Laboratoire de CYBERJUSTICE Laboratory

GUIDE TO BEST PRACTICES RELATING TO THE CREATION OF PRIVACY POLICIES IN THE CULTURAL[i] SECTOR

IVADO

SYNAPSE C

September 2019

Laboratoire de CYBERJUSTICE Laboratory

Table of Contents

Terms of Mandate

As part of the "Start-up Program for Collaborative Research Projects with IVADO's Industrial Members", Synapse C, a non-profit organization that aims to develop and pool expertise in data enhancement for arts and culture in Quebec and Canada, and IVADO, an organization dedicated to bringing together industry professionals and academic researchers in order to develop leading-edge expertise in the fields of data science, optimization, and artificial intelligence, have contacted the Cyberjustice Laboratory, a technology law research centre of the Faculty of Law of the Université de Montréal, to participate in a collaborative research project.

The objective is to conduct a study on data collection in the arts and culture sector in Canada, including the development of privacy policies that reflect best practices in the field from the creation date of this guide. More specifically, Synapse C has mandated the Cyberjustice Laboratory to:

- Conduct an analysis of Quebec and federal data protection law; and
- Draft a guide to best practices on privacy policies for Quebec and Canadian organizations that would benefit from having their data shared and valued by third parties, such as Synapse C, so that these third parties may collect data from these organizations while respecting individual rights.

The approach of this guide to best practices will be twofold. To do so, we intend to conduct an analysis of Quebec and federal law so that Synapse C can provide standardized recommendations for both Quebec and Canadian arts and culture sector stakeholders, as these organizations wish to have a better understanding of the issues surrounding Personal Information (PI), particularly with respect to privacy policies. It is important to note, however, that the analysis does not cover legislation applicable to other provinces in the private sector, specifically the Personal Information Protection Act of British Columbia[1], as well as Alberta's Personal Information Protection Act[2]. It is also important to consider the rapid evolution of technology and applicable legislation, as this guide and privacy policies are limited to the situation prevailing at the time of writing.

Introduction

[1] *Personal Information Protection Act,* S.B.C. 2004, ch. 6
[2] *Personal Information Protection Act,* S.A. 2003, ch. P-6.5.

"The world's most valuable resource is no longer oil, but data." Since the publication of this article in *The Economist* in 2017, few are still skeptical about the scale of the societal transformation brought about by the advent of an era of big data or massive data. Indeed, the use of data, combined with its processing, can boost social and economic value, but also raises a variety of questions around risks and the ways in which they are framed.

On the one hand, it can contribute to boosting productivity and improving or promoting new products, processes, organizational methods and markets, and what the Organization for Economic Co-operation and Development (OECD) calls "Data Driven Innovation"[3]. On the other hand, one cannot hide the fact that these data are issued by real people , subjects to rights, and that the processing of these data leads to the disclosure of personal or sensitive information depending on the context. Data protection must, therefore, go hand in hand with data use.

Thus, there is a growing awareness of data protection among citizens, while companies want to obtain and retain as much data as possible for their processes, services, etc. How can these two requirements be combined, particularly in the cultural field where many companies, NPOs, or public bodies coexist and may wish to exchange or pool their data for joint ventures or to improve the public experience?

1 - Definitions and Concepts

[3] Studies of companies suggest that data use and analysis increases productivity faster than in non-user companies by about 5-10%.

In order to better understand the protection of personal information, it is essential to understand the definition of the data as the primary focus of protection,

What is Data?

Technically, the field ofcomputer science defines data as a representation of information in a program, whether in the text of the program itself, called "source code", or in the execution of the program. This data, mainly represented as code, then represents elements of the software that can be interactions, transactions, or other.

When one seeks to define data in a legal rather than a technical framework, it becomes important to differentiate between information and data. Indeed, data are raw elements that must be interpreted in order to derive information and, therefore, do not necessarily mean the same thing . This distinction is essential since it justifies the creation of a specific right to data protection, distinct from the right to information protection, which includes intellectual property rights and confidentiality rights.

Nevertheless, it should be recognized that some data are easier to interpret than others and, therefore, may provide access to sensitive information about individuals. This is why, with the aim of establishing adequate protection of data concerning individuals, also called Personal Information (PI), we must look at classification methods so that we may adapt our actions to various types of data collected. The application of legal principles and obligations, whether they come from the Quebec or federal legislator, changes according to the type of data.

How is Data Classified?

Although there is no clear consensus on how to classify data, nevertheless, it is possible to put forward certain classification criteria that are essential to the development of privacy protection of individuals.

Personal information:

In this sense, the essential criteria for classification is that of the personal nature of the data.

In Quebec, personal information is any information that relates to a physical person and allows that person to be identified[4]. The Personal Information Protection and Electronic Documents Act (hereinafter "Federal Private Sector Act", also known by its acronym “PIPEDA”) defines personal information as information about an identifiable individual[5]. Here are a few examples:

- "The information may include age, name, identification number, income, ethnicity or blood type;
- An opinion, evaluation, comment, social status or disciplinary action;[6]
- An employment record, a credit or loan record, a medical record, the existence of a dispute between a consumer and a merchant, or a person's future plans (for example, the intention to acquire goods or services or to change jobs).”[6]

As a general rule, information will be deemed to relate to an "identifiable individual" when it is reasonably possible to identify an individual through the use of that information, alone or in combination with other information.

[4] Sec. 2 of Protection of Personal Information in the Private Sector Act
[5] Sec. 3 of Protection of Personal Information in the Private Sector Act
[6] Office of the Privacy Commissioner of Canada, *PIPEDA in Brief*, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/ , May 2019.

Data sensitivity:

In Quebec law, data sensitivity is not legally defined as such. On the other hand, section 10 of the Protection of Personal Information in the Private Sector Act (hereinafter "Quebec Private Sector Act") and section 63.1 of the Act Respecting Access to Documents held by Public Bodies and the Protection of Personal Information state in the same way that a public body or an enterprise “must take the security measures that are necessary to ensure the protection of personal information collected, used, released, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes of its intended use , the quantity, and distribution of the information, and the medium on which it is stored.”

Under federal law, data sensitivity is not directly defined either. The Federal Private Sector Act merely states that any information may be considered sensitive depending on the context and that the security measures to be taken to protect personal information depend on the nature and sensitivity of that context[7].

Exchanges of information that may contain personal information:

A relevant approach for the development of privacy policies is to distinguish between the parties involved in data flows and to allow an immediate assessment of the personal nature of the information exchanged between them.

The table below, taken from the OECD report, *Data in the Digital Age*, illustrates, on a scale of 1 to 10, the level of personal information in a data exchange, where 1 equals a low rate of personal information and 10 equals a high rate of personal information.

[7] Section 7.2 (1) and section 10.1 (8) of the Federal Private Sector and sections 4.3.4 and 4.7.2 of Schedule 1 of the Federal Private Sector Act.

Type of data	*Personal content*									
Business to Business (B2B)	1	2	3	4	5	6	7	8	9	10
GVC data	X									
Engineering (M2M)				X						
IoT (M2M					X					
Financial/human resources								X		
Business to Consumer (B2C)										
Media							X			
Consumer								X		
Services (e.g. health, financial)								X		
Government to Citizen (G2C)										
Services (e.g. health, tax, identity, social-welfare protection)										X
IoT (e.g. metro, CCTV)										X
Citizen to Citizen (C2C)										
Social media										X
Communication (e.g. e-mail, messages, voice)										X

What is data processing?

Processing is not specifically defined in federal privacy legislation but, in practice, it includes the collection, use, analysis, modification, storage, disclosure or destruction of personal information.

Processing of personal data is not necessarily computerized: paper files and other communication media are also involved and must be protected under the same conditions. Data processing must have a specific purpose prior to the collection and use of the data.

What is a privacy policy?

A privacy policy is a document containing the various measures and rules adopted by an organization or company to ensure the security and appropriate use of data collected in the relationship between the said organization or company and a natural person using its services. In particular, the confidentiality policy shall include information on how the data are collected, stored and used by the concerned organization or company and how they are transmitted to third parties, where appropriate.

2 - State of Data Law in the Quebec and Federal Context

Canadian privacy law in Canada is plural, as both the provinces and the federal government have legislated in this area. In the private sector, the following laws exist:

- Personal Information Protection and Electronic Documents Act (Federal)
- Act respecting the protection of personal information in the private sector (Quebec)
- Personal Information Protection Act (Alberta)
- Personal Information Protection Act (British Columbia)
- General laws that contain specific provisions on data protection, for example in medical law.

While the following laws concern the public sector:

- *Privacy Act (Federal)*
- *Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information (Quebec)*
- *Freedom of Information and Protection of Privacy Act (Alberta)*
- *Freedom of Information and Protection of Privacy Act (British Columbia)*
- *Freedom of Information and Protection of Privacy Act (Ontario)*
- *Right to Information and Protection of Privacy Act (New Brunswick)*
- *Access to Information and Protection of Privacy Act (Newfoundland and Labrador)*
- *Freedom of Information and Protection of Privacy Act (Saskatchewan)*
- *The Freedom of Information and Protection of Privacy Act (Manitoba)*
- *Freedom of Information and Protection of Privacy Act (Nova Scotia)*
- *Freedom of Information and Protection of Privacy Act (Prince Edward Island)*

In order to present this legal framework in a way that is useful for the development of privacy policies, we have chosen to detail the fundamental legal principles of the protection of personal information as well as resulting individual rights by mainly studying the Quebec Private Sector Act and the Federal Private Sector Act. Indeed, there are normative invariants, namely equivalent principles, which produce the same effects, throughout this legislation and these will be identified in the context of developing privacy policies.

Application of Law:

Quebec's privacy laws are older and more comprehensive than federal laws. With a few exceptions, the Québec Private Sector Act takes precedence over the Federal Private Sector Act in Québec[8]. In the course of our analysis, we did not study the Alberta and British Columbia statutes, which also take precedence over the federal legislation, because of the invariants in all of these statutes and their qualification as substantially similar to the federal Private Sector Act by the Office of the Privacy Commissioner of Canada.

Quebec

The Quebec Private Sector Act is a law that applies to personal information that a private enterprise, whose activities take place entirely in Québec, collects, holds, uses or communicates with third parties, regardless of the nature of the medium and the form in which it is accessible: written, graphic, sound or visual, computerized or otherwise. However, it does not apply to the collection, possession, use, or disclosure of communication of journalistic, historical or genealogical material for the legitimate purpose of informing the public.

With respect to non-profit organizations (NPOs), the Quebec Private Sector Act applies[9] in that they carry on "*an organized economic activity, whether or not it is of a commercial nature*[10] .

The *Act Respecting Access to Documents held by Public Bodies and the Protection of Personal Information* (hereinafter the "Québec Public Sector Act") is a law that applies to documents held by a Quebec public body in the performance of its duties, whether their conservation is ensured by the public body or by a third party. It applies regardless of the form of such documents: written, graphic, sound, visual, computerized or other.

[8] Organizations in the Province of Quebec Exemption Order (DORS/2003-374)
[9] Quebec Private Sector Act, Section 1
[10] CCQ, Section 1525

Federal

The Federal Private Sector Act is a law that applies to any organization that collects, uses or discloses personal information in the course of commercial activities, excluding federal government institutions subject to the *Privacy Act* (hereinafter referred to as the "*Federal Public Sector Act*"). Organizations whose data processing is carried out in Quebec, Alberta or British Columbia are exempted from the application of the federal Private Sector Act because provincial laws supersede it. The Act does not apply to personal information collected, used or disclosed by an organization for strictly journalistic, artistic or literary purposes.

The Federal Public Sector Act is intended to apply to federal public sector organizations and governs the collection, use and disclosure of personal information by the government in the course of providing services. However, this Act does not apply to Synapse C, nor to the organizations whose data it wishes to share and enhance. In theory, not-for-profit organizations are not subject to the Federal Private Sector Act. However, the federal law applies to NPOs, with the exception of NPOs in the provinces of Quebec, Alberta and British Columbia, that collect, use or disclose personal information in the course of commercial activities. Upon reading the information transmitted by Synapse C, provincial NPOs, with the exception of NPOs in the provinces of Quebec, Alberta and British Columbia, whose data will be shared and enhanced, mainly collect personal information in the course of their commercial activities, which does not exempt them from their obligations under the Federal Private Sector Act. Indeed, the Act defines commercial activity as "any particular transaction, act or conduct, or any regular course of conduct that is of a commercial nature, including the selling, bartering or leasing of donor, membership or other fundraising lists."

Throughout the drafting of this guide to best practices, we have chosen to base ourselves primarily on Quebec law, whose obligations are more comprehensive than federal law, which implies that any Canadian organization[11] complying with the obligations of Quebec law will be in compliance with federal law. Indeed, because of the invariance of the principles and obligations relating to the protection of personal information, the Quebec law has been deemed substantially similar[12] by the Office of the Privacy Commissioner of Canada.

[11] With the exception of agencies in the provinces of Alberta and British Columbia whose legislation we have not reviewed

[12] Substantially similar legislation provides a privacy protection mechanism that is consistent and equivalent to that of the Federal Private Sector Act, incorporates the ten principles of Schedule 1 of the Federal Private Sector Act, provide an independent and effective oversight and redress mechanism and investigative powers,

Key principles that must apply to any processing of personal information:

Transparency: Consistent with the principle of transparency, privacy legislation requires organizations to document and make available to individuals, in clear and comprehensible language, specific information about their policies and practices relating to the management of personal information.

Quebec laws specify which information must be provided in the context of the collection of personal information by a public body[13] and in the context of the creation of a file on a person in the private sector[14].

- **The legal basis for any processing of personal information**: Organizations must obtain consent for the collection, use and disclosure of personal information, subject to limited exceptions. For consent to be valid, it must be clear, free, and informed, and given for specific purposes[15]. It must, therefore, be reasonably expected that the individuals concerned understand the nature, purpose, and consequences of the collection, use, or disclosure of personal information to which they have consented. An organization shall not, as a condition of the supply of a product or service, require consent beyond that which is required to fulfill an explicitly specified and legitimate purpose. The form of consent (explicit or implicit) may vary depending on the nature of the information and the reasonable expectations of the individual. Individuals may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. Federal law provides a general obligation that personal information must be collected by fair and lawful means: consent must not be obtained through deception, coercion or deceptive practices. Even with valid consent, organizations are subject to a general legal requirement that personal information be collected, used, and disclosed only for purposes that a reasonable person would consider appropriate in the circumstances.

and restrict the collection, use and disclosure of personal information to purposes that are appropriate and legitimate.

[13] Quebec Public Sector Act, section 65.

[14] Quebec Private Sector Act, section 8.

[15] Quebec Private Sector Act, section 14.

Purpose limitation: Organizations are generally required to identify the purposes for which personal information is collected at or before the time of collection[16]. Organizations must also document these purposes in accordance with the Transparency Principle.

The requirement to identify the purposes for which personal information is collected will subsequently:

- delineate the type and amount of personal information to be collected;
- inform the individual of the purposes for which the information is being collected;
- determine the security measures to be adopted to ensure the protection of personal information;
- determine how often the information should be updated;
- limit the use of personal information; and
- determine when the information is to be destroyed.

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law.

- **The Limiting Collection Principle**: Quebec's laws[17] on the protection of personal information generally require that the collection, use and disclosure of personal information be limited (both in nature and in volume) to the extent that it is necessary to fulfill the purposes identified by the organization. Personal information shall be retained no longer than necessary for the fulfillment of those purposes.

- **The Principle of Proportionality:** Quebec's privacy laws generally state that the overriding obligation that organizations may collect, use and disclose personal information are only for purposes that a reasonable person would consider appropriate in the circumstances. The principle of proportionality is also incorporated into some of the other principles. For example, the retention obligation imposed on organizations is proportional to the level of sensitivity of the personal information; the more sensitive the personal information, the greater the level of protection required[18]. Similarly, the extent to which personal information must be accurate, complete, and up-to-date will depend upon its intended use, taking into account the interests of the individual.

[16] Quebec Private Sector Act, sections 4 and 5, Quebec Public Sector Act, section 65.
[17] Quebec Private Sector Act, section. 5, Quebec Public Sector Act, section. 64.
[18] Quebec Private Sector Act, section 10, Quebec Public Sector Act, section 63.1.

- **Limiting use, disclosure and retention**: Consistent with the necessity principle, Quebec's privacy laws[19] generally require organizations to retain personal information only as long as necessary to fulfill the purposes for which it was collected, subject to a valid legal requirement.

  Personal information that is no longer necessary for the identified purposes should be destroyed, erased, or made anonymous.

  Organizations should develop guidelines and implement procedures for the retention of personal data, including minimum and maximum retention periods and procedures governing the destruction of data.

- **Accountability:** Privacy legislation[20] reflects the key principle of accountability. Organizations are responsible for the protection of personal information under their control, including personal information that they transfer to third parties for processing, for which they must provide a comparable level of protection by contractual or other means.
  Organizations must designate and identify an individual who is accountable for the organization's compliance with other privacy principles and must implement policies and practices to give effect to those principles.

- **Safeguards:** Each of the Quebec[21] and federal laws[22] on the protection of personal information contains specific provisions on the protection of these. Essentially, these provisions require organizations to implement reasonable technical, physical, and administrative measures to protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, modification or destruction. In Québec in particular, each organization is responsible for ensuring the confidentiality of the personal information it holds. To this end, it must designate a responsible representative for access to documents and the protection of personal information, whose identity must be disclosed to the *Commission d'Accès à l'Information.*

- **Accuracy**: Organizations are required to ensure that the personal information in their records is accurate, complete, and up-to-date, particularly when the information is used to

[19] Quebec Private Sector Act, sections 12 and 36. Quebec Public Sector Act, section 52.1.
[20] Québec Public Sector Act, section 8. Québec Private Sector Act, section 91.
[21] Quebec Private Sector Act, section 10. Quebec Public Sector Act, section. 63.1.
[22] Federal Private Sector Act, section 5.

make a decision about the individual to whom it relates or is likely to be disclosed to another organization[23].

Individual rights to be guaranteed when processing personal information:

It goes without saying that the organization collecting personal information has an obligation to adequately inform the individual concerned before providing it. Once this obligation is fulfilled by the organization, the organization may be faced with a variety of rights that the individual may wish to exercise:

- **Right of access to data/copies of personal information**: Organizations shall, upon request and subject to limited exceptions, inform individuals of the existence, use, and disclosure of their personal information and shall give them access to that information, including a list of third-party organizations to which the information has been disclosed[24].

  The right of access does not require an organization to provide copies of records of personal information; rather, it requires the providing of access, which may include the consultation of files in the organization's offices. In general, an individual's request should be sufficiently specific to allow an organization to identify relevant records. The organization must respond within a prescribed time or within a reasonable time, as the case may be, at minimal or no cost to the individual, and must make the information available in a clear and comprehensible form. Exceptions to the right of access vary from one statute to another and must be carefully considered. Examples of statutory exemptions include: information protected by solicitor-client or litigation privilege, confidential commercial information, information about another person, information relating to national security matters, and information obtained through a formal dispute resolution process.

- **Right to rectify errors**: The Quebec Private Sector Act[25] and the federal Private Sector Act[26] generally require that when an individual demonstrates the inaccuracy or

[23] Quebec Private Sector Act, section 11. Quebec Public Sector Act, section. 72.
[24] Quebec Private Sector Act, Sections 27 and 35. Quebec Public Sector Act, Sections 9 and 92

[25] Quebec Private Sector Act section 8. Quebec Public Sector Act, section 89.
[26] Federal Private Sector Act, Schedule, Ninth Principle

incompleteness of personal information held by an organization, the organization must correct the inaccuracies and/or add a note to the information, as appropriate.

- **Right to object to processing**: Although the federal Private Sector Act does not include a specific right to object to processing, the Quebec Private Sector Act[27] prohibits organizations from requiring, as a condition of the supply of a product or service, that individuals give their consent to the collection, use or disclosure of their personal information beyond what is necessary to achieve the legitimate and explicitly specified purpose. In addition, an individual must be able to withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. Upon receipt of any withdrawal, individuals must be informed of the consequences of such a withdrawal.

- **Right to Withdraw Consent**: An individual should be able to withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. Individuals must be informed of the consequences of such withdrawal.

- **Right to Object to Marketing**: Consent is required for the collection, use or disclosure of personal information for marketing purposes. The form of consent required will vary depending on the circumstances, the sensitivity of the information, and the reasonable expectations of the individual. Where opt-out consent is appropriate, individuals must be informed of the marketing purposes at or before the time of collection, and in a clear and understandable manner. Individuals must be able to withdraw easily from the practice; the withdrawal must be effective immediately and be persistent; and the information collected and used must be destroyed or effectively de-identified as soon as possible thereafter.

- **Right to complain to the appropriate privacy authority or authorities:** Individuals have the right to complain to the appropriate privacy authority or authorities. Before doing so, individuals must be able to raise privacy issues with the designated representative within the organization who is responsible for the organization's compliance. Organizations must have easily accessible and user-friendly procedures for responding to complaints or inquiries and must take steps to deal effectively with complaints accordingly.

[27] Quebec Private Sector Act, section 9.

3 - Transmission of Information to Third Parties

As part of its support mission, Synapse C is called upon to enhance the value of data from the organizations it supports in the Canadian cultural sector, notably through sharing or through various analyses. This data probably contains personal information. For this purpose, it is important for organizations to provide in their privacy policies the possibility of transmitting personal information to Synapse C for purposes defined by the organization, with the help of Synapse C.

Synapse C will be treated as a third party in terms of personal information protection. In order for the processing carried out by Synapse C on behalf of cultural organizations to be legal, it is essential that the transmission of data containing personal information follow the obligations contained in the law.

It seems relevant to recall here that any transmission of information outside Quebec or originating outside Quebec is subject to federal law.

In Quebec, it is possible to transfer personal information to third parties, provided that the consent of the person concerned is obtained or authorized by law[28]. The Private Sector Act provides some exceptions to the requirement to obtain the consent of the person concerned before transferring personal information to a third party[29]

Moreover, if personal information is communicated to a person or organization outside Quebec or entrusted to it for holding, use, or communication, the organization transmitting the information must first ensure that:

- the information will not be used for purposes not relevant to the subject of the file or communicated to third parties without the consent of the persons concerned[30]; and
- in the case of nominative lists, that the persons concerned have a valid opportunity to refuse the use of their personal information for purposes of commercial or philanthropic prospecting and to have this information removed from the list, if necessary.

If either of the two conditions is not met, the organization must refuse to disclose the personal information.

[28] Quebec Private Sector Act Sections 13 and 17
[29] Quebec Private Sector Act Sections 18, 18.1, 22, 23
[30] With the exception of the cases provided for in sections 18 and 23 of the Quebec Private Sector Act

At the federal level, organizations that disclose information containing personal information to third parties for processing purposes remain responsible for it. Moreover, they must ensure that the third party offers a degree of protection comparable to that of the organization[31].

In addition, organizations must notify consumers at the time of collection that their personal information may be processed in a foreign country[32].

4 - Towards Maximum Protection

Quebec and Canadian companies in the cultural sector, through their clientele, their potential subcontractors, or the processing of data from persons residing in the EU or California, may be subject to the European Union's General Regulation on Data Protection[33] (hereinafter "European Regulation") or the California Personal Data Protection Act[34]. Therefore, it is important to take into account certain principles resulting from these laws, in order to ensure better protection of personal data and peace of mind, especially when processing personal data of European or Californian residents. Moreover, although not explicitly stated in Quebec and federal laws today, certain rights guaranteed by the European Regulation and the California law could be incorporated into Quebec and/or federal law in the future, since the principles on which they are based are similar, and sometimes even identical.

This is the case, for example, of the right to data portability or the right to oblivion, both of which are enshrined in the European Regulation. The stated objective of the European legislator on these issues is to give individuals "control" over their data.

Right to data portability: Although Quebec and federal private sector legislation provides a right of access to personal information, it does not provide for the right to data portability. The right to portability provides individuals with the ability to retrieve a portion of their data in an open, machine-readable format. This allows them to easily store or transmit data from one information system to another for re-use for personal purposes.

[31] Federal Private Sector Act, section 4.1.3
[32] Guidelines on Transborder Processing of Personal Data
[33] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of April 27th 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, may 4th 2016.
[34] California Consumer Protection Act of 2018, No. 17-0039

Right to erasure / right to oblivion: Although laws give individuals the right to withdraw their consent and challenge the accuracy, completeness, and currency of their personal information, they do not grant a specific right to require organizations to "erase" or delete their personal information per se.

Reuse of Data:

Theoretically, data is a form of capital that cannot be depleted and can be reused for unlimited purposes. Its reuse throughout the economy has beneficial impacts, as data can potentially be reused to open up significant opportunities for growth or to generate benefits in ways that were not foreseeable when the data were created. This underscores the role of data as a key infrastructure for the knowledge economies of the 21st century, an infrastructure to which access will be a critical social and economic policy issue.

Despite growing evidence of its economic and social benefits, the reuse of data across organizations, sectors, and countries remains below its potential, as individuals, businesses, and governments often face barriers to data reuse that can be compounded by a reluctance to share. The social and economic risks associated with the possible disclosure of confidential information (i.e. certain personal data and trade secrets) are often cited as the main reason for this reluctance .

Improving data access is seen as an effective way to maximize the social and economic value of data, while addressing the risks and challenges associated with data access and reuse. For this reason, it is important that organizations that have privacy policies in place and who would like third party companies such as Synapse C to analyze this data to improve efficiency and synergies in the cultural sector in Montreal, Quebec, and Canada, should consider allowing the transfer of data to these third parties in their privacy policies.

5 - Recommendations

It is recommended that organizations, including third party companies such as Synapse C, wishing to process data for the purpose of improving data collection and analysis in the Canadian cultural sector, follow these recommendations when collecting, using, and disclosing personal information, as well as when requesting access to personal information.

As previously mentioned, most of these recommendations are drawn from the Quebec Private Sector Act which, while substantially similar to federal legislation, is more protective of personal information. It would appear, however, that there is an interesting exception to Synapse C, regarding the transmission of information to third parties[35].

In addition, before mentioning the various recommendations, we would like to draw the attention of the readers of this guide to best practices to the fact that it is strongly recommended not to use or disclose previously collected personal information at the risk of violating the various privacy laws. The only instances where organizations could continue to process personal data collected in the past would be where previous privacy policies already allowed it.

Here are ten principles taken from Schedule I of the federal Private Sector Act, taken and distilled into Quebec legislation, which will enable organizations and suppliers such as Synapse C to have a broader understanding of their **obligations regarding the personal information** they may collect in the course of their activities:

1. The organization is responsible for the personal information it manages. It must appoint a person responsible for compliance.

2. The organization must identify the purposes (objectives) for the collection of the information prior to and throughout the collection process. Personal information shall not be collected for any purpose other than those purposes.

[35] If Synapse C receives information from third parties in other provinces, these organizations will be as responsible as Synapse C for the personal information and must ensure that Synapse C provides at least equal protection to the organizations. When information containing personal information is sent by Synapse C to third parties outside Quebec, Synapse C will also have to ensure that the protection of personal information provided by the third parties is at least comparable to that offered by Synapse C, which will otherwise remain responsible for the personal information transmitted to the third parties.

3. The organization will obtain the consent of any individual for the collection, use and/or disclosure of personal information about him or her.

4. The collection shall be fair and lawful.

5. The use, disclosure, and retention of personal information will be limited

6. The personal information collected must be as accurate and up-to-date as possible.

7. Personal information collected shall be secured according to the sensitivity of the information.

8. Information about the organization's policies and practices relating to its management of personal information shall be readily available to the public.

9. Access to personal information shall be available to any person who requests it. The use to which it is put and whether it has been disclosed to third parties must also be disclosed. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. An individual shall be able to address a complaint concerning an organization's compliance with the above principles. The complaint must be addressed to the Chief Compliance Officer (c.f. Principle 1).

With regard to the subject that interests us more specifically, the *Commission d'accès à l'information du Québec* has published a *Guide en matière de protection des renseignements personnels dans le développement des systèmes d'information*[36] in which it has given several pieces of advice **to improve online privacy policies and the transparency of personal information collection and privacy protection practices** for organizations subject to the Quebec Act. In addition, the Office of the Privacy Commissioner of Canada has also issued similar recommendations. In our view, this guidance is intended to apply more broadly to the various

[36] Government of Quebec, 2002, updated in 2015, online : http://www.cai.gouv.qc.ca/documents/CAI_G_dev_syst_info_pub.pdf

entities collecting personal data in the cultural sector. In addition, we encourage organizations to consider adopting standardized privacy policies that are easy for everyone to understand.

1. Have a privacy policy that is appropriate to the activities of the cultural sector:

    a. While the privacy policies of other organizations may be useful as a reference, avoide the copy/paste of existing models of companies operating in a different sector
    b. Describe the type of personal information collected by the entity.

2. Be accurate and transmit useful information:
    a. No superfluous or vague terms;
    b. Clearly identify what personal information is being collected and for what purpose; and
    c. Clearly indicate whether the personal information collected is transferred to third parties, who the third parties are, and what services they provide that require the transfer of the personal information.

3. Do not only mention that cookies are used:

    a. Explain how cookies work (data collected) and how they are used/disclosed to third parties; and
    b. Also provide information on in-store practices.

4. Presenting the privacy options available to customers, users or other affected individuals:
    a. Inform customers, users or other affected individuals of the entity's options regarding the collection, use or disclosure of their information (e.g., opt-out of having their personal information used for marketing purposes); and
    b. Clearly explain how they can exercise the choices available to them.

5. Explain how to access the personal information held by the institution:
    a. Allow customers, users or other affected persons to request correction or deletion of such information.

6. Regularly update information regarding the protection of personal information:

a. Ensure that the Privacy Policy and other notices reflect the entity's current privacy management practices, especially when new processing occurs or new data are collected;
b. Ensure that information is updated as soon as a change occurs;
c. Indicate the date of the last update/amendment of the Privacy Policy; and
d. Archive previous versions of the Privacy Policy.

7. Provide contact information for the entity:
    a. Facilitate communication with the entity, at a minimum through an email address;
    b. Suggest several ways to contact the entity regarding privacy/privacy issues; and
    c. Make such information available at locations other than the Privacy Policy only.

8. Ensuring that privacy information is visible and easily accessible:
    a. Place an access link to the Privacy Policy in a prominent place on the home page;
    b. Suggest additional information points when a client has to make a decision that will impact on his or her privacy / personal information; and
    c. Highlight key information in the privacy policy.

9. Use plain language.

10. Structure the privacy policy in a way that facilitates consultation by users.

While this may seem logical, it seems worth emphasizing that the collection, processing, and transfer of personal information for the following purposes is prohibited:

- collecting, using or disclosing personal information in an unlawful manner or by committing unlawful acts;
- profiling (categorization/sorting) of individuals in a manner that allows for unfair, unethical or discriminatory treatment;
- collecting, using or disclosing personal information that would indicate intent or cause serious harm to an individual; and
- publishing personal information with the intent to coerce the individual afterwards.

In conclusion, Synapse C informed the Cyberjustice Laboratory of its desire to have informed consent from users or clients of the organizations. Indeed, consent is essential when collecting personal information from individuals. In principle, **consent to the collection, communication or use of personal information** must be clear, free, informed, and given for specific purposes[37]. This is a key value of Quebec and federal legislation on the subject.

Here are seven principles, jointly produced by the Office of the Privacy Commissioner of Canada and the Offices of the Information and Privacy Commissioners of Alberta and British Columbia, to ensure that organizations obtain meaningful consent during the collection, use, and disclosure of personal information:

1. Emphasize key elements of the collection, use, and disclosure of personal information to third parties. Information must be clear, easily accessible, and not overload, which could result in the loss of the user. The person giving consent must understand the nature, purposes, and consequences of what they are consenting to.
   In order for consent to be considered valid, or meaningful, organizations must inform individuals of their privacy practices in a comprehensive and understandable manner. Organizations must allow individuals to quickly review key elements impacting their privacy decisions right up front as they are considering using the service or product on offer, making the purchase, or downloading the app, etc. The following are key elements that organizations should communicate to individuals:

   - What information is being collected
   - With which parties personal information is being shared
   - For what purposes personal information is collected, used or disclosed
   - Risk of harm and other consequences

2. Information must be provided to individuals in manageable and easily-accessible ways (potentially through hyperlinks providing increasingly precise information) and individuals should be able to control how much more detail they wish to obtain, and when.

[37] Quebec Private Sector Act, section 14.

3. Individuals cannot be required to consent to the collection, use or disclosure of personal information beyond what is necessary to provide the product or service – they must be given a choice. These choices must be explained clearly and made easily accessible. Collections, uses or disclosures of personal information over which the individual cannot assert any control (other than to not use a product or service) are called conditions of service. For a collection, use or disclosure to be a valid condition of service, it must be integral to the provision of that product or service such that it is required to fulfill its explicitly specified and legitimate purpose. Organizations should be transparent and prepared to explain why any given collection, use or disclosure is a condition of service, particularly if it is not obvious.

4. When seeking consent online, organizations should do more than simply transpose in digital form their paper-based policies from the offline environment. The digital environment is dynamic in nature, and its capabilities should be considered and harnessed. Organizations are encouraged to use a variety of communications strategies – including “just-in-time” notices, interactive tools, and customized mobile interfaces – to explain their privacy practices.

5. Have a graphical user interface so that receiving information is simple and understandable. In particular, it is not recommended to segment the information too much, resulting in an unnavigable informational maze for the Internet user.

6. Make consent a dynamic and continuous process by ensuring that it occurs at several points in time. This can be done through regularly updated frequently asked questions, periodic reminders to individuals or by using new technologies such as chatbot.

7. Demonstrate accountability by being in a position to demonstrate compliance with the validity of a user's consent at any time.

In addition, Synapse C will need to ensure that the organizations whose data it would like to collect clearly indicate in their privacy policies what types of data containing personal information will be shared with Synapse C and for what purposes.

Finally, the creation of a privacy policy is only a first step in bringing cultural organizations into compliance with the various privacy laws, as well as the possibility of cultural data being

transferred to Synapse C. As a next step, it will be necessary for these organizations to have additional policies, including data security and archiving.

If Synapse C has the need and IVADO is supportive of it, the Cyberjustice Laboratory is competent to draw up such best practice guides on data security and archiving.

[i] This Guide is for information purposes only and does not constitute legal advice or opinion. You may contact the Cyberjustice Laboratory team for any additional information or questions or to obtain personalized advice.