# Protection of Privacy Policy
## Questions and Answers
April 2020

To ensure compliance with applicable law and regulation, and to maintain the privacy of OLG's customers, OLG has created a new internal policy governing the handling of Personal Information in its custody and under its control. The *Protection of Privacy* policy (the "Policy") outlines requirements for all divisions at OLG and is consistent with the Enterprise Compliance Framework and the *Freedom of Information and Protection of Privacy Act* ("FIPPA").

## Questions and Answers

### 1. Who does the Policy apply to?

The Policy applies to all divisions and employees at OLG, including consultants hired by OLG. Furthermore, the policy identifies specific responsibilities for key roles throughout OLG, including divisional leaders, departmental managers and specific SME groups (such as the Privacy Office, Corporate Compliance and the Information Security Office [ISO]).

### 2. Have requirements changed significantly compared to previous policies?

The requirements in the Policy have been revised to encompass a wider range of topics and responsibilities. The Policy has been developed in alignment with the Enterprise Compliance Framework (ECF) to reflect its requirements. Managers should review the Policy to understand its requirements and consider whether the current practices of their teams and departments are aligned with the policy.

### 3. At a high level, what are the key requirements under the Policy?

The Policy includes several requirements, including the following:

- Divisions and/or departments must implement their own functional policies, procedures or controls to ensure compliance with FIPPA.
- Divisions and/or departments must engage the Privacy Office to complete Privacy Impact Assessments to identify and address privacy risks regarding significant projects and initiatives involving the collection/use/disclosure of Personal Information.
- Divisions and/or departments must obtain evidence that Service Providers and/or Vendors who collect/use/disclose OLG Personal Information do so in compliance with FIPPA.
- Divisions and/or departments must report and respond to privacy breaches in accordance with the Privacy Breach Response Protocol. Any information security incident must also promptly be reported to the ISO.
- Employees must keep physical records containing Personal Information confidential, including by securing physical records in a manner rendering them inaccessible to employees who do not require access.
- Completion of OLG's e-learning privacy training is mandatory for newly hired employees.

### 4. Do divisional leaders or managers have unique responsibilities for their team?

Under the Policy, OLG divisional leaders (on behalf of their respective divisions) own the risk of non-compliance with FIPPA and are responsible for supervising operations, including those conducted and managed by OLG. Divisional leaders are expected to:

- Conduct and manage, and where applicable, operate their business in compliance with FIPPA and ensure Service Providers and Vendors do the same;
- Align day-to-day operational practices with this policy and assign Regulatory Leads as appropriate to help manage privacy risks;
- Consult with the Privacy Office to assess privacy risks for significant strategic, operational decisions, policy matters and conduct Privacy Impact Assessments, when applicable; and
- Supervise the implementation of appropriate controls and remediation of issues to mitigate privacy risk and safeguard Personal Information.

Under the Policy, managers must:

- Conduct their duties in compliance with FIPPA and ensure that employees do the same;
- Verify that employees complete onboarding training as well as any other assigned training based on their role;
- Participate in and engage the Privacy Office to complete Privacy Impact Assessments and other privacy risk assessments;
- Report privacy issues to the Privacy Office and Corporate Compliance immediately upon discovery in order to determine which notification requirements, if any, arise from the issue reported, i.e. breach notification to the Information and Privacy Commissioner of Ontario or affected individuals; and
- Address privacy issues in an appropriate and timely manner.

Managers must review the Policy to understand the responsibilities and requirements that are relevant to their operations.

### 5. What should I do with the new Policy?

Departments should review their current practices, including their policies, procedures and controls, and ensure that these are in alignment with the new Policy. If you are unsure, please contact the Privacy Office. Divisions are responsible for ensuring that they are operating in a manner that protects the privacy of OLG's customers and ensures consistent compliance with FIPPA and this Policy.

### 6. Does the Policy cover privacy breaches too?

Yes, the Policy sets out requirements and responsibilities relating to privacy breaches. The Policy includes the Privacy Breach Response Protocol (Appendix C) which details the steps employees are required to take when they suspect or discover a privacy breach. The Policy also includes specific criteria to be used by Privacy Office to evaluate and respond to Privacy Breaches (Appendix D).

### 7. How can I learn more about privacy and requirements under FIPPA?

The Privacy Office has developed e-learning modules available on InsideOLG that explain requirements under FIPPA and how they apply to OLG. Login to MySuccess and search "Privacy" to access the "Privacy at OLG" and "Privacy Breach Management" modules. The Privacy Office is always available to assist employees, teams and departments on the requirements of FIPPA and how they apply to OLG.

## 8. How does OLG monitor compliance with the Policy?

The Privacy Office conducts Privacy Impact Assessments and provides strategic advice to OLG stakeholders regarding compliance with privacy requirements. Corporate Compliance, in collaboration with the Privacy Office, conducts monitoring and testing throughout OLG and with Service Providers to identify control weaknesses, privacy gaps and other potential opportunities for improving OLG's program.

## 9. Who should I speak to about the Policy?

The Privacy Office is always available to assist divisions, departments and employees with questions regarding privacy requirements. Reach out to the Privacy Office at privacy@olg.ca or contact a member of OLG's Privacy team:

- Sandra Ferguson – sferguson@olg.ca
- Sandra Fletcher – sfletcher@olg.ca
- Richard Brilli – rbrilli@olg.ca