Report on the Adequacy of Identity Governance Transparency

GDPR, PIPEDA, and the Pan-Canadian Trust Framework (PCTF)

DIACC Special Group Insights

Table of Contents

Contents of this paper have been submitted by the DIACC International Pilots Special Interest Group. For further information about the topics discussed in this paper, or to join the DIACC community, visit www.diacc.ca or contact info@diacc.ca.

About DIACC

Created as a result of the federal government's Task Force for the Payments System Review, the Digital ID & Authentication Council of Canada **(**DIACC**)** is a non-profit coalition of public and private sector leaders who are committed to developing a Canadian digital identification and authentication framework that will secure Canada's full and secure participation in the global digital economy.

DIACC innovation papers focus on current issues and opportunities for the digital identity ecosystem. DIACC innovation papers are guided by the DIACC's 10 Digital ID & Authentication ecosystem principles and by the priorities of DIACC members. DIACC papers provide insights to governance of business, legal, and technical audiences in Canada and around the world. DIACC papers are not endorsements and do not represent a qualified organization's opinion of the DIACC. DIACC innovation papers are pragmatic and address real-world issues; are open and transparent; vision future opportunities; communicate learning from past projects; are authored by DIACC member domain experts with real-world expertise.

About DIACC Special Interest Groups

A DIACC Special Interest Group (SIG) provides a mechanism in which to engage our community in discussion around a specific interest. They enable more opportunities to connect subject matter experts from around the world and to broaden the conversations outside of our DIACC membership.

A DIACC SIG does not create intellectual property but rather contemplates a specified question to make a recommendation to DIACC regarding the next steps that should be considered for incorporation into the DIACC strategy and roadmap.

About the Primary Authors

Alessandro Ortalda is doctoral researcher at the Vrije Universiteit Brussels (Brussels, Belgium) and training coordinator for the Brussels Privacy Hub. He holds a bachelor degree in History from Ca' Foscari University (Venice, Italy) and a master of social science in International Security and Law from Southern Denmark University (Odense, Denmark), where he graduated in 2015 with a thesis entitled "The international law on the use of force in the context of information technology". After his master's degree, he worked as a cybersecurity consultant, specializing in advisory services to governments and international organizations concerning

national cybersecurity and strategy, cyber-capacity building, and national digital identity systems

Mark Lizar holds a bachelor of Law, Criminology, and Anthropology from Carleton University (Ottawa, Canada) and pursued a career in digital identity before completing an MSc in Social Research Methods from South Bank University (London, UK) where he graduated with a thesis entitled "Towards a Framework of Contextual Integrity: Legality, Trust and Compliance of CCTV Signage", published in the Canadian Queen's University Text 'Eyes everywhere, the Global Growth of Surveillance', Routledge. After his masters degree, he became CEO of Open Consent Group and specialized in Notice & Consent working on standards for digital identity governance and interoperability. Contributing to the development of the Pan-Canadian Trust Framework. Consulting in both the private and public sector, managing a Privacy Assurance Lab for advancing data governance projects.

Additional SIG support and contributions made by:

- Pierre A. Roberge, General Manager, Digital Identity Laboratory of Canada
- Dick Dekkers, Director Business Development, Digidentity
- Fred Carter, Senior Policy & Technology Advisor at the Office of the Information and Privacy Commissioner of Ontario, Canada
- Sanjay Khanna, CEO/Co-Founder, ValidCert Inc.
- Sal D'Agostino, CEO, IDmachines and Co-Founder, OpenConsent

Abstract

International transfer in the context of transborder use of digital identity is growing rapidly. This means that digital identity systems' owners and service providers must navigate different laws and accommodate their practices to different regional requirements.

This report on the adequacy and interoperability of data governance transparency examines the different information and entity transparency requirements.

This report is based on the appending table which maps the transparency requirements in both European and Canadian law. The mapping is conducted in order to evaluate whether the two normative instruments are aligned with each other, so as to be suitable for international transfer, in the context of transborder use of digital identifiers, credentials and digital wallets.

Executive Summary

In the last few years, the importance of digital identity has grown exponentially, from being an instrument employed primarily to secure closed systems (such as corporate networks) to being a platform for governments to deliver eGovernment public services.

This report looks at Transborder use of digital identity in the context of international transfer, control, and access to private/personal data between Canada and the European Union. In particular, it looks at such data transfer considering the obligation to inform individuals during data processing and investigate whether the provisions of the Canadian legal framework adequately match those of the European legal framework. At the time of writing, the only official exercise of this kind is represented by the European Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act. Accordingly, the Canadian legal framework is considered adequate for the data protection standards of the European Union(1). However, since the publication of this decision in 2001, both Canadian and European data protection norms and digital governance have evolved following the publication of new legal instruments. Thus, a new baseline assessment is necessary to build and assess the adequacy of digital identity system governance.

Introduction

This report on the adequacy and interoperability of data governance transparency examines the different information and entity transparency requirements for privacy notice.

The goal of this document is to identify:

- a path forward for a standardized notice governance model, in a manner that can express the requirements in the Canadian Personal Information Protection and Electronic Documents Act last amended on June 23, 2015 (hereinafter, PIPEDA) and the European General Data Protection Regulation (GDPR).
- transparency and accountability governance gaps through an assessment of adequacy in order to assert whether Canadian law is already suitable to ensure compliance with the European obligation (and vice versa) in case of international transfer.
- how the use of international standards can be used for co-regulating adequacy safeguards.

This assessment then reports on the utility of the Pan-Canadian Trust Framework to supplement PIPEDA to address adequacy gaps in digital identity governance, by assessing its Notice & Consent Conformance Profile Final Recommendation V1.0 component (PCTF N&C). Even so, this report is critical of aligning to the PCTF, as it is not mandatory for Canadian organizations to adopt.

The next sections introduce and describe the data protection frameworks currently in force in Canada and Europe.

Canadian Privacy Framework

Canada has two federal privacy laws that are investigated by the Office of the Privacy Commissioner of Canada:

- the Personal Information Protection and Electronic Documents Act (PIPEDA), which regulates how businesses handle personal information.
- the Privacy Act, regulates how the federal government handles personal information;

In addition, every province and territory has its own laws that apply to provincial government agencies and their handling of personal information. In this analysis, sincePIPEDA sets national standards for privacy practices in the private sector and, in practice, provincial privacy laws co-exist and are deemed to be substantially similar with PIPEDA. `In this regard, whether or not

transparency is required for who controls processing, who is accountable, who is the beneficial owner of the data processed and if there is a meaningful choice of benefit or consent when required.

European data protection framework

The main european legal instrument on data protection is Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter, also General Data Protection Regulation, GDPR). The GDPR spells out the principles that guide the behavior of entities processing personal data, and from these derive requirements for standardized notification compliance.

One of the principles adopted by the GDPR is the Transparency Principle. Accordingly, individuals shall be timely and effectively informed on the objectives, modalities, and processing elements connected to the use of personal data. Including the duty to inform individuals and provide notice with a specific set of information that, to a minimum, shall be provided to individuals. This obligation becomes particularly important in the context of international data transfer, such as between Canada and Europe. Indeed, the set of information to be provided to individuals in Canada might differ from that required for citizens when in Europe. Thus, Canadian organizations might not be equipped to ensure compliance during the data transfer.

Canada - Europe private and personal data exchange

The goal of this document is to identify:

- a path forward for a multi-jurisdictional/provincial, standardized notice governance model, required by the the Canadian Personal Information Protection and Electronic Documents Act last amended on June 23, 2015 (hereinafter, PIPEDA) and the European General Data Protection Regulation (GDPR).
- transparency and accountability gaps through an assessment of adequacy in order to assert whether Canadian law is already suitable to ensure compliance with the European obligation (and vice versa) in case of international transfer.
- how the use of international standards can be used for co-regulating adequacy safeguards.

This gap assessment then reports on the utility of the Pan-Canadian Trust Framework to supplement PIPEDA to address adequacy gaps in digital identity governance, by assessing its

Notice & Consent Conformance Profile Final Recommendation V1.0 component (PCTF N&C). Even so, this report is critical of aligning to the PCTF, as it is not mandatory for Canadian organizations to adopt.

Adequacy Assessment

The goal of the present section is to assess the information requirements in Canada and Europe, which is then used to assess the level of adequacy between the two legal frameworks for data processing transparency and accountability. However, it is first necessary to clarify the vocabulary as the frameworks use different terms to assign accountability.

The table below maps the regulatory terminology to illustrate how specific adequacy concepts and their legal elements are labeled in the corresponding instruments.

GDPR terms	**PIPEDA terms**	**PCTF N&C terms**
Personal data	Personal information	Personal information
Data subject	Individual	Subject
Data controller	Organization and Designated individual[1]	Disclosing / Requesting Organization / Notice & Consent Operator[2]
Data processor		
Data processing	Collection, use, or disclosure in the course of commercial activities	Collection, use, or disclosure
Data Protection Officer	Individual(s) designated by the organization to oversee compliance	N/A
Special categories of personal data	Sensitive personal information	Sensitive information

[1] PIPEDA does not distinguish "controller" and "processor".
[2] PCTF adopts a functional taxonomy for roles, rather than a responsibility or governance-based taxonomy as the GDPR. Thus, full adherence of terms is not possible

Results of the assessments and mitigation proposals

The following table builds on the requirements mapping and analysis (provided in the appendix to this document) and assesses the adequacy of PIPEDA and the PCTF's information notice requirements with GDPR's information requirements. Each requirement can be assigned one of four values while the line numbers also correspond to the assessment tables in the appendix:

- (Red) No adequacy: the requirement is not addressed
- (Yellow) Partial adequacy: the requirement is addressed but not in the same way as GDPR
- (Green) Adequacy: the requirement is addressed adequately

#	GDPR Notice Requirement	Assessment of PIPEDA	Assessment of PCTF	Analysis and rationale
1	The identity of data controller [articles 13, 14]	Partial adequacy	Partial adequacy	PIPEDA requires that the identity information is to be provided 'upon request'. PCTF does not mandate this information (uses 'could' instead of 'shall').
2	The contacts of data controller [articles 13, 14]	No adequacy	Partial adequacy	PIPEDA does not mandate to include contact details ('business contact information' in PIPEDA). PCTF does not mandate this information (uses 'could' instead of 'shall').
3	The identity of data controller' representative (if applicable) [articles 13, 14]	No adequacy	Partial adequacy	Canadian entities processing data of Europeans might fall in the territorial scope of Article 2.3. This requires them to designate a representative in the Union as per article 27. The role is not present in PIPEDA. Therefore there is no requirement to disclose information about it. PCTF does not mandate this information (uses 'could' instead of 'shall').
4	The contacts of data controller' representative (if applicable) [articles 13, 14]	No adequacy	Partial adequacy	See #3
5	The contacts of the Data	Partial adequacy	Partial adequacy	PIPEDA provides that the information is to be provided 'upon request'.

	Protection Officer (if applicable) [articles 13, 14]			PCTF does not mandate this information (uses 'could' instead of 'shall').
6	The purpose of the data processing [articles 13, 14]	Partial adequacy	Partial adequacy	PIPEDA does not mandate this information (uses 'should' instead of 'shall') as this can be a result of derogations specified in the regulation. PCTF does not mandate this information (uses 'could' instead of 'shall').
7	The categories of personal data concerned (when data not collected from data subject) [article 14]	Adequate	No adequacy	PIPEDA 'Shall include [..] a description of the type of personal information'
8	The recipients or categories of recipients of the personal data (if applicable) [article 13];	Partial adequacy	Partial adequacy	The identity of Recipients or category of recipients are not required or suggested in PIPEDA, only 'what information is made available to related organizations'.
9	The legal authority for processing personal information [articles 13, 14][3]	Partial adequacy	Partial adequacy	PIPEDA does not have the granular concept of 'legal basis' but a broader framework from consent and a set of exceptions to it. An analysis of PIPEDA's exceptions is needed to understand if the exceptions of PIPEDA map to GDPR's legal basis. PCTF does not mandate this information (uses 'could' instead of 'shall').
10	The legitimate interest pursued by the controller or third parties (if applicable) [articles 13, 14]	No adequacy	Partial adequacy	Although PIPEDA Div 1-7.1.a might be assimilated to GDPR's 'legitimate interest', it often contains processing that is not in the best interests of the data subject. PIPEDA absence of any information requirement (as they are not required for processing outside of consent) makes this effectively void.
11	The intention of the data controller to transfer personal data to a third country or international	No adequacy	Partial adequacy	PIPEDA does regulate extraterritorial data transfer. PCTF does not mandate this information (uses 'could' instead of 'shall').

[3] In the context of consent as a legal authority PIPEDA might only be partially adequate with GDPR. Not reflected in this analysis is that PIPEDA has been enhanced with additional legal instruments which are not assessed here. In particular, 'meaningful consent' which has a high legal standard that requires notice of privacy risk and harms.

	organization [articles 13, 14]			
12	In case of transfer, the existence or absence of an adequacy decision by the Commission, or, where applicable, reference to the safeguards and the means by which to obtain a copy of the data [articles 13, 14]	No adequacy	No adequacy	PIPEDA does regulate extraterritorial data transfer. Reference to safeguards during transfers are not found in PIPEDA nor PCTF Notice and Consent module.
13	The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period [articles 13, 14]	Partial adequacy	Partial adequacy	PIPEDA limits collection. However, it does not require including this information in the privacy notice. Moreover, Principle 4 does not deal with temporal limits for data storage. PCTF does not mandate this information (uses 'could include' instead of 'shall').
14	The existence of the right to request access to and rectification or erasure of data or restriction of processing concerning the data subject or to object to processing and the right to data portability [articles 13, 14]	Partial adequacy	Partial adequacy	PIPEDA envisages the possibility for individuals to access data upon request and ask for rectification, but it does not explicitly require to put this disclaimer in the privacy notice. PCTF does not mandate this information (uses 'could' instead of 'shall').
15	In case of consent as legal basis for processing, the existence of the right to withdraw consent at any time [articles 13, 14]	Partial adequacy	Adequacy	PIPEDA does not mandate this information (use of 'should' instead of 'shall').

16	The right to lodge a complaint with a supervisory authority [articles 13, 14]	Partial adequacy	No adequacy	PIPEDA only encourages an information duty, unless this is specifically requested by the data subject. GDPR mandates to put this information in the privacy notice.
17	The source of the personal data, and if applicable, whether they came from publicly accessible sources (only when data not collected from data subject) [article 14]	Partial adequacy	No adequacy	See #15
18	Whether the provision of data is a statutory or contractual requirement, or a requirement to enter into a contract, and whether the data subject is obliged to provide the data and the consequences of failure to provide such data (only when data collected from data subject) [article 13]	Partial adequacy	Partial adequacy	Source of identity attributes (personal data) is encouraged but not required in both PIPEDA and the PCTF.
19	The existence of automated decision-making, including profiling [articles 13, 14]	No adequacy	No adequacy	PIPEDA does not distinguish between manual and automated processing.
20	In the case of automated decision-making, information on the logic involved, the significance of processing, and its envisaged	No adequacy	No adequacy	See #18

	consequences for the subject [articles 13, 14]			
21	Information shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child [article 12]	Partial adequacy	Adequacy	GDPR is stricter and more granular. Also, this requirement applies to all the information provided to the data subject, while PIPEDA only requires to inform the user on the purpose.
22	Information shall be provided in writing, or by other means, including, where appropriate, by electronic means [article 12]	Partial adequacy	Adequacy	GDPR sets writing as default unless the data subjects requests otherwise. PIPEDA puts the same options at the same level.
23	When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. [article 12]	Partial adequacy	Adequacy	GDPR sets writing as default unless the data subjects requests otherwise. PIPEDA puts the same options at the same level.

The assessment of the requirements reveals how, for the most part, Canadian law is not operationally aligned with those in Europe. However, this is not the result of a completely different approach to data protection. Indeed, the PIPEDA appears to be highly aligned with the GDPR in terms of scoping, subject matter, principles, and safeguards for individuals. Most of the requirements reach the level of partial adequacy, demonstrating a certain level of alignment. However, partial adequacy is not enough, and is observed to often be the result of a different level of enforcement granularity PIPEDA and PCTF adopt, with the GDPR implementing a more strict enforcement approach.

Further analysis towards governance interoperability should include the principle of proportionality, which is highly relevant, both in terms of balancing rights of stakeholders (GDPR; Recital 4) and in terms of the performance of transparency to mitigate digital privacy risks[4], indicative to Article 35, 7(b) of the GDPR and the Canadian regulatory approach.

This means that a correction for this misalignment can be implemented with relative ease, since for the most part it is not necessary to address new obligations, but is sufficient to increase the level of detail of the provisions. In order to avoid changes to the normative framework, such correction could be provided by means of a code of conduct with standardized notice record and receipt management.

Conclusion

For Canadian and international businesses it is not feasible to amend the set of information required by Canadian law every time a transfer of data to Europe occurs in a digital product or service. This approach would require disproportionate effort as it demands the entity to assess every single data transfer, to look at the destination of the data, and then amend the set of information accordingly. A simpler approach would be to utilize a standard set of transparency and consent defaults that includes the minimum information required in Canada and Europe.

Recommendations

Transparency and accountability now have international standards for records for privacy access enforcement mechanisms.

1. Always ensure the maximum level of transparency and accountability as possible;
    a. use standards for privacy notice semantics and records.[5]
    b. provide consent notice receipts in a standard record format with a standard record information structure to make transparency proportionate and trust-able.
    c. to reduce and eliminate dark patterns ensure transparency/notice or notification is mandatory...controller and authority.

[4] Proof of notice records and receipts can be used to transfer liability and manage privacy risk. Much like a receipt for a financial transaction provides proof of purchase.

[5] Standards for privacy notice records and receipts refer to a conformance suite consisting of; ISO/IEC 29100 for notice record assessment format, ISO/IEC 29184 for online privacy notice conformance criteria, with a Consent Receipt found in AppendixD as evidence, ISO/IEC 27560, consent record/receipt information structure, W3C Data Privacy Vocabulary Controls for legal semantics that are human + machine readable). ToiP - Controller Credential, Kantara Initiative Record and Receipt information structure, as well as the ANCR Record,

2. Map functional/technical roles in digital identity trust (the PCTF) to privacy stakeholders for clear transparency and accountability and use international standards --> ISO/IEC for identifying Canadian citizens and legally accountable parties and justifications for processing data.
3. Utilize standards to implement records for auditing the processing of data with digital identifiers.
    a. embed transparency with 2 factor privacy notices that generate a notice record and provide people with a receipt for proof of notice and evidence of consent in digital identity management systems.
    b. use Privacy Notice Credentials to sign Receipts to create micro-credentials that un-link identifiers, safeguard personal information and transport identifiers, attributes and verifiable credentials in records people can own, understand and control.
4. Utilize international privacy instruments as best practice guidance for transparency and accountability that can scale in and out of Canada (e.g., Council of Europe 108+).

What's next

1. Socialize the report with provincial/territorial governance authorities and privacy regulators to raise awareness of the urgent need for updating privacy rules to protect the Canadian single digital market.
2. Outline further a pilot and use case in support of a diploma credential and micro-credential. Led by the requirements provided from the education consortia for an eIDAS gateway.

Appendix A: Table Identifying privacy notice adequacy gaps

The following table maps and compares the information requirements in GDPR, PIPEDA, and the PCTF Notice & Consent (PCTF N&C) component. For each one, it describes what information should be provided including the articles and provisions where such information requirements are sanctioned.

In this table the term Notice is used and interpreted broadly referring to privacy notifications, disclosures, surveillance signs, and signals that present transparency to an Individual.

#	Transparency and Accountability Requirement	GDPR	PIPEDA	PCTF N&C
1	Notice to identify the organization which is accountable for data processing. Knowing or Notice of who you are consenting too is an operational requirement for legal evidence of consent.	The identity of data controller [articles 13, 14]	The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known (upon request) [Sc. 1-4.1.2]	In a digital identity system, information in the notice statement could include: [...] the identity and details of the Requesting Organization [NOTI 3]
2	The notice of a contact for the individual to access privacy rights or information in proportion to processing.	The contacts of data controller [articles 13, 14]	N/A	In a digital identity system, information in the notice statement could include: [...] contact information [...] of an authorized person who can answer Subject's questions about the collection [NOTI 3]
3	Notice of the identity of the organization that represents the notice controller in the jurisdiction of Individual and/or context of service provision.	The identity of data controller' representative (if applicable) [articles 13, 14]	N/A	In a digital identity system, information in the notice statement could include: [...] the identity and details of the Requesting Organization [NOTI 3]
4	The contact of the representative organization to access to privacy rights.	The contacts of data controller' representative (if applicable) [articles 13, 14]	N/A`	In a digital identity system, information in the notice statement could include: [...] contact information [...] of an

				authorized person who can answer Subject's questions about the collection [NOTI 3]
5	The contact of the accountable person or privacy officer for the administration of privacy rights.	The contacts of the Data Protection Officer (if applicable) [articles 13, 14]	The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known (upon request) [Sc. 1-4.1.2]	In a digital identity system, information in the notice statement could include: [...] contact information [...] of an authorized person who can answer Subject's questions about the collection [NOTI 3]
6	Notice of purpose of use for the collection, use, disclosure and processing if not inherent to the subject's actions.	The purpose of the data processing [articles 13, 14]	The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected [Sc. 1-4.2.3]	In a digital identity system, information in the notice statement could include: [...] the purpose for which the personal information is being requested [NOTI 3]
7	Label to indicate the type and sensitivity of data that is processed is a minimum requirement.	The categories of personal data concerned (when data not collected from data subject) [article 14]	The information made available [to the individual] shall include [...] a description of the type of personal information held by the organization [Sc. 1-4.8.2.c]	N/A
8	3rd party recipient of personal data.	The recipients or categories of recipients of the personal data(if applicable) [article 13];	**(e)** what personal information is made available to related organizations (e.g., subsidiaries). [Schedule 1-4.8.2]	N/A[6]
9	The legal authority or justifications is specified in GDPR and ISO/IEC standards, and indicates what rights or digital identity controls can apply in context.	The legal basis for the processing [articles 13, 14]	N/A	In a digital identity system, information in the notice statement could include: [...] the legal authority for collecting the personal information or justification that clarifies the legal rationale for its collection [NOTI 3]
10	Legitimate interests refer to processing or surveillance relevant to the purpose specified and has 3 step assessment. An example would be an insurance company monitoring for fraud.	The legitimate interest pursued by the controller or third parties (if applicable) [articles 13, 14]	An organization may collect personal information without the knowledge or consent of the individual only if [...] the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way [Div 1-7.1.a]	In cases where legislation or regulation does not require consent, notice SHOULD still be provided unless legislation, regulation, or policy prohibit it, or circumstances justify [NOTI 1]

[6] In the PCTF Privacy component, the names or categories of third-party recipients of personal information is required [Privacy Component Open 1]

11	Transparency over the transborder flow of personal information.	The intention of the data controller to transfer personal data to a third country or international organization [articles 13, 14]	N/A	In a digital identity system, information in the notice statement could include: [...] notification that data will be stored outside of a relevant jurisdiction in cases where that will be done, as required by data residency related legislation, regulation, or policy, notification [NOTI 3]
12	Notice of the adequacy of data governance for privacy rights access and controls when data is transferred across borders.	In case of transfer, the existence or absence of an adequacy decision by the Commission, or, where applicable, reference to the safeguards and the means by which to obtain a copy of the data [articles 13, 14]	N/A	N/A
13	Notice that provides the length of time personal data will be stored.	The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period [articles 13, 14]	Both the amount and the type of information collected shall be limited to that which is necessary to fulfill the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle [Sc. 1-4.4.1]	In a digital identity system, information in the notice statement could include: [...] the period of time for which the personal information requested will be stored or used [NOTI 3]
14	Notice of the rights to access, amend, restrict, object or control the processing of personal data.	The existence of the right to request access to and rectification or erasure of data or restriction of processing concerning the data subject or to object to processing and the right to data portability [articles 13, 14]	N/A	The Notice and Consent Processor SHOULD provide Subjects with the ability to manage all consent decisions made. These features SHOULD be easy to use, providing an efficient and optimal means for Subjects to manage consent decisions [MANA 7]
15	Notice of right to withdraw consent at any time.	In case of consent as legal basis for processing, the existence of the right to withdraw consent at any time [articles 13, 14]	An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal. [Sc. 1-4.3.8]	Where a Subject has the right to withdraw their consent at a later date, the Requesting Organization [...] MUST: • inform the Subject of this right (subject to reasonable notice and applicable conditions or restrictions) at the time consent is requested;

				• inform the Subject of how to exercise this right; and • ensure that the process for withdrawing consent is as easy for the Subject as providing consent. [CONS 8]
16	Notice that provide access to privacy right to complain and be heard by a regulator.	The right to lodge a complaint with a supervisory authority [articles 13, 14]	Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory bodies accept complaints about the personal-information handling practices of the companies they regulate [Sc. 1-4.10.3]	N/A
17	Disclosure of the source of personal data when not provided by the individual.	The source of the personal data, and if applicable, whether they came from publicly accessible sources (only when data not collected from data subject) [article 14]	Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. [Sc. 1-4.9.1]	In a digital identity system, information in the notice statement could include: [...] the identity and details of the potential sources of the requested personal information, be they Disclosing Organizations or the Subject concerned [NOTI 3]
18	Notice of whether data is optional, why data is required e.g. statutory, for a contract, and what the consequence is - if someone does not provide personal data.	Whether the provision of data is a statutory or contractual requirement, or a requirement to enter into a contract, and whether the data subject is obliged to provide the data and the consequences of failure to provide such data (only when data collected from data subject) [article 13]	N/A	N/A
19	Notice if a profile is created with a digital identifier. What Automated data processing is the profile used for?	The existence of automated decision-making, including profiling [articles 13, 14]	N/A	N/A
20	Notice of profiling, logic of automated decision making. Notice what are the consequences and risk	In the case of automated decision-making, information on the logic involved, the significance of processing,	N/A	N/A

	of harm	and its envisaged consequences for the subject [articles 13, 14][7]		
21	referring specifically to the quality, performance, and usability of notifications for privacy and privacy rights access. Derived from principle to be open.	Information shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child [article 12]	Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. [Sc. 1-4.3.3]	The Notice and Consent Processor MUST ensure that the information to be included in a notice statement is unambiguous. In a digital identity context, this could include, for example, the specific personal information to be shared and the necessary metadata. [NOTI 4]
22	Requirements for the provision and availability of notice and notice records	Information shall be provided in writing, or by other means, including, where appropriate, by electronic means [article 12]	The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes. [Sc. 1-4.2.2]	The notice statement SHOULD be presented in writing and MUST be provided in language that enables Subjects to reasonably understand how their personal information will be used or disclosed. [...] Where it is not practical for the notice statement to include additional details pertaining to the request (e.g., full terms and conditions, detailed metadata), a convenient means SHOULD be provided to allow the Subject to review those details, ideally as part of the digital workflow being delivered. This MUST NOT be used as a means to make the notice statement less visible, transparent or Accessible. [NOTI 5]
23	Notice, notification, and disclosures to be provided orally when requested.	When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. [article 12]	The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this	N/A

[7] Under PIPEDA, meaningful consent is required in which the risk of harms must be clearly be notified to the Individual, which goes beyond what the GDPR requires

			can be done orally or in writing. An application form, for example, may give notice of the purposes. [Sc. 1-4.2.3]	