Service Provider Contract Privacy Checklist

Below is a list of provisions that a public body should consider including in contracts with service providers when the service provider performs a service on behalf of a public body and in doing so has access to personal information subject to the *Protection of Privacy Act* (POPA). The contract should also include provisions regarding an individual's right of access to their own personal information under the *Access to Information Act* (ATIA).

DISCLAIMER: This checklist IS NOT a complete list of contract provisions that are generally in contracts, such as indemnification clauses. The applicability of these clauses depends on the nature of the work of the service provider for the public body and must be customized accordingly. A public body should consult with legal counsel when entering into contracts as a measure of ensuring their legal interests will be met through the contract provisions.

TOPIC	DESCRIPTION	YES	NO (Reason)
Control and Accountability	The contract specifies the relationship between the public body and the service provider as it relates to the services provided and that any collection, use or disclosure of personal information by the service provider on behalf of the public body must only be carried out in accordance with the terms of the contract.		
	"Personal information" is defined in the contract as defined in POPA.		
	The contract specifies that any personal information that is collected, or otherwise generated or used, and that is in the custody of the service provider for the purpose of providing the services to the public body, is in the control of the public body and that POPA and ATIA apply to this information.		
	The contract specifies that as a service provider to the public body, as it relates to the personal information in the custody of the service provider to provide the services, the service provider is bound to comply with POPA and ATIA as an "employee" of the public body.		
	The contract specifies the types of records containing personal information (list them) that the service provider has access to or that it will create as part of performing the services for the public body.		
	The contract requires the service provider to enter into confidentiality agreements with any of its employees who will have access to personal information to perform the services for the public body, which agreement must align with the service provider's duties under the contract as it relates to its handing of the personal information.		
	The contract restricts the use of subcontractors to perform any of the services without express written consent of the public body. If said consent is given, the contract requires the contractor to bind, through its contract with any subcontractor, the subcontractor to the terms of the contract between the service provider and public body as it relates to its duties concerning the personal information therein.		
	The contract requires the service provider to comply with the terms of the agreement and as an employee of the public body to ATIA and POPA.		

TOPIC	DESCRIPTION	YES	NO (Reason)
Control and Accountability	The contract specifies that the service provider is fully and solely responsible for the actions of its employees, subcontractors, and agents who act on its behalf in the performance of its functions under the contract. If applicable, the contract restricts a service provider's ability to subcontract.		
	The service provider has designated in the contract a senior individual within its organization to be the point of contact for complying with privacy and security obligations set out in the contract, and the contract specifies that any privacy and security issues that arise under the contract or for ascertaining compliance with the privacy provisions therein, the public body's Privacy Officer will be involved.		
	The contract clarifies how the service provider would notify the public body of any requests it receives to produce personal information it has in its custody to a government or law enforcement agency outside of Alberta.		
	The contract requires the service provider to provide the public body, upon request, with an up-to date list of all employees, subcontractors, or agents who have access to the personal information for the purposes of providing the services.		
	The contract specifies that any failure of the service provider, or of its employees or subcontractors, to follow the terms relating to the collection, use, disclosure, security or management of the personal information as set out in the contract is considered a breach of the contract.		
	The contract requires the service provider to advise the public body in advance in the event of any change in ownership of all or a part of the contractor's business.		
	The contract requires the service provider to immediately notify the public body in the event of any proceedings for bankruptcy or insolvency brought by or against the contractor under applicable bankruptcy or insolvency laws or any notice of creditor's remedies.		
	Audit and inspection of records or personal information The contract specifies when and how the public body will ensure oversight of the requirements in the contract, including that it may require compliance reports from the service provider as specified therein, and may enter the service provider's premises to inspect, audit, or require a third party to audit the service provider's compliance with the privacy, security, and information management requirements under the contract and that the service provider must co-operate with any such audit or inspection.		
	The contract requires the service provider to maintain specific information to enable the conduct of inspections and audits, i.e. the maintenance of some form of audit trail (electronic or paper form) for as long as the public body determines as necessary, and for compliance reporting purposes.		

TOPIC	DESCRIPTION	YES	NO (Reason)
Legal Authorities for Collection, Use or Disclosure	**Collection of personal information** (POPA sections 2, 4 and 5) The contract specifies that the contractor will collect personal information on behalf of the contractor and specify the authority under POPA for this collection. **Note**: Any collection must be limited to the personal information that is necessary for the service provider to perform the services.		
	The contract specifies what personal information may be collected by the service provider and prohibits the collection of any other personal information.		
	The contract requires the service provider to adhere to the requirements in POPA for collecting personal information, including for direct collection and notice. Any permitted indirect collection is identified in the contract along with the legal authority for this indirect collection.		
	The contract requires the service provider to give notice as required by section 5(2)(d) of POPA if the personal information collected will be entered into an automated system to generate content or make decisions, recommendations or predictions.		
	The contract requires that when collecting personal information from an individual, the service provider or its employees inform the individual that it/they are a service provider to the public body, performing the services on behalf of the public body, that the collection is subject to POPA, and that they are authorized thereunder to collect the information. Note: This could be done by way of notice.		
	Accuracy of personal information (POPA section 6) The contract requires that the service provider make every reasonable effort to ensure the accuracy and completeness of any personal information collected <u>where this information will be used to make a decision that will directly affect the individual to whom the information relates</u>. The contract requires that this information be retained for at least one year after using it to make a decision.		
	Use of personal information (POPA sections 11, 12, 14, 17) The contract specifies the permitted uses of the personal information (including any generated, such as derived data) by a service provider and the authority under POPA for this use.		
	The contract requires the service provider to adhere to the requirements in POPA for any use of the personal information including that it may only use this personal information to the extent necessary to enable the service provider to carry out its permitted use.		
	The contract restricts the service provider from using the personal information other than as permitted in the contract. **Note**: consider including a non-exhaustive list of prohibited activities to provide clarity, such as for marketing or training systems to improve services.		

TOPIC	DESCRIPTION	YES	NO (Reason)
Legal Authorities for Collection, Use or Disclosure	**Disclosure of personal information** (POPA sections 13 and 19) The contract specifies the permitted disclosures of personal information, including what specific personal information may be disclosed, and the authority under POPA for these disclosures. Note: If the service provider is permitted to disclose personal information with consent, then the contract should set out the process for obtaining consent as required by POPA and section 2 of the Regulation.		
	The contract restricts the service provider from disclosing personal information other than as permitted in the contract and the service provider is required to adhere to the requirements in POPA for any permitted disclosures of the personal information.		
	The contract requires the service provider to notify the public body if it receives any request or demand for disclosure of personal information for a purpose not authorized under the contract, and which may be required by law, immediately on receiving the request or demand and must not disclose the personal information unless permitted to do so in writing by the public body.		
Requests for Access or Correction	**Access to information and Correction requests** (ATIA section 7) The contract requires the service provider to respond to and manage, on behalf of the public body, access requests received under section 7 of ATIA or and/or correction request under section 7 of POPA. • Roles and responsibilities of each of the public body and service provider are clarified. • The specific responsibilities of the service provider for access request and correction requests are set out in the contract. • The contract specifies reporting requirements concerning responses to access requests. • Interaction with the OIPC for reviews, as between the parties, is specified as to roles and responsibilities concerning this interaction.		
	The contract requires the service provider to cooperate with the public body for any access to information or correction requests received by the public body, including requests made for information, other than just for personal information, that may be subject to the right of access under ATIA.		
Safeguards and Retention	**Protection of personal information** (POPA sections 10, 20, 25(2) and M-Regulation section 7) The contract requires the service provider to implement reasonable security arrangements to protect the personal information, which arrangements must, at minimum, meet the requirements of the public body's administrative, technical and physical safeguards and its security classification system, as set out in its PMP, and in accordance with POPA and section 7 of the M-Regulation. **Note**: The public body must make an assessment of the service provider's security policies and procedures to ensure they meet this threshold if the service provider does not adopt the public body's security policies and procedures for protecting the personal information.		

TOPIC	DESCRIPTION	YES	NO (Reason)
Safeguards and Retention	**Retention of records or personal information** (POPA sections 6 and 18(1)) The contract specifies the retention and disposal requirements that the service provider must adhere to for records or personal information, including data derived from personal information and non-personal data, including the minimum and maximum retention period and the secure disposal methods to be used. Note: When personal information is used to make a decision about an individual there are specific retention requirements (see Accuracy of personal information).		
	The contract specifies the conditions governing the disposition of any records containing personal information and sets out a certification process.		
	The contract specifies retention requirements for audit logs that are long enough for any investigations undertaken by the service provider, public body, and the OIPC concerning the duties of the service provider and their employees or subcontractors under the contract as they relate to the collection, use, disclosure, security and management of the personal information as set out in the contract.		
	Downstream adherence to the contract The contract requires all employees to sign a confidentiality agreement that ensures the service provider's compliance with its duties under the contract and with POPA and ATIA.		
	The contract requires the service provider to bind any subcontractors used in providing the service to the requirements of the service provider in the contract as it relates to the personal information.		
	The contract requires the service provider to train all its employees and any subcontractors who will have access to the personal information on the service providers duties under the contract as it relates to the personal information and for its obligations under POPA. The contract requires retraining to occur on an annual basis. The contact requires the service provider to inform the public body in writing when this training occurs and to whom it was given and when.		
	The contract requires the service provider to provide the public body with a copy of its training material including any updates.		
	Privacy and security assessments (POPA sections 10 and 26, section 1(1)(c) of the Regulation, and sections 2, 3 and 7 of the M-Regulation. The contract requires the service provider to cooperate in the development and any updating of any PIAs required to be created under POPA by the public body and for any required to be submitted to the OIPC for review. The contract requires the service provider to cooperate in a review of a PIA conducted by the OIPC.		
	The contract requires the service provider to conduct a security threat risk assessment at intervals specified in the contract, or as requested by the public body, as a measure to satisfy the public body that the personal information will be reasonably protected.		

TOPIC	DESCRIPTION	YES	NO (Reason)
Safeguards and Retention	**Notification of breach** (POPA section 10(2)) "Breach" is defined in the contract as "an incident involving the loss of, unauthorized access to or unauthorized disclosure of personal information".		
	The contract specifies what the service provider is to do if there is a breach (unauthorized access to or disclosure of personal information or loss), including: • the service provider must immediately notify the public body's Privacy Officer on learning about the breach; • the service provider's employees and subcontractors must immediately notify the service provider on learning about a breach; • it must cooperate with the public body on containment and management of the breach; • it must cooperate with the public body on meeting any of its notice requirements to affected individuals, the Minister and the Commissioner about the breach; and it must work with the public body on implementing any measures as may be necessary, or as recommended by the OIPC, to mitigate the risk of recurrence.		
Complaints Handling	**Complaints and investigations** (POPA section 38) The contract addresses how complaints received by the service provider concerning any allegation of non-compliance by the service provider (or its employees or subcontractors) with POPA will be addressed and managed and roles and responsibilities relating thereto are addressed in the contract.		
Termination	**Termination or expiry of the contract** The contract sets out how the contract may terminate including that it may terminate for breach of contract.		
	The contract addresses what is to happen to the records on termination of the contract, including when the contract is terminated for breach of its provisions, such as all personal information and records must be returned to the public body on termination of the contract and that the service provider shall not keep copies of the information.		
	The contract includes clear expectations regarding portability of the records created by the service provider, including those containing personal information, to ensure that on termination, the information can be moved across different platforms with minimal integration issues and it will be readable to the public body.		
	The contract requires that the duty of the service provider to keep confidential the personal information to which it has access during the term of the contract extends beyond the term of the contract and is in perpetuity.		