BILL 64 Vs GDPR

Comparison of protection measures for personal information in the private sector.

Overview table of Bill 64 and GDPR

Prudence AI Inc.

Multidisciplinary law firm in AI, Data protection Risk Analysis, Privacy and confidentiality, AI ethics and cybersecurity.

We help organizations or all sizes to develop, implant or use solutions that are AI responsible. We also have extensive experience in the healthcare sector.

Hitachi Systems Security Inc.

Hitachi Systems Security Inc. is a global provide of privacy and security services since 1999.

HISYS-SEC's mission is to support the trust in the digital economy by developing solutions in Privacy+Security. Our team of experts helps our clients in more than 50 countries, 24 hours a day and 7 days a week.

		Québec **Bill 64 ACT RESPECTING THE PROTECTION OF PERSONAL INFORMATION IN THE PRIVATE SECTOR (ARPPIPS)**	European Union **General data protection regulation (GDPR)**
1. Scope	1.1. temporal	The reviewing of the bill will take place in the fall.	It is fully applicable since the 25th of May 2018
	1.2. Territorial	On all of Quebec territory: ● Applicable to all private sector: Any enterprise which collects, stores, uses or transmits personal information. ● Applicable to the public sector ● Applicable to political parties	Applicable to the public and private sector. Criterion of establishment : Data processor and Data subcontractor established in the EU, or the EEA Targeting criteria: DP and DS are established outside EU/EEA but their processing activities are linked to: * the offer of goods and services to concerned individuals in the EU, payment being required from the individuals or not; or *the tracking of these individuals, if the behavior takes place inside the EU.
	1.3. Material	- The scope for enterprises is unchanged. Specifics: - The targeted personal information includes those collected by the enterprise, even if storage is done by third-party. - The ARPPIPS will not be applied to “personal information concerning the performance of duties within an enterprise by the person concerned, such as the person’s name, title and duties, as well as the address, email address and telephone number of the person’s place of work.”	Applicable to personal information processing, automated or not or in part, as much as to non-automated personal data which is to be part of a file. Not applicable - To processing done in the context of a strictly personal or domestic activity (personal shopping, personal finance management). - To anonymized information

2. **Definitions**	2.1. Personal information	Personal information is any information which relates to a natural person and allows that person to be identified. Whatever support or format is being used. Targets also employees and applicants to a job. Business coordinates are excluded from the laws' scope.	"Personal data" are defined as any information relating to an identified or identifiable natural person ('data subject'). an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
	2.2. Processing	Bill 64 refers mostly to the notion of "collection". However in its explanatory notes, it is stressed that a particular attention was paid to "any information system project or electronic service delivery project involving **the collection, use, release, keeping or destruction of personal information**"	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
3. **Data processing general framework**	3.1. Great principles pertaining to personal information processing	Two great principles, set out in the Bill's preamble, govern the text: - Enhanced confidentiality is put at the heart of people's privacy. - A stricter approach to obtaining consent, central to any personal data processing	The data must be: - Processed in a lawful, loyal and transparent manner with respect to the concerned individual; - Collected for limited, strictly defined purposes (i.e. predetermined, lawful and express); - Adequate, relevant and limited to what is necessary with regard the purposes (principle of data minimization); - Exact, and if necessary, up to date; - Stored during a period not exceeding what is necessary with regard to the purposes; - processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage,
	3.2. Privacy by design and by default	The highest level of privacy must be ensured by default (Privacy by default), without any intervention by the concerned individual.	Implementation of means of privacy protection from the determination and creation of processing and by default.

		The data protection representative must be consulted at the beginning of the project and can intervene at any moment to suggest personal data protection measures.	
4. Legal grounds justifying the lawfulness of personal data processing	4.1. Consent	Consent must be clear, free and informed and be given for specific purposes. It is request for each purpose, in simple and clear terms, distinct from other communicated information communicated to the concerned individual. If the person concerned so requests, assistance is provided to help him understand the scope of the consent requested. Consent is not necessary - if it is used for purposes consistent with the purposes for which it was collected; - if it is clearly used for the benefit of the person concerned - if its use is necessary for study or research purposes or for the production of statistics, and the information is de-identified. Consent collection is not necessary for concluding a commercial transaction to which a person carrying on an enterprise intends to be a party, the person may communicate such information, without the consent of the person concerned, to the other party to the transaction	Consent is one of the 6 legal grounds allowing for the justification of the personal data of a concerned individual. Consent must be freely given, specific, informed and unambiguous, given in an understanding and accessible manner and is only valid for the specific purpose it was given for. It must be unambiguous for certain categories and withdrawable at any moment.
	4.2. Consent of the minor:	Age of consent of the minor: 14 years old. Before 13 years old, it is necessary to obtain the consent of the person having custody of the child, unless the data processing is manifestly in the minor's benefit.	Minimum age of 16 for minor consent, unless the custody holder gives his/her authorization Member States may provide for a lower age by national law, provided that such age is not below the age of 13 years

	4.3. Other legal grounds for processing	The personal data processing without consent is authorized for the performance of a contract.	Without consent, only 5 other legal grounds justify the processing of personal data: **The existence of a legal obligation** **The execution of a contract of precontractual clauses** **The protection of the concerned individual vital interests** **The execution of important reasons of public interest or incumbent under public authority.** **The legitimate interest pursued by the data processor**
5. Sensitive information	5.1. Definition of sensitive information	“personal information is sensitive if, due to its nature or the context of its use or release, it entails a high level of reasonable expectation of privacy” “.	personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
	5.2. Operating regime	“Such consent must be given expressly when it concerns sensitive personal information.” Thus, as soon as a personal information is deemed sensitive, the express consent is required	Ban on sensitive personal information processing Exception: processing is possible if: ➢ Consent, explicit of concerned individual; ➢ processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law ➢ processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent ➢ processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

			➢ processing relates to personal data which are manifestly made public by the data subject ➢ processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity ➢ processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued ➢ processing is necessary for the purposes of preventive or occupational medicine; ➢ processing is necessary for reasons of public interest in the area of public health ➢ processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
	5.3. Personal data related to criminal convictions and offences are processed	Processing possible if explicit consent	Processing possible if done under the supervision of a public authority
6. Rights of individuals	6.1. Transparency and information	Obligatory information of individuals: - Policies available on the organization's website - Concerned individual's information during the collection of personal information	Right to be informed on personal data processing, the collection must be done directly or indirectly from the concerned individual.
	6.2. Right to data	- Right to access - Right to deletion - Right to rectification - Right to notification of personal data transfer - Right to de-indexation	Right of access Right to rectification Right to erasure Right to treatment limitation Right to portability Right of opposition Right not to be subject to a decision based solely on automated means, including profiling, producing legal effects or similar

7. **Role associated to the compliance management**	7.1. Data controller	No definition of data controller; “Any person carrying on an enterprise is responsible for protecting the personal information held by the person.” “The person exercising the highest authority within a public body shall see to ensuring that this Act is implemented and complied with within the body.” “ Possible division of responsibilities in processing between the function of: person in charge of access to documents **person in charge of the protection of personal information.** the person responsible for information security the person responsible for document management.	Data controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data The data controller is responsible for compliance with GDPR and must be capable of demonstrating that the GDPR is being respected (accountability principle) **Joint responsibility:** Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.
	7.2. Subcontractor	No mention/specific obligation	natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; the controller must verify that the processor implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk the processing done by the processor must be regulated by a contract. The processing can be held liable if in breach of contract and violation of data protection statute.

	7.3. Data protection officer	The function of data protection officer (person in charge of the protection of personal information) is done by the highest-ranked individual in the enterprise. This function may be delegated in writing, in part of completely, to a personnel member	The data protection officer is the moral or physical person in charge of GDPR compliance within the organization that designated him or her, in charge of all data processing within the organization
8. Compliance management measures	8.1. Registry keeping	Registry only confidentiality incidents, (public or private)	The controller must keep a registry of data processing activities done under his/her responsibility. The processor must also keep a registry of all processing activities done in the name of the controller
	8.2. Data protection impact assessment /assessment of the privacy-related factors of any information system project or electronic service delivery project	**Assessment of the privacy-related factors** Obligatory for the introduction of any information system project or service delivery project or of the transfer of communication outside of Quebec.	The data controller has the obligation to do a Data protection impact assessment if the data processing could result in a high risk to the rights and freedoms of natural persons.
9. Security of personal data	9.1. Security obligation	Establishing the security measures necessary to ensure the protection of the personal information collected, used, communicated, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored.	The controller and the processor have the obligation to implement the appropriate technical and organization measures to guarantee the security level adapted to the data processing risk.
	9.2. Breach of data/ Confidentiality incident	In case of confidentiality incident presenting a risk of serious injury, the enterprise has the obligation of notifying promptly: - The CAI - Any person whose personal information is concerned - any person or body that could reduce the risk. The enterprise must maintain a register of confidentiality incidents and transmit it to the CAI on request.	In case of a data breach: ● Obligation to notify, within 72 hours, the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. ● Obligation to notify the concerned individual of data breach as soon as possible, if it is likely to result in a risk to the rights and freedoms of natural persons.

10. **International transfers**		An enterprise must conduct an assessment of privacy-related factors in case of data transfer outside of Quebec (see above). During this assessment, the *equivalence* must be established and the processing must be based the subject of a written agreement that takes into account, in particular, the results of the assessment and, if applicable, the terms agreed on to mitigate the risks identified in the assessment. The government will publish in the Gazette officielle du Québec a list of States whose legal framework governing personal information is equivalent to the personal information protection principles applicable in Québec.	The personal data transfers outside the borders of the EU are possible under the condition that appropriate safeguards be put in place to ensure the security of transfer: - Existence of a decision of adequation of the European Commission for the country to which the transfer will be made - The establishment of appropriate safeguards such as Corporate binding rules or standard contractual clauses between agencies...
11. **Controls and Sanctions**	11.1. Responsible authority	The Commission d'acces a l'information du Quebec (CAI) with reinforced powers. Examples: - Possible to deliver opinions of non-compliance. In case of notification of confidentiality incident, possible to order measures destined to protection of concerned individuals such as the delivery of personal information or destruction of personal information.	European level: European data protection board (EDPB) National level: National supervisory authorities of the EU Member States Missions to inform, protect, accompany, advise, control, sanction, anticipate... Examples of powers: - Investigation powers - Serious warning of the organization when the processing activities have had breach consequences at the GDPR - Impose temporary or definite temporary limits, including a ban, to processing Etc .
	11.2. Cooperation with supervisory authority	No mention/specific obligation	Controller and processor must cooperate with supervisory authority, upon request, with the execution of the supervisory authority.

	11.3. Administrative sanctions	**Financial administrative sanctions:** 50 000$ for a physical person 10 000 000$ for an organization or 2% of global turnover of the past year, if that amount is higher.	**Administrative sanctions**: administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, or € 20 millions or 4% of global turnover (whichever amount is highest).
	11.4. Civil or criminal fines	50 000$ in the case of natural persons 25 000 000$ or, if greater, the amount corresponding to 4% of worldwide turnover for the preceding fiscal year. In case of renewed breaches, the fines are doubled.	A person who has suffered moral or material harm has the right to be compensated for the damage caused. Member States shall lay down the rules on other penalties applicable to infringements of the GDPR.