Dialogue

Privacy Impact Assessment Operating Guideline

Version: 2
Date of last revision: August 1, 2024
Effective Date: August 1, 2024

CONFIDENTIAL

1. Objective

1.1 Dialogue) is responsible for ensuring that Personal Information in its custody or control is Processed in accordance with Applicable Privacy Legislation. This includes ensuring that any Processing Activity respects the rights and interests of individuals to whom such information relates, in particular by identifying, assessing and mitigating any potential privacy impacts throughout the Processing Activity's design, development and implementation, as appropriate. This assessment is more commonly referred to as a "Privacy Impact Assessment" or "PIA", and represents a risk management and accountability tool, helping Dialogue comply with Applicable Privacy Legislation and demonstrate its commitment to handling Personal Information in accordance with such laws. In some cases, Dialogue may also be required to conduct a PIA in situations specified under Applicable Privacy Legislation, as further detailed below.

1.2 This Privacy Impact Assessment Operating Guideline applies to any Dialogue Agent who is responsible for, or otherwise involved in, a Processing Activity, and describes whether and, if so, how to carry out a PIA. This Operating Guideline may be supplemented or superseded from time to time by any specific and valid procedures governing a given Processing Activity or operation.

2. Definitions

2.1 Refer to Appendix A of the Internal Privacy Policy for the Glossary of Terms.

3. Roles and Responsibilities

3.1 The Privacy Officer is responsible for the implementation and revision of this Operating Guideline.

3.2 Dialogue Agents are required to adhere to this Operating Guideline.

3.3 The Dialogue Agent leading any prospective or update to a Processing Activity is accountable and responsible for conducting any required PIA.

4. Details

4.1 Determining Whether to Conduct a PIA

4.1.1 A PIA must be carried out whenever a new or substantially modified Processing Activity is likely to create a **risk to the privacy interests of individuals**, in particular by taking into account the nature, scope, context and purposes of Processing. To determine whether the Processing Activity is likely to create such risk, the Dialogue Agent leading the Processing Activity must complete the Privacy Impact Assessment Intake Form and return it to the Privacy Officer for review and confirmation. If the Processing Activity is deemed to meet this risk threshold, the Dialogue Agent leading the Processing Activity must carry out a PIA in accordance

with the steps outlined in section 4.2 of this Operating Guideline and, where appropriate, consult with the Privacy Officer, Legal & Compliance Department, and IT Security Department (and where the Processing of Personal Health Information is involved, the Medical Director (and/or lead Custodian). The PIA should generally be conducted as early as possible in the design and development phase of the Processing Activity to avoid creating unnecessary delays or costs during its implementation phase.

4.1.2 If the Processing Activity involves Personal Information about Quebec residents (or the Processing of Personal Information in the course of carrying on an enterprise in Quebec (whether or not it involves the Processing of Personal Information about Quebec residents), a PIA may also be required in any of the following situations, regardless of whether the Processing Activity presents a high risk to the privacy interests of individuals:

4.1.2.1 **Information System or Electronic Service Delivery System –** Whenever a project to acquire, develop or overhaul an information system or electronic service delivery system involves a collection, use, disclosure, retention or destruction of such Personal Information, regardless of the project's potential impact on the privacy of individuals. This includes projects involving third-party Service Providers and other third parties. The PIA must be carried out in a manner proportionate to the sensitivity of the Personal Information, the purposes for which it will be Processed, the quantity and distribution of the information and the medium on which it is stored.

4.1.2.2 **Transfers Outside Quebec –** Whenever such Personal Information is communicated outside Quebec. For example, this includes Personal Information shared with a third-party Service Provider in another jurisdiction or that is stored, accessed or otherwise Processed in another jurisdiction. This also technically includes transfers of Personal Information to other Canadian provinces. The PIA must consider the sensitivity of the Personal Information, the purposes for which it will be Processed, the protection measures in place, and the legal framework applicable in the recipient jurisdiction. When transferring or Processing Personal Information outside of Quebec, Dialogue must ensure that its written contracts take into account the results of any PIAs and applicable risk mitigation terms. The same applies where Dialogue entrusts a person or body outside Quebec with Processing Personal Information on its behalf.

4.1.2.3 **Disclosure for Study, Research or Statistical Purposes** – Whenever such Personal Information is disclosed without

consent to a third party wishing to use the information for study or research purposes or for the production of statistics.

4.1.3 Depending on the nature of the activity, a PIA may be required prior to any proposed new or update to a Processing Activity involving Personal Health Information. Dialogue Agents must contact the Privacy Officer to determine whether a PIA is required. Where a PIA is required, the relevant Health Services Provider (including lead Custodian) will be involved in ensuring that the proposed Processing Activity and related policies and procedures align with the Health Services Provider's professional and legal obligations. Where applicable, such as in the province of Alberta, Health Services Providers will review and endorse the PIA to ensure it meets privacy and security requirements under Applicable Privacy Legislation, including Provincial Health Privacy Legislation. For further details on the role of Health Services Providers in developing and submitting PIAs to privacy regulators, refer to the Custodian Manual.

4.1.4 To determine whether the Processing Activity falls within any of the aforementioned situations, the Dialogue Agent leading the Processing Activity must complete the Privacy Impact Assessment Intake Form and return the same to the Privacy Officer for review and confirmation. If the Processing Activity qualifies as a project to acquire, develop or overhaul an information system or electronic service delivery system, the Dialogue Agent leading the Processing Activity must carry out a PIA in accordance with the steps outlined in section 4.2 of this Operating Guideline and, in particular, consult the Privacy Officer from the outset of such project. The PIA must be conducted as early as possible in the design and development phase of the project to avoid creating unnecessary delays or costs during its implementation phase.

4.1.5 In all situations necessitating a PIA, the Dialogue Agent leading the Processing Activity must consult and cooperate with the Privacy Officer to establish a process for carrying out the PIA that complies with applicable legal requirements.

4.2 Conducting a PIA

4.2.1 The Dialogue Agent leading the Processing Activity or project is responsible for preparing and completing the PIA using the Privacy Impact Assessment (Template) in collaboration with the Privacy Officer, IT Security Department and, where appropriate, Legal & Compliance Department and Medical Director (and/or lead Custodian). Other departments and Dialogue Agents may also be called upon to participate in the conduct of the PIA and, therefore, they are required to assist in this process as necessary and appropriate in the circumstances.

4.2.2 The Privacy Impact Assessment (Template) must be completed in accordance with the following steps:

4.2.2.1 **Step one – Provide a description of the data processing operations and data flows.** The PIA should adequately describe the data processing operations involved, paying careful attention to the nature, scope, context and purposes of the activity or project involved. *This step should generally reflect the information provided in the* Privacy Impact Assessment Intake Form *as well as any additional information that may be relevant.*

4.2.2.2 **Step two – Assess and document the business case to ensure that it is reasonable and proportionate.** The PIA should document the overall business case and assess its necessity, effectiveness, proportionality and minimal intrusiveness so as to ensure that the Processing Activity is reasonable in the circumstances. *This step should generally reflect the information provided in the* Privacy Impact Assessment Intake Form *as well as any additional information that may be relevant.*

4.2.2.3 **Step three – Identify, assess and, if appropriate, mitigate any privacy risks related to the Processing Activity.** The PIA should describe the Processing Activity's level of compliance with relevant principles and requirements under Applicable Privacy Legislation and identify potential privacy risks. In turn, the level of risk should be assessed and, if appropriate, mitigated by implementing additional risk mitigation measures so as to ensure that the residual risk remains acceptable. The Privacy Officer must recommend Personal Information protection measures applicable to any proposed project.

4.2.2.4 **Step four – Assess acceptability of any residual risk and, if appropriate, consider additional risk mitigation strategies.** If there are any residual privacy risks that exist after having applied the aforementioned control measures, Dialogue should consider whether these residual risks are acceptable in the circumstances and, if not, consider implementing additional measures. Dialogue must be able to explain why it believes a particular residual risk is acceptable in the circumstances and must document the same in Part IV of the Privacy Impact Assessment (Template).

4.2.2.5 **Step five – Assign roles and responsibilities and establish appropriate deadlines for the implementation of measures**

identified in steps three and four. The PIA should establish an action plan and indicate which departments, Dialogue Agents or individuals are responsible for implementing certain risk mitigation measures identified in steps three and four. The PIA should also establish deadlines for the implementation of these measures. Once a measure is fully implemented, the PIA must be updated in order to reflect the same.

(a) Approval must be obtained from the Privacy Officer, Chief Technology Officer, and where applicable, the Medical Director (and/or lead Custodian) prior to officially launching the project or activity. Such approval may be conditional upon the implementation of all or only some of these risk mitigation measures, as deemed appropriate in the circumstances.

4.2.2.6 **Step six – Identify a role or function responsible for periodically reviewing and, if appropriate, updating the PIA.** The PIA must be periodically reviewed so as to reflect changes to the implementation status of any risk mitigation measure or to the underlying Processing Activity. Note that if there is a substantive change to the Processing Activity, it may necessitate the carrying out of a new PIA in accordance with this Operating Guideline. In any event, the PIA should clearly identify a role or function within Dialogue that is responsible for reviewing the same, no less than annually, and updating the PIA. If the role or function is someone other than the Privacy Officer, they should consult with the Privacy Officer (and Medical Director/lead Custodian) as appropriate.

4.3 Role and Responsibilities of Privacy Officer

4.3.1 Dialogue has designated the Privacy Officer to exercise the role and function of person in charge of the protection of Personal Information within its organization in accordance with the Dialogue Internal Privacy Policy. The Privacy Officer can be reached at privacy@dialogue.co.

4.3.2 In addition to any responsibilities assigned to them in this Operating Guideline or in any related policies or procedures, the Privacy Officer has the following responsibilities in respect of any PIA carried out in accordance with this Operating Guideline:

4.3.2.1 Receiving completed Privacy Impact Assessment Intake Form and confirming whether a PIA is required;

4.3.2.2 Participating in the design and elaboration of the PIA;

4.3.2.3 Proposing appropriate and relevant measures to help ensure the protection of Personal Information, such as:

(a) Appointment of a person to be responsible for implementing the Personal Information protection measures.

(b) Measures to protect the Personal Information in any document relating to the Processing Activity or project.

(c) Description of participants' responsibilities with regard to the protection of Personal Information.

(d) Training activities for participants on the protection of Personal Information.

4.3.3 Where appropriate, in the course of carrying out a PIA, engaging in consultations with Health Services Providers and relevant privacy regulators in respect of certain Processing Activities;

4.3.4 Reviewing all completed PIAs;

4.3.5 Submitting PIAs, when required, with the appropriate privacy regulator; and

4.3.6 Where appropriate, monitoring completed PIAs on a regular basis to ensure that measures are fully implemented and effective at reducing privacy risks. If necessary, the Privacy Officer may require additional measures to be implemented in respect of a particular Processing Activity, taking into account relevant changes, including any changes to Applicable Privacy Legislation that may affect the Processing Activity.

4.4 Timing of a PIA

4.4.1 Where a PIA is required to be conducted in accordance with this Operating Guideline, it must be carried out and completed before the official launch of the project, initiative, program or activity to which the PIA relates (or any material change and/or update thereto) and, in any event, no later than the time Personal Information is first Processed in connection therewith, unless otherwise authorized in writing by the Privacy Officer.

5. ENFORCEMENT

5.1 The Privacy Officer may audit at any time to ensure compliance with this Operating Guideline. Failure to report known violations of this Operating Guideline to the Privacy Officer is considered a violation of this Operating Guideline.

5.2 Dialogue Agents who violate this Operating Guideline may be subject to appropriate disciplinary action up to and including termination or termination of

contractual agreements, denial of access to information technology resources, and other actions as well as both civil and criminal penalties.

6. Questions and Complaints

6.1 Dialogue Agents are encouraged to submit any inquiries or complaints regarding this Operating Guideline to their manager or the Privacy Officer at privacy@dialogue.co.

Version History:

Version Number	Effective Date	Revision Date	Approval
1	August 1, 2022	August 1, 2022	Nathalie Delisle, Chief Privacy Officer Dr. Marc Robin, Medical Director
2	August 1, 2024	August 1, 2024	Dominique Payette, Privacy Officer