business transaction)).

Ultimately, it was decided not to propose an amendment on the basis that if an organization needed to use personal information with direct identifiers (i.e., personal information that has not been "de-identified") for research, analysis or development, the organization could rely on the legitimate interest exception to consent under s. 18(3) (provided that the organization conducts an assessment and otherwise complies with the conditions for this exception to consent). Given that any proposed amendment would effectively duplicate a core element of the legitimate

interest provision as it is currently drafted in the CPPA, such an amendment was deemed unnecessary.

Section 22

Prospective business transaction

22 (1) Organizations that are parties to a prospective business transaction may use and disclose an individual's personal information without their knowledge or consent if

(a) the information is de-identified before it is used or disclosed and remains so until the transaction is completed; […]

Exception — paragraph (1)(a)

(2) The requirement referred to in paragraph (1)(a) does not apply if it would undermine the objectives for carrying out the transaction and the organization has taken into account the risk of harm to the individual that could result from using or disclosing the information.

CANON Comment:

No amendments recommended.

Section 39

Socially beneficial purposes

39 (1) An organization may disclose an individual's personal information without their knowledge or consent if

(a) the personal information is de-identified before the disclosure is made;

(b) the disclosure is made to

(i) a government institution or part of a government institution in Canada,

(ii) a health care institution, post-secondary educational institution or public library in Canada,

(iii) any organization that is mandated, under a federal or provincial law or by contract with a government institution or part of a government institution in Canada, to carry out a socially beneficial purpose, or

(iv) any other prescribed entity, and

(c) the disclosure is made for a socially beneficial purpose.

CANON Proposed Amendment:

Socially beneficial purposes

39 (1) An organization may disclose an individual's personal information without their knowledge or consent if

(a) the personal information is de-identified before the disclosure is made;

(b) the disclosure is made to

(i) a government institution or part of a government institution in Canada,

(ii) a health care institution, post-secondary educational institution or public library in Canada,

iii) any organization that is mandated, under a federal or provincial law or by contract with a government institution or part of a government institution in Canada, to carry out a socially beneficial purpose, or

(iv) any other prescribed entity; ~~and~~

(c) the disclosure is made for a socially beneficial purpose~~.~~; and

(d) the organization complies with the prescribed requirements.

[…]

General

[X] Disclosure for socially beneficial purposes

The Governor in Council may make regulations respecting the conditions for the disclosure by an organization under section 39(1) of an individual's personal information without their knowledge or consent for socially beneficial purposes.

[…]

Distinguishing — classes

124 Regulations made under subsection 122(1), ~~or~~ section 123, or section **[X]** may distinguish among different classes of activities, government institutions or parts of government institutions, information, organizations or entities.

[…]

Order in council

130 (4) Sections 39 and **[X]** come into force on a day to be fixed by order of the Governor in Council.

CANON Comment:

The proposed addition at s. 39(1)(d) and associated amendments outlined above address concerns expressed regarding the volume and breadth of disclosures of personal information that could occur in reliance upon this exception to consent by introducing the power for regulations to set out privacy protective requirements and other guardrails as condition(s) for any such disclosure. Such guardrails might include, for example, a requirement for the disclosing organization to enter into a contract with the recipient of the de-identified information that includes appropriate contractual restrictions (e.g., limitations on the permitted uses/disclosures of the data, a covenant on the recipient not to attempt to re-identify the data, etc.). Further, CANON received comments recommending that, rather than leave the specific requirements in regulations, the provision be expanded to include certain requirements (such as those mentioned above) that would serve to enhance the privacy protections afforded to individuals whose personal information might be disclosed pursuant to this provision.

While outside the scope of CANON's focus for proposed amendments, we note that CANON also received several comments expressing concern regarding the broad definition of "socially beneficial purposes" and, by implication, the range of circumstances in which de-identified information could be disclosed under the authority of this provision.

Section 74

Proportionality of technical and administrative measures

74 An organization that de-identifies personal information must 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.

CANON Comment:

No amendments recommended to the text of the provision. However, certain concerns were raised by stakeholders regarding a lack of clarity with respect to the relationship between this s. 74 and the definition of "de-identify". As noted above in our comment under the definition of "de-identify", we recommend moving s. 74 up to become a subsection of s. 2.

Section 75

Prohibition

75 An organization must not use information that has been de-identified ~~information,~~ alone or in combination with other information, to identify an individual~~,~~ except ~~in order~~

(a) to conduct testing of the effectiveness of security safeguards that ~~the organization~~ it has put in place; ~~to protect the information.~~
(b) to comply with any requirements under this Act or under federal or provincial law;
(c) to conduct testing of the fairness and accuracy of models, processes and systems that were developed using information that has been de-identified;
(d) to conduct testing of the effectiveness of its de-identification processes;
(e) for a purpose or situation authorized by the Commissioner under section 116; and
(f) in any other prescribed circumstance.

CANON Proposed Amendment:

75 An organization must not use information that has been de-identified, alone or in combination with other information, to identify an individual except

(a) where the organization can rely on consent or another authority under this Act to use the personal information;
(b) ~~(a)~~ to conduct testing of the effectiveness of security safeguards that it has put in place;
(c) ~~(b)~~ to comply with any requirements under this Act or under federal or provincial law;
(d) ~~(c)~~ to conduct testing of the fairness and accuracy of models, processes and systems that were developed using information that has been de-identified;
(e) ~~(d)~~ to conduct testing of the effectiveness of its de-identification processes;

(f) ~~(e)~~ for a purpose or situation authorized by the Commissioner under section 116; ~~and~~ or
(g) ~~(f)~~ in any other prescribed circumstance.

CANON Comment:

The proposed amendment at s. 75(a) helps to ensure an organization that takes steps to de-identify personal information for safeguarding, data minimization or other privacy sensitive measure is not, as a consequence, more restricted than it would otherwise have been to use the data in identifiable form. Notably, under the GDPR, pseudonymization (i.e., de-identification) is referenced throughout the statutory framework as a means to safeguard personal information. Simply put, clear and concise drafting of this section is necessary to avoid inadvertently prohibiting innocuous re-identification activities by an organization that uses de-identification for these wholly legitimate and appropriate purposes.

Further, the proposed amendment at s. 75(a) aligns with the assumption that the primary purpose of this provision is to prevent the re-identification of de-identified information by an organization that receives that information from another organization, rather than to prevent an organization that has itself de-identified the information for safeguarding, data minimization or other privacy sensitive measure from permitted uses internally.

There was also discussion about a proposed amendment to expressly contemplate the re-identification of personal information "for the purposes of preventing or mitigating harm to the individual". This proposed amendment was suggested as, from a public policy perspective, it would be desirable and otherwise entirely appropriate to ensure that organizations are not restricted by the CPPA from using de-identified information, alone or in combination with other information, for the purposes of preventing or mitigating harm to the individual to whom such information relates. However, such a provision may not be necessary, as presumably an organization seeking to re-identify de-identified information for such purposes could rely on the proposed s. 75(a) and/or the existing exception enabling organizations to comply with any requirements under the Act (which would include obligations to safeguard personal information and notify affected individuals for the purpose of mitigating harm).

Finally, as a minor drafting point, we have replaced "and" with "or" to clarify that each exception is independent and need not occur in conjunction with the rest.

The above amendments are critically necessary in light of the substantial penalties introduced under s. 128 for contraventions of s. 75.

Section 116

De-identified information

116 For the purpose of paragraph 75(e), the Commissioner may, on request by an organization, authorize a purpose or situation in which the organization may use information that has been de-identified, alone or in combination with other information, to identify an individual if, in the Commissioner's opinion, it is clearly in the interests of the individual.

CANON Comment:

No amendments recommended.

Section 128

Offence and punishment

128 Every organization that knowingly contravenes section 58, subsection 60(1), section 69 or 75 [*prohibition section discussed above*] or subsection 127(1) or an order under subsection 93(2) or that obstructs the Commissioner or the Commissioner's delegate in the investigation of a complaint, in conducting an inquiry or in carrying out an audit is

> **(a)** guilty of an indictable offence and liable to a fine not exceeding the higher of $25,000,000 and 5% of the organization's gross global revenue in its financial year before the one in which the organization is sentenced; or

(b) guilty of an offence punishable on summary conviction and liable to a fine not exceeding the higher of $20,000,000 and 4% of the organization's gross global revenue in its financial year before the one in which the organization is sentenced.

CANON Comment:

No amendments recommended. However, we note that the substantial penalties associated with the re-identification prohibition under s. 75 highlight the importance of ensuring clear and concise drafting of s. 75 to avoid inadvertently prohibiting reasonable and expected re-identification activities by an organization that uses de-identification as a safeguarding, data minimization or other privacy sensitive measure.

PART 3 – AIDA

Section 6

Anonymized data

6 A person who carries out any regulated activity and who processes or makes available for use anonymized data in the course of that activity must, in accordance with the regulations, establish measures with respect to

> **(a)** the manner in which data is anonymized; and
>
> **(b)** the use or management of anonymized data.

CANON Comment:

The proposed text of the *Artificial Intelligence and Data Act* ("**AIDA**") in Bill C-27 does not contain a definition of "anonymized data". We recommend amending AIDA to include the same definition as is contained in the CPPA to ensure the concept of anonymized data is utilized consistently in both statutory frameworks. As set out above, the definition would read:

> ***anonymize*** means to irreversibly and permanently modify personal information, in accordance with generally accepted best practices, to ensure that there is no reasonably foreseeable risk in the circumstances that an individual can be identified from the information, whether directly or indirectly, by any means.