MAXIMUS | Canada	*Genesys Cloud Platform* *Privacy Impact Assessment*

OVERVIEW

Maximus Canada Inc. (Maximus) is conducting an assessment fors.21
s.21 contact centre solution with Genesys Cloud (Genesys). Genesys provides "Contact Centre as a Service" functionality, improves the agent experience and delivers an enhanced set of provisioning.s.21
s.21

The implementation of a replacement for the current systems.21
s.21 A reliable and efficient Contact Centre platform is imperative to
s.21

Genesys Cloud is utilized and accessed via a web browser; there is no requirement for a specific type of end user device or software. The service is used by Contact Centre supervisors and agents to efficiently and consistently manage customer engagement and multi channel agent-citizen communications. The service allows agents to seamlessly switch between channels, effectively respond to inquiries, capture integral information and maximize response time.

No new personal information is collected directly from the citizen as a result of migration to Genesys Cloud. Genesys is hosted and stored in Amazon Web Services (AWS) cloud in Canada. Data is accessed externally only for system troubleshooting/maintenance which is permissible under FIPPA legislation.

Genesys is an international leader in supporting business operations with strategic insights to respond and resolve issues in the provision of complex contact centre services. Through modernization and automation of IT solutions, organizations are able to leverage and maximize existing resources and reduce operating costs to meet or exceed optimum service levels.

Genesys has implemented key privacy and security safeguards that protect the confidentiality, integrity and availability of sensitive personal information including remedies and/or mitigation strategies to address potential compromises to personal information.

PART 1 GENERAL ADMINISTRATIVE DETAILS

1. Organization/work unit/author identification

Organization:	Maximus Canada Inc.		
Work unit (if applicable):	s.21		
Author:	Bev Hooper		
Email:	Bev.hooper@maximuscanada.ca	Phone:	(250) 405-3726
Executive Sponsor	Michael Long, Senior Vice President Shared Delivery Services		
Email:	Michael.long@maximuscanada.ca	Phone:	(250) 405-5566
Chief Privacy Officer	Bev Hooper		
Email:	Bev.hooper@maximuscanada.ca	Phone:	250 405-3726

2. Initiative description

Maximus Canada Inc. (Maximus) has been working directly with Genesys Laboratories Canada Inc. (Genesys) s.21 to provide s.21 of Contact Centre (CC) services and offering. To enable and support s.21 Maximus is currently assessing s.21 the Genesys Cloud platform.

Genesys seamlessly consolidates CC and business communications in an all-in-one omni channel platform. The system uniquely leverages technology to maximize the citizen experience and enable reliable and efficient interactions with personalized and contextual proactive communications across any channel. This provides multi channel touchpoints, unified services, and collaboration to realize greater operational efficiency. Genesys offers email management tools, categorized calls, interactive voice response (IVR), comprehensive messaging and robust engagement tools for optimum customer service.

Genesys has customer relationship management solutions and cloud-based capabilities that s.21

To ensure connected experiences with citizens that are customized to meet their needs, the Genesys solution provides intelligent call routing, telephony, voice interactions and features for agents which include:

- Individual agent assistance (IVR communications)
- Web chat, SMS, video-chat, co-browse, email functionality
- Call recording
- Queue status management
- Skills-based routing
- Wrap-up codes
- Consult transfer
- After-call work (ACW)/wrap-up
- Automatic call distribution (ACD)
- Citizen satisfaction survey across all channels (and associated reporting)
- Courtesy callback
- Non-business hours treatment for digital channels
- Increased control over agent access provisions
- Agent performance data and reporting
- Expanded dashboard and reporting structure
- Increased customization offerings
- Provision of end-to-end process visibility and optimization s.21 s.21
- s.21

Genesys also deploys a project team for analysis, design, provisioning, configuration, consultation and deployment of the services to include:

- *Automated Call Routing (IVR Schedule, secure call flow, queues, specific messaging)*
- *Network Assessment*
- *Add-ons (co-browse, voice services/BYOC Cloud, queues, callback flow, chat routing, email routing, SMS and email routing from external locations* s.21 s.21 *enhanced scripts, SSO integration, specialized alerts, recording, screen recording)*
- *Quality Assurance and Compliance (capabilities which allow CC management to evaluate and score interactions between agents and callers. A quality team can identify performers for positive feedback, agents who need more training or coaching, and situations that merit modification of call scripts). The functionality is enabled through call and screen recordings, and recording to text data for QA analysis (e.g. SMS, email, web chat). Call recordings, screen recordings and digital recordings are stored in Genesys Cloud hosted by AWS in Canada. By default, Genesys Cloud generates and stores the public/private key pair used by the recording encryption process. If required,* s.21

- *AppFoundry Integration* –s.21
- *Web Services Data Action* –s.21
- *Knowledge Base Program*

Genesys Laboratories Canada Inc. is a national service provider for organizations in over 100 countries. Through the power of the cloud and AI, Genesys technology connects partners and clients to redefine and improve the contact centre experience and customer engagement. Genesys has pioneered flexible innovative technology solutions to enable organizational interactions and personalization at scale through Genesys Cloud which is recognized as an all-in-one solution and the world's leading public cloud contact center platform. The company is dedicated to achieving the highest standards of excellence from product design to implementation and support. Genesys has been recognized by its customers, partners and the industry for its commitment to omni-channel contact centre software.

3. Scope of this PIA

This PIA outlines the proactive assessment conducting by Maximus for a potential migration to the Genesys Cloud platform by Genesys Laboratories Canada Inc. There are no changes to the existing collection, use and disclosure of personal information. All data is stored in the cloud by AWS, Canada. Data is accessed externally only for system troubleshooting/maintenance, which is permissible under FIPPA legislation.

4. Related documentation

This document is the first Privacy Impact Assessment that is being undertaken related to the Genesys Cloud solution. A Security Threat Risk Assessment to address security concerns for implementation of Genesys has been deemed essential and will be developed.

PART 2 OPERATIONS AND RISK ANALYSIS

5. Collecting personal information

No new citizen personal information would be collected during the use of Genesys. The system is required to provide CC communications, tools and supports for citizens and to meet operational service requirements per contractual agreements (as noted in point 2. above). See Appendix A for a list of existing personal information data elements.

6. Implications of withdrawing consent

None - Genesys would be implemented s.21 to replace the current system. The system would be used by Maximus CC employees to support operational service requirements and meet contractual agreements.

7. Notification statement

Notification statement	
Statement:	Citizens are notified (in accordance with the applicable legislation) via existing Maximus IVR messaging that their personal information will be used in order to administer and support services.
Initiative contact	
Position name or title:	Bev Hooper, Chief Privacy Officer
Mailing address:	2nd Floor – 722 Johnson Street, Victoria BC, V8W 1L4
Email:	Bev.hooper@maximuscanada.ca
Phone number:	(250) 405-3726

8. Personal information inventory

Data Element	Sensitivity	Purpose(s)	Role of user	Third party disclosure	Purpose for third party disclosure	Retention period
No new personal information would be collected, used or disclosed as a result of this system upgrade. See Appendix A for a listing of all existing	*Med – High*	*To provide CC programming for administration of client services.*	*Call centre agents/supervisors*	*Only as authorized by the client.*	*As determined by the client.*	*As applicable (client directed)*

personal information data elements.						

9. Personal information flow table/diagram

N/A – there would be no new collection, use or disclosure of personal information involved with this initiative. See Appendix A for a listing of all existing personal information data elements.

PART 3 SECURITY OF PERSONAL INFORMATION

8. Please describe the physical, technical and administrative security measures related to the initiative.

		Security Measures	
	Type	**Type of storage device**	**Security Measures**
1.	Physical	Electronic records, secure servers.	**Maximus:** No access to the physical infrastructure supporting the Genesys Cloud environment. Genesys Cloud is hosted by Amazon Web Services (AWS) in Canada. Data would be accessed externally only for system troubleshooting/maintenance which is permissible under FIPPA legislation. **Genesys:** s.15

			s.15 s.21 s.21 s.21 s.21 s.21 https://help.mypurecloud.com/articles/genesys-cloud-security-policy/ s.21
2.	Technical	On premises (physical/virtual servers)	**Maximus:** No technical access to the Genesys Cloud environment. This type of access is restricted to the service provider (Genesys). Genesys Cloud is hosted by Amazon Web Services (AWS) in Canada. Data would be accessed externally only for system troubleshooting/maintenance which is permissible under FIPPA legislation. **Genesys:** Specific Genesys Cloud employees have access to customer data. Permissions are granted based on the principle of least privilege. This practice ensures that only authorized personnel have access to system administration or information security administration. Genesys Cloud operations have a formal account management process and perform quarterly audits on users with access to production data. Permission for access to Genesys Cloud must be granted at the s.21 Genesys will create individual user accounts for each employee or contractor that has a business

s.13

			need to access the Genesys Cloud production environment. The following guidelines will be followed with regard to user account management: • User accounts are requested and authorized by our management. • User accounts follow the concept of least privilege. • Access to the Genesys Cloud Production environment requires multifactor authentication. • User accounts are s.21 s.21 • Quarterly review process for this access is in place. s.15 s.21 Genesys Cloud server instances are s.21 instead, s.21 s.21 s.21 It is required that all server instances be built on new virtual machines, and the old server instances terminated and deleted. s.21 Individual vulnerabilities are assessed for risk to Confidentiality, Integrity, and Availability and implemented accordingly. The Genesys Cloud

			suite of application services is based on a distributed cloud architecture built atop AWS. Genesys Cloud utilizes AWS services to provide highly available environments, including, but not limited to, the following: • Genesys Cloud uses s.21 s.21 is either at capacity or has failed, it routes traffic to other instances in seconds to compensate. Both Genesys Cloud's public APIs and backend instances s.21 • Genesys Cloud uses AZs which are geographical locations engineered to be insulated from failures in other AZs. Each AZ consists of one or more discrete data centers, each with redundant power, networking, and connectivity, housed in separate facilities. Dedicated fiber lines connect AZs so that normal connectivity has very low latency and AZ outages are detectable in seconds. All Genesys Cloud services are deployed into multiple AZs making them tolerant in the event of a data center or even entire AZ failure. • Genesys Cloud uses s.21 s.21 providing a durable infrastructure to store important data and is designed to deliver eleven 9's of durability. Your data is redundantly stored across multiple facilities and multiple devices in each facility. s.21 s.2 is designed for up to 99.99%

			availability of objects over a year and is backed by the s.21 service level agreement. This ensures that the service is reliable. • Genesys Cloud has more than 200 microservices running on s.21 s.21 s.21 and each microservice has at least s.21 running s. s.21 load balance requests across the microservice instances and detect failed instances s.21 routing requests to other instances. s.21 are also in s.21 which scale up the number of instances to meet demand automatically and replace failed instances with new healthy instances in s.21 • Genesys Cloud uses s.21 s.21 for caching data from databases and external services to make Genesys Cloud responsive. The nodes in each s.21 spread across multiple AZs so that the loss of a single AZ does not bring s.21 If any node in the s.21 fails, then the other nodes take over the failed node's work s.21 If a s.21 then the s.21 can be redeployed and begins caching data from the data's home of record s.21 • In addition to the database s.21 Genesys Cloud makes heavy use of s.21 highly available, with automatic and synchronous data replication across three facilities in a region. This helps protect your data against individual machine failures or even facility-level

			failures. s.15 https://help.mypurecloud.com/articles/genesys-cloud-security-policy/ https://www.genesys.com/company/trust
3.	Administrative/ technical	Contact Centre management system	**Maximus:** s.15 **Genesys:** s.15 https://help.mypurecloud.com/articles/genesys-cloud-privacy-policy/ https://help.mypurecloud.com/wp-content/uploads/2020/12/Genesys-Cloud-Privacy-Policy-december-2020.pdf

s.13

s.13

9. Please describe how you monitor compliance.

Maximus:

Detailed auditing mechanisms (including actions and a time stamp). Maximus will also implement processes to ensure adequate audit capabilities are in place. The application retains a detailed audit trail of all personal information accesses. Failed logins will be audited and the system is pw protected. Maximus agents or supervisors s.21 s.21 Only CC personnel (e.g. agents and supervisors) as well as the Maximus Quality Management department have access to voice calls, video/webchat, email and SMS (text) messages with role-based access and strong pw standards.

Genesys:

See the Genesys Cloud Service Terms and Conditions for details on monitoring compliance (Genesys Cloud Security Policy: mypurecloud.com). Data will be accessed externally only for system troubleshooting/ maintenance which is permissible under FIPPA legislation.

PART 4 ACCESS, ACCURACY, CORRECTION, & RETENTION

10. How can individuals request their own personal information?

All existing channels for client access to personal information are not changing and determined by contractual requirements.

11. How can an individual have their personal information updated, corrected, or annotated?

See above.

12. What is your legal or business requirement for the information and how long must you retain information to meet this requirement?

Maximus:

Maximus is under contract with its clients to effectively manage CCs in order to meet contractual and/or service level requirements. The Genesys platform is required to support and provide these processes and related services. Contact and log data is retained in accordance with retention policies, legal conditions and contractual obligations of Maximus' clients.

Genesys:

All transaction data for all media types recorded in Genesys must be retained as specified for the term stated in s.21 If log(s) are required as part of an investigation that has commenced, then the log(s) must be retained indefinitely.

13. How will your organization dispose of the personal information after the retention period is completed?

To be determined by contractual requirements.

PART 5 SIGNATURES

By signing this document, you accept the analysis and risks associated with this initiative. You affirm that you are authorized to sign on behalf of your work unit and/or organization.

Amanda Gray
Director
Strategic Technology Office
Maximus Canada Inc.

Date

Kent Berger North
Chief Security Officer
Maximus Canada Inc.

Date

Bev Hooper
Chief Privacy Officer
Maximus Canada Inc.

Date

Michael Long
Senior Vice President
Shared Delivery Services
Maximus Canada Inc.

Date

Deborah Shera
President
Maximus Canada Inc.

Date

APPENDIX A

Risk Mitigation Table

Identify the privacy risks associated with the initiative and indicate the probability of the risk occurring (low, medium or high) and the severity of the potential impact on individuals.

When scoring the mitigation strategies, consider how the solution will affect the probability or impact should the breach occur. No initiative is completely without risk, so risk will never be zero. See the Scoring Table below to assist in filling out this Risk Mitigation Table.

The final risk score is an indication of the outstanding risk after you have applied the mitigation strategies. It provides your management team with an understanding of the risks the organization will incur if they proceed with the initiative.

Risk Mitigation Table

	Risks	Probability Score (P)	Impacts	Impact Score (I)	Mitigation Strategy	Mitigation Score (M)	Risk Score (P) + (I) – (M)
1.	*Employee could access personal information and use or disclose it for personal purposes.*	s.21	*Privacy breach occurs; Genesys is deemed not secure and unreliable; embarrassment to the affected employee; loss of reputation as an employer for Maximus.*	*5*	*Maximus:* *Internal privacy and employee policies, terms of employment; agreements, training, etc.* *Enforcement of IT security policies, pw protected access, user provisions to system based on need-to-know principles, auditing, permission restrictions, controls and monitoring.* *Genesys:* *Internal*	s.21	s.21

					employee policies, protocols, terms of employment; contractual terms, training, etc. *Enforcement of IT policies, pw protected access, user provisions to system based on need-to-know principles, permission restrictions, controls and monitoring.*		
2.	*Personal information is accessed externally by another individual.*	s.2	*Privacy breach occurs; Genesys is deemed as not secure and unreliable; embarrassment to the affected employee; loss of reputation as an employer for Maximus.*	5	*Maximus:* *Employee is assigned a unique userid/pw which protects PI. Technical security policies, protocols, safeguards and firewalls.* *Genesys:* *Technical security policies, protocols, safeguards and firewalls.*	s.21	s.21
3.	*Unauthorized use or disclosure of PI.*	s.21	*Privacy breach occurs; Genesys is deemed as not secure and*	5	*Maximus:* *Internal privacy/breach*	s.21	s.21

			unreliable; embarrassment to the affected employee; loss of reputation as an employer for Maximus.		*and employee policies, terms of employment; agreements, training, etc.* *Enforcement of IT security policies, pw protected access, user provisions to system based on need-to-know principles, auditing, permission restrictions, controls and monitoring.* *Genesys:* *Internal privacy and employee policies, terms of employment; contractual terms, training, etc.* *Enforcement of IT security policies, pw protected access, user provisions to system based on need-to-know principles, permission restrictions, controls and monitoring.*		

5.	*Client's personal information is compromised when transferred to Genesys.*	s.21	*Privacy breach occurs; Genesys is deemed not secure and unreliable; embarrassment to the affected employee; loss of reputation as an employer for Maximus.*	*5*	*Maximus:* *Transmission is encrypted and over a secure line. Major IT security and privacy safeguards and policies in place to address management and protection of PI.* *Genesys:* *Transmission is encrypted and over a secure line. Major technical safeguards and policies in place to address management and protection of PI. Contractual privacy flow downs to service providers.*	s.21	s.21
6.	*Infrastructure failure*	s.21	*Genesys unavailable for use by Maximus and employees.*	*5*	*Maximus:* *Business continuation, disaster recovery and emergency preparedness plans.* *Genesys:* *Business continuation,*	s.21	s.21

					disaster recovery and emergency preparedness plans.		
7.	*Accidental disposal of media containing PI*	s.21	*Media (e.g. paper, hard drives, portable electronic device) not disposed of, degaussed or destroyed before decommissioning.*	*5*	*Maximus:* *Stringent privacy, retention and disposition policies, procedures and protocols in place for disposal of media containing PI.* *Genesys:* *Stringent privacy, retention and disposition policies, procedures and protocols in place for disposal of media containing PI per contractual agreement with Maximus.*	s.21	s.21

Heat mapping, the process of applying colour to risk levels, will provide management with a strong visual of the risks associated with your initiative. By approving the PIA and initiative, your organization's management is indicating that those risks are within the organization's tolerance for risk.

Risk Mitigation Table					
	Probability	**(P) Scores**	**Impact and Mitigation Levels**	**(I) and (M) Scores**	**(P) + (I) – (M) Risk Score**

s.21

OVERVIEW

Maximus Canada Inc. (Maximus) is conducting an assessment for s.21 s.21 contact centre solution with Genesys Cloud (Genesys). Genesys provides "Contact Centre as a Service" functionality, improves the agent experience and delivers an enhanced set of provisioning. s.21 s.21

The implementation of a replacement for the current system s.21 s.21 A reliable and efficient Contact Centre platform is imperative to increase productivity, ensure compliance with contractual obligations and to meet business priorities.

Genesys Cloud is utilized and accessed via a web browser; there is no requirement for a specific type of end user device or software. The service is used by Contact Centre supervisors and agents to efficiently and consistently manage customer engagement and multi channel agent-citizen communications. The service allows agents to seamlessly switch between channels, effectively respond to inquiries, capture integral information and maximize response time.

s.13

No new personal information is collected directly from the citizen as a result of migration to Genesys Cloud. Genesys is hosted and stored in Amazon Web Services (AWS) cloud in Canada. Data is accessed externally only for system troubleshooting/maintenance which is permissible under FIPPA legislation.

Genesys is an international leader in supporting business operations with strategic insights to respond and resolve issues in the provision of complex contact centre services. Through modernization and automation of IT solutions, organizations are able to leverage and maximize existing resources and reduce operating costs to meet or exceed optimum service levels.

Genesys has implemented key privacy and security safeguards that protect the confidentiality, integrity and availability of sensitive personal information including remedies and/or mitigation strategies to address potential compromises to personal information.

PART 1 GENERAL ADMINISTRATIVE DETAILS

1. Organization/work unit/author identification

Organization:	Maximus Canada Inc.		
Work unit (if applicable):	s.21		
Author:	Bev Hooper		
Email:	Bev.hooper@maximuscanada.ca	Phone:	(250) 405-3726
Executive Sponsor	Michael Long, Senior Vice President Shared Delivery Services		
Email:	Michael.long@maximuscanada.ca	Phone:	(250) 405-5566
Chief Privacy Officer	Bev Hooper		
Email:	Bev.hooper@maximuscanada.ca	Phone:	250 405-3726

2. Initiative description

Maximus Canada Inc. (Maximus) has been working directly with Genesys Laboratories Canada Inc. (Genesys) s.21 to provide s.21 of Contact Centre (CC) services and offering. To enable and support s.21 Maximus is currently assessing the transfer of s.21 to the Genesys Cloud platform.

Genesys seamlessly consolidates CC and business communications in an all-in-one omni channel platform. The system uniquely leverages technology to maximize the citizen experience and enable reliable and efficient interactions with personalized and contextual proactive communications across any channel. This provides multi channel touchpoints, unified services, and collaboration to realize greater operational efficiency. Genesys offers email management tools, categorized calls, interactive voice response (IVR), comprehensive messaging and robust engagement tools for optimum customer service.

s.13

Genesys has customer relationship management solutions and cloud-based capabilities that integrate current Maximus contact centre capabilities with existing systems and applications.

To ensure connected experiences with citizens that are customized to meet their needs, the Genesys solution provides intelligent call routing, telephony, voice interactions and features for agents which include:

- Individual agent assistance (IVR communications)
- Web chat, SMS, video-chat, co-browse, email functionality
- Call recording
- Queue status management
- Skills-based routing
- Wrap-up codes s.13
- Consult transfer
- After-call work (ACW)/wrap-up
- Automatic call distribution (ACD)
- Citizen satisfaction survey across all channels (and associated reporting)
- Courtesy callback
- Non-business hours treatment for digital channels
- Increased control over agent access provisions
- Agent performance data and reporting
- Expanded dashboard and reporting structure
- Increased customization offerings
- Provision of end-to-end process visibility and optimization s.21 s.21
-

Genesys also deploys a project team for analysis, design, provisioning, configuration, consultation and deployment of the services to include:

- *Automated Call Routing (IVR Schedule, secure call flow, queues, specific messaging)*
- *Network Assessment*
- *Add-ons (co-browse, voice services/BYOC Cloud, queues, callback flow, chat routing, email routing, SMS and email routing from external locations* s.21 s.21 *. enhanced scripts, SSO integration, specialized alerts, recording, screen recording)*
- *Quality Assurance and Compliance (capabilities which allow CC management to evaluate and score interactions between agents and callers. A quality team can identify performers for positive feedback, agents who need more training or coaching, and situations that merit modification of call scripts). The functionality is enabled through call and screen recordings, and recording to text data for QA analysis (e.g. SMS, email, web chat). Call recordings, screen recordings and digital recordings are stored in Genesys Cloud hosted by AWS in Canada. By default, Genesys Cloud generates and stores the public/private key pair used by the recording encryption process. If required,* s.21

- *AppFoundry Integration* – s.21
- *Web Services Data Action* –s.21
- *Knowledge Base Program*

Genesys Laboratories Canada Inc. is a national service provider for organizations in over 100 countries. Through the power of the cloud and AI, Genesys technology connects partners and clients to redefine and improve the contact centre experience and customer engagement. Genesys has pioneered flexible innovative technology solutions to enable organizational interactions and personalization at scale through Genesys Cloud which is recognized as an all-in-one solution and the world's leading public cloud contact center platform. The company is dedicated to achieving the highest standards of excellence from product design to implementation and support. Genesys has been recognized by its customers, partners and the industry for its commitment to omni-channel contact centre software.

3. Scope of this PIA

This PIA outlines the proactive assessment conducting by Maximus for a potential migration to the Genesys Cloud platform by Genesys Laboratories Canada Inc. There are no changes to the existing collection, use and disclosure of personal information. All data is stored in the cloud by AWS, Canada. Data is accessed externally only for system troubleshooting/maintenance, which is permissible under FIPPA legislation.

4. Related documentation

This document is the first Privacy Impact Assessment that is being undertaken related to the Genesys Cloud solution. A Security Threat Risk Assessment to address security concerns for implementation of Genesys has been deemed essential and will be developed.

PART 2 OPERATIONS AND RISK ANALYSIS

5. Collecting personal information

No new citizen personal information would be collected during the use of Genesys. The system is required to provide CC communications, tools and supports for citizens and to meet operational service requirements per contractual agreements (as noted in point 2. above). See Appendix A for a list of existing personal information data elements.

6. Implications of withdrawing consent

None - Genesys would be implemented s.21 to replace the current system. The system would be used by Maximus CC employees to support operational service requirements and meet contractual agreements.

7. Notification statement

Notification statement	
Statement:	Citizens are notified (in accordance with the applicable legislation) via existing Maximus IVR messaging that their personal information will be used in order to administer and support services.
Initiative contact	
Position name or title:	Bev Hooper, Chief Privacy Officer
Mailing address:	2nd Floor – 722 Johnson Street, Victoria BC, V8W 1L4
Email:	Bev.hooper@maximuscanada.ca
Phone number:	(250) 405-3726

8. Personal information inventory

Data Element	Sensitivity	Purpose(s)	Role of user	Third party disclosure	Purpose for third party disclosure	Retention period
No new personal information would be collected, used or disclosed as a result of this system upgrade. See Appendix A for a listing of all existing	*Med – High*	*To provide CC programming for administration of client services.*	*Call centre agents/supervisors*	*Only as authorized by the client.*	*As determined by the client.*	*As applicable (client directed)*

personal information data elements.						

9. Personal information flow table/diagram

N/A – there would be no new collection, use or disclosure of personal information involved with this initiative. See Appendix A for a listing of all existing personal information data elements.

PART 3 SECURITY OF PERSONAL INFORMATION

8. Please describe the physical, technical and administrative security measures related to the initiative.

		Security Measures	
	Type	**Type of storage device**	**Security Measures**
1.	Physical	Electronic records, secure servers.	**Maximus:** No access to the physical infrastructure supporting the Genesys Cloud environment. Genesys Cloud is hosted by Amazon Web Services (AWS) in Canada. Data would be accessed externally only for system troubleshooting/maintenance which is permissible under FIPPA legislation. **Genesys:** s.15

			s.15 s.21 s.21 s.21 s.21 s.21 https://help.mypurecloud.com/articles/genesys-cloud-security-policy/ s.21
2.	Technical	On premises (physical/virtual servers)	**Maximus:** No technical access to the Genesys Cloud environment. This type of access is restricted to the service provider (Genesys). Genesys Cloud is hosted by Amazon Web Services (AWS) in Canada. Data would be accessed externally only for system troubleshooting/maintenance which is permissible under FIPPA legislation. **Genesys:** Specific Genesys Cloud employees have access to customer data. Permissions are granted based on the principle of least privilege. This practice ensures that only authorized personnel have access to system administration or information security administration. Genesys Cloud operations have a formal account management process and perform quarterly audits on users with access to production data. Permission for access to Genesys Cloud must be granted at the s.21 Genesys will create individual user accounts for each employee or contractor that has a business

s.13

s.13

			need to access the Genesys Cloud production environment. The following guidelines will be followed with regard to user account management: • User accounts are requested and authorized by our management. • User accounts follow the concept of least privilege. • Access to the Genesys Cloud Production environment requires multifactor authentication. • User accounts are s.21 s.21 • Quarterly review process for this access is in place. s.15
			Genesys Cloud server instances are s.21 instead, s.21 s.21 s.21 It is required that all server instances be built on new virtual machines, and the old server instances terminated and deleted. s.21 Individual vulnerabilities are assessed for risk to Confidentiality, Integrity, and Availability and implemented accordingly. The Genesys Cloud

			suite of application services is based on a distributed cloud architecture built atop AWS. Genesys Cloud utilizes AWS services to provide highly available environments, including, but not limited to, the following: • Genesys Cloud uses s.21 s.21 is either at capacity or has failed, it routes traffic to other instances in seconds to compensate. Both Genesys Cloud's public APIs and backend instances s.21 • Genesys Cloud uses AZs which are geographical locations engineered to be insulated from failures in other AZs. Each AZ consists of one or more discrete data centers, each with redundant power, networking, and connectivity, housed in separate facilities. Dedicated fiber lines connect AZs so that normal connectivity has very low latency and AZ outages are detectable in seconds. All Genesys Cloud services are deployed into multiple AZs making them tolerant in the event of a data center or even entire AZ failure. • Genesys Cloud uses s.21 s.21 providing a durable infrastructure to store important data and is designed to deliver eleven 9's of durability. Your data is redundantly stored across multiple facilities and multiple devices in each facility. s.21 s.2is designed for up to 99.99%

			availability of objects over a year and is backed by the s.21 service level agreement. This ensures that the service is reliable. • Genesys Cloud has more than 200 microservices running on s.21 s.21 s.21 instance, and each microservice has at least s.21 running s s.21 load balance requests across the microservice instances and detect failed instances s.21 routing requests to other instances. s.21 are also in s.21 which scale up the number of instances to meet demand automatically and replace failed instances with new healthy instances in s.21 • Genesys Cloud uses s.21 s.21 for caching data from databases and external services to make Genesys Cloud responsive. The nodes in each s.21 spread across multiple AZs so that the loss of a single AZ does not bring s.21 If any node in the s.21 then the other nodes take over the failed node's work s.21 If a s.21 then the s.21 can be redeployed and begins caching data from the data's home of record s.21 • In addition to the database s.21 Genesys Cloud makes heavy use of s.21 is highly available, with automatic and synchronous data replication across three facilities in a region. This helps protect your data against individual machine failures or even facility-level

s.13

			failures. s.15 https://help.mypurecloud.com/articles/genesys-cloud-security-policy/ https://www.genesys.com/company/trust
3.	Administrative/ technical	Contact Centre management system	**Maximus:** s.15 **Genesys:** s.15 https://help.mypurecloud.com/articles/genesys-cloud-privacy-policy/ https://help.mypurecloud.com/wp-content/uploads/2020/12/Genesys-Cloud-Privacy-Policy-december-2020.pdf

s.13

s.13

9. Please describe how you monitor compliance.

Maximus:

Detailed auditing mechanisms (including actions and a time stamp). Maximus will also implement processes to ensure adequate audit capabilities are in place. The application retains a detailed audit trail of all personal information accesses. Failed logins will be audited and the system is pw protected. Maximus agents or supervisors s.21 s.21 Only CC personnel (e.g. agents and supervisors) as well as the Maximus Quality Management department have access to voice calls, video/webchat, email and SMS (text) messages with role-based access and strong pw standards. s.13

Genesys:

See the Genesys Cloud Service Terms and Conditions for details on monitoring compliance (Genesys Cloud Security Policy: mypurecloud.com). Data will be accessed externally only for system troubleshooting/ maintenance which is permissible under FIPPA legislation.

PART 4 ACCESS, ACCURACY, CORRECTION, & RETENTION

10. How can individuals request their own personal information?

All existing channels for client access to personal information are not changing and determined by contractual requirements.

11. How can an individual have their personal information updated, corrected, or annotated?

See above.

12. What is your legal or business requirement for the information and how long must you retain information to meet this requirement?

Maximus:

Maximus is under contract with its clients to effectively manage CCs in order to meet contractual and/or service level requirements. The Genesys platform is required to support and provide these processes and related services. Contact and log data is retained in accordance with retention policies, legal conditions and contractual obligations of Maximus' clients.

Genesys:

All transaction data for all media types recorded in Genesys must be retained as specified for the term stated in s.21 If log(s) are required as part of an investigation that has commenced, then the log(s) must be retained indefinitely.

13. How will your organization dispose of the personal information after the retention period is completed?

To be determined by contractual requirements.

s.13

PART 5 SIGNATURES

By signing this document, you accept the analysis and risks associated with this initiative. You affirm that you are authorized to sign on behalf of your work unit and/or organization.

Amanda Gray
Director
Strategic Technology Office
Maximus Canada Inc.

Date

Kent Berger North
Chief Security Officer
Maximus Canada Inc.

Date

Bev Hooper
Chief Privacy Officer
Maximus Canada Inc.

Date

Michael Long
Senior Vice President
Shared Delivery Services
Maximus Canada Inc.

Date

Deborah Shera
President
Maximus Canada Inc.

Date

APPENDIX A

Risk Mitigation Table

Identify the privacy risks associated with the initiative and indicate the probability of the risk occurring (low, medium or high) and the severity of the potential impact on individuals.

When scoring the mitigation strategies, consider how the solution will affect the probability or impact should the breach occur. No initiative is completely without risk, so risk will never be zero. See the Scoring Table below to assist in filling out this Risk Mitigation Table.

The final risk score is an indication of the outstanding risk after you have applied the mitigation strategies. It provides your management team with an understanding of the risks the organization will incur if they proceed with the initiative.

Risk Mitigation Table

	Risks	Probability Score (P)	Impacts	Impact Score (I)	Mitigation Strategy	Mitigation Score (M)	Risk Score (P) + (I) – (M)
1.	*Employee could access personal information and use or disclose it for personal purposes.*	s.2	*Privacy breach occurs; Genesys is deemed not secure and unreliable; embarrassment to the affected employee; loss of reputation as an employer for Maximus.*	*5*	*Maximus:* *Internal privacy and employee policies, terms of employment; agreements, training, etc.* *Enforcement of IT security policies, pw protected access, user provisions to system based on need-to-know principles, auditing, permission restrictions, controls and monitoring.* *Genesys:* *Internal*	s.2	s.21

					employee policies, protocols, terms of employment; contractual terms, training, etc. *Enforcement of IT policies, pw protected access, user provisions to system based on need-to-know principles, permission restrictions, controls and monitoring.*		
2.	*Personal information is accessed externally by another individual.*	s.21	*Privacy breach occurs; Genesys is deemed as not secure and unreliable; embarrassment to the affected employee; loss of reputation as an employer for Maximus.*	5	*Maximus:* *Employee is assigned a unique userid/pw which protects PI. Technical security policies, protocols, safeguards and firewalls.* *Genesys:* *Technical security policies, protocols, safeguards and firewalls.*	s.21	s.21
3.	*Unauthorized use or disclosure of PI.*	s.21	*Privacy breach occurs; Genesys is deemed as not secure and*	5	*Maximus:* *Internal privacy/breach*	s.21	s.21

			unreliable; embarrassment to the affected employee; loss of reputation as an employer for Maximus.		*and employee policies, terms of employment; agreements, training, etc.* *Enforcement of IT security policies, pw protected access, user provisions to system based on need-to-know principles, auditing, permission restrictions, controls and monitoring.* *Genesys:* *Internal privacy and employee policies, terms of employment; contractual terms, training, etc.* *Enforcement of IT security policies, pw protected access, user provisions to system based on need-to-know principles, permission restrictions, controls and monitoring.*		

5.	*Client's personal information is compromised when transferred to Genesys.*	s.21	*Privacy breach occurs; Genesys is deemed not secure and unreliable; embarrassment to the affected employee; loss of reputation as an employer for Maximus.*	*5*	*Maximus:* *Transmission is encrypted and over a secure line. Major IT security and privacy safeguards and policies in place to address management and protection of PI.* *Genesys:* *Transmission is encrypted and over a secure line. Major technical safeguards and policies in place to address management and protection of PI. Contractual privacy flow downs to service providers.*	s.21	s.21
6.	*Infrastructure failure*	s.21	*Genesys unavailable for use by Maximus and employees.*	*5*	*Maximus:* *Business continuation, disaster recovery and emergency preparedness plans.* *Genesys:* *Business continuation,*	s.21	s.21

					disaster recovery and emergency preparedness plans.		
7.	*Accidental disposal of media containing PI*	s.2	*Media (e.g. paper, hard drives, portable electronic device) not disposed of, degaussed or destroyed before decommissioning.*	5	*Maximus:* *Stringent privacy, retention and disposition policies, procedures and protocols in place for disposal of media containing PI.* *Genesys:* *Stringent privacy, retention and disposition policies, procedures and protocols in place for disposal of media containing PI per contractual agreement with Maximus.*	s.21	s.21

Heat mapping, the process of applying colour to risk levels, will provide management with a strong visual of the risks associated with your initiative. By approving the PIA and initiative, your organization's management is indicating that those risks are within the organization's tolerance for risk.

Risk Mitigation Table					
	Probability	**(P) Scores**	**Impact and Mitigation Levels**	**(I) and (M) Scores**	**(P) + (I) – (M) Risk Score**

s.21

Page 041 of 156 to/à Page 052 of 156

Withheld pursuant to/removed as

DUPLICATE

Privacy Impact Assessment Update Template for Ministries

Contents

Before you start 1
PART 1: GENERAL INFORMATION 2
PART 2: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA 4
PART 3: INITIATIVE CHANGES 4
PART 4: SIGNATURES 6

Use this privacy impact assessment (PIA) update template if you work for or are a service provider to a ministry in the Government of B.C. and are significantly changing your initiative.

Before you start

- An initiative is an enactment, system, project, program or activity
- Contact your Ministry Privacy Officer (MPO) for help with your PIA
- Your MPO fills in the shaded areas
- Find information on the PIA review process and question-by-question help on PCT's website
- If you have any questions, email Privacy.Helpline@gov.bc.ca or call the Privacy and Access Helpline 250-346-1851
- If you are starting a new initiative and need to complete a new PIA or complete a PIA for an enactment, find the correct template to use
- Protecting privacy involves managing records and providing reasonable security for information throughout its lifecycle. Contact your Government Records Officer for questions about information management and your Ministry Information Security Officer for questions about information security.

PART 1: GENERAL INFORMATION

Initiative title:	Service BC_Maximus Cloud Migration_Update
Original PIA title:	Service BC Contact Service Centre Solution V4
Original PIA number:	MTICS16066
Ministry:	Citizen's Services
Branch or unit:	Service BC
Your name and title:	Pia Dewar, Senior Information Privacy Analyst
Your email:	Pia.Dewar@gov.bc.ca
Initiative Lead name and title:	Richard Harris, A/Manager, Business Development, Service Delivery
Initiative Lead email:	Richard.Harris@gov.bc.ca
Ministry Privacy Officer:	Shawna Lynch
MPO email:	Shawna.Lynch@gov.bc.ca

Your MPO will complete the questions in the table below.

FOR MPO USE ONLY
Type of PIA (PI or non-PI):
PI
Is this a data-linking program under FOIPPA?
No
Is this a common or integrated program or activity?
No
Related PIAs, if any:
MTICS16066; CITZ17026; CITZ19072; CITZ21029
Would you describe this as a high-risk or complex initiative? If yes, why?
No

Briefly summarize the initiative to be published in the Personal Information Directory. This summary may be similar to the answer to question 1 below.
Maximus Canada is contracted by Service BC to carry out service delivery activities and responsibilities on SBC's behalf. Maximus is upgrading facilities, and frameworks to include use of a cloud solution in place of an on-premise solution. The only update occurring is that information holdings for service deliveries are being migrated to Genesys Cloud, off of Cisco Finesse (the previous on-premises solution).
Is there a new Information Sharing Agreement as part of this initiative? If yes, please have the Information Sharing Agreement Supplement attached to this PIA when submitting to PCT.
No

s.13

1. What is the update to your initiative?

This update assesses the migration of information holdings that Maximus Canada holds on behalf of Service BC as contracted service providers, from Cisco Finesse (an on-premises solution), to Genesys Cloud, an in-Canada-only cloud service hosted by AWS Canada. The collection, use, and disclosure of any information, personal or otherwise, that Maximus is migrating remains the same; this update focuses on the migration to Cloud hosting only.

2. Is any personal information stored outside of Canada?

No

3. Does your initiative involve sensitive personal information?

Yes

- If yes, go to question 4.
- If no, go to question 5

4. Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)?

No

- If yes, go to question 5
- If no, contact your MPO and go to Part 3

5. Where are you storing the personal information involved in your initiative?

If the change to your initiative is not related to sensitive personal information stored outside of Canada, and if you have already completed an Assessment of Disclosure for Storage Outside of Canada as part of your original PIA, go to Part 3.

After you answer this question go to Part 3.

PART 2: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section if you are storing sensitive personal information outside of Canada. You will likely need your MPO's help to complete this section.

6. Is the sensitive personal information stored by a service provider?

Type "yes" or "no" to indicate your response.

- If yes, fill in the table below (add more rows if necessary) and go to question 8
- If no, go to question 7

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?

7. Provide details on the disclosure, including where the sensitive personal information is stored.

8. Describe the contractual terms in place (if applicable).

If you wish to modify the Privacy Protection Schedule, email Privacy.Helpline@gov.bc.ca or call 250 356-1851 for approval.

For example, indicate if you have attached the Privacy Protection Schedule.

9. Are you relying on an existing contract, such as an enterprise offering from the Office of the Chief Information Officer (OCIO)?

Type "yes" or "no" to indicate your response.

- If yes, go to question 9.1
- If no, go to question 10

9.1 Which enterprise service are you accessing?

There may be a corporate PIA or other information to help you.

10. What controls are in place to prevent unauthorized access to sensitive personal information?

11. Provide details about how you will track access to sensitive personal information.

12. Describe the privacy risks for disclosures outside of Canada.

Use the table below to indicate the privacy risks, potential impacts and likelihood of occurrence and level of privacy risk. For each privacy risk identified, describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) that you outlined above.

Privacy risk	Impact to individuals	Likelihood of unauthorized collection, use, disclosure, or storage of the sensitive personal information (low, medium, high)	Level of privacy risk (low, medium, high, considering the impact and likelihood)	Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)	Is there any outstanding risk? If yes, please describe.

Outcome of Part 2

The outcome of Part 2 will be **a risk-based decision made by the head of the ministry on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 12.

PART 3: INITIATIVE CHANGES

13. Proposed changes to collection, use and disclosure

Use the table below to list each change to collection, use and disclosure of personal information.

Your MPO will help you identify whether each step represents collection, use or disclosure and make sure you have legal authority for what you want to do.

Describe each change to the way that your initiative involves personal information	MPO fills in collection, use and disclosure	MPO fills in FOIPPA authority	MPO fills in other legal authority
N/A			

Optional: Insert a drawing or flow diagram under this table or in an appendix if you think it will help to explain how each different part is connected.

14. Proposed changes to storage, security, accuracy, correction and retention

List each change you'll make to personal information in your initiative in the table below.

	Brief description of the change	MPO fills in FOIPPA authority (if applicable)	MPO fills in other legal authority (if applicable)
Storage	Services provided to Service BC by Maximus Canada will now be stored on Genesys	**S. 33.2(u)**	

	Cloud to meet operational services, and requirements. The only change being proposed is that of storage. Collection, use, and disclosure of any/all information remain the same.		
Physical security	s.15 s.21 s.21 s.21 s.21 s.21 https://help.mypurecloud.com/articles/genesys-cloud-security-policy/ s.21		
Technical security	Specific Genesys Cloud employees have access to customer data. Permissions are granted based on the principle of least privilege. This practice ensures that only authorized personnel have access to system administration or information security administration. Genesys Cloud operations have a formal account management process and perform quarterly audits on users with access to production data. Permission for access to Genesys Cloud must be granted at the s.21 Genesys will		

s.13

	create individual user accounts for each employee or contractor that has a business need to access the Genesys Cloud production environment. s.15 s.21		
	Genesys Cloud server instances are s.21 instead, s.21 s.21 s.21 It is required that all server instances be built on new virtual machines, and the old server instances terminated and deleted. s.21 Individual vulnerabilities are assessed for risk to Confidentiality, Integrity, and Availability and implemented accordingly. The Genesys Cloud suite of application services is based on a distributed cloud architecture built atop AWS. Genesys Cloud utilizes AWS services to provide highly available environments. Amazon also does not access Genesys Cloud customer data. https://help.mypurecloud.com/articles/genesys-cloud-security-policy/ *https://www.genesys.com/company/trust*		
Accuracy	All existing channels for client access to personal information are not changing and determined by contractual requirements. Any data requiring updates would occur in their normal course of service delivery and duties carried out by Maximus service providers in the context of a program, or initiative.		

s.13

9

Correction	Similar to concerns regarding information accuracy, a private citizen may request the updating of any personal information through the previously-established channels afforded through service deliveries and/or program initiatives.		
Retention	All information held by Maximus on behalf of SBC in Genesys is still subject to the contextually relevant retention schedules, as described by specific program requirements or as outlined in prior assessments.		

15. Is there a change to a personal information bank?

Beyond location of the data, no.

Describe the type of information in the bank
N/A
Name of lead ministry or agency involved
N/A
Any other ministries, agencies, public bodies or organizations involved
N/A
Business contact title and phone number for person responsible for managing the PIB
N/A

16. Describe any additional risks that arise from the changes you described above.

Describe any additional risks that arise from collecting, using, storing, accessing or sharing personal information in your initiative that have not been addressed by the questions on the template. Add new rows if necessary.

Possible risk	Response
Risk 1:	
Risk 2:	
Risk 3:	
Risk 4:	

PART 4: SIGNATURES

PCT Summary

This section summarizes PCT's review of the PIA, identifies decisions made that are not otherwise noted.

PCT Comment:

PCT Signatures

This PIA is based on a review of the material provided to PCT as of the date below.

Role	Name	Electronic signature	Date signed
PCT Privacy Advisor			

Ministry Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored or disclosed, the program area will engage with their MPO and if necessary, complete a PIA update to submit to PCT. Your ministry may choose to add signatories.

Please ensure that you have reviewed the privacy risks and risk responses in Part 4: Assessment of Disclosures Outside of Canada.

Ministry Comments:

Role	Name	Electronic signature	Date signed
Initiative lead			
Assistant Deputy Minister or designate			

Privacy and Security Officers	Name	Electronic signature	Date signed
Ministry Privacy Officer			
Ministry Information Security Officer Only required if MISO was involved in the PIA			

Privacy Impact Assessment Update Template for Ministries

Contents

Before you start 1
PART 1: GENERAL INFORMATION 2
PART 2: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA 4
PART 3: INITIATIVE CHANGES 4
PART 4: SIGNATURES 6

Use this privacy impact assessment (PIA) update template if you work for or are a service provider to a ministry in the Government of B.C. and are significantly changing your initiative.

Before you start

- An initiative is an enactment, system, project, program or activity
- Contact your Ministry Privacy Officer (MPO) for help with your PIA
- Your MPO fills in the shaded areas
- Find information on the PIA review process and question-by-question help on PCT's website
- If you have any questions, email Privacy.Helpline@gov.bc.ca or call the Privacy and Access Helpline 250-346-1851
- If you are starting a new initiative and need to complete a new PIA or complete a PIA for an enactment, find the correct template to use
- Protecting privacy involves managing records and providing reasonable security for information throughout its lifecycle. Contact your Government Records Officer for questions about information management and your Ministry Information Security Officer for questions about information security.

PART 1: GENERAL INFORMATION

Initiative title:	Service BC_Maximus Cloud Migration_Update
Original PIA title:	Service BC Contact Service Centre Solution V4
Original PIA number:	MTICS16066
Ministry:	Citizen's Services
Branch or unit:	Service BC
Your name and title:	Pia Dewar, Senior Information Privacy Analyst
Your email:	Pia.Dewar@gov.bc.ca
Initiative Lead name and title:	Richard Harris, A/Manager, Business Development, Service Delivery
Initiative Lead email:	Richard.Harris@gov.bc.ca
Ministry Privacy Officer:	Shawna Lynch
MPO email:	Shawna.Lynch@gov.bc.ca

Your MPO will complete the questions in the table below.

FOR MPO USE ONLY
Type of PIA (PI or non-PI):
PI
Is this a data-linking program under FOIPPA?
No
Is this a common or integrated program or activity?
No
Related PIAs, if any:
MTICS16066; CITZ17026; CITZ19072; CITZ21029
Would you describe this as a high-risk or complex initiative? If yes, why?
No

Briefly summarize the initiative to be published in the Personal Information Directory. This summary may be similar to the answer to question 1 below.
Maximus Canada is contracted by Service BC to carry out service delivery activities and responsibilities on SBC's behalf. Maximus is upgrading facilities, and frameworks to include use of a cloud solution in place of an on-premise solution. The only update occurring is that information holdings for service deliveries are being migrated to Genesys Cloud, off of Cisco Finesse (the previous on-premises solution).
Is there a new Information Sharing Agreement as part of this initiative? If yes, please have the Information Sharing Agreement Supplement attached to this PIA when submitting to PCT.
No

1. What is the update to your initiative?

This update assesses the migration of information holdings that Maximus Canada holds on behalf of Service BC as contracted service providers, from Cisco Finesse (an on-premises solution), to Genesys Cloud, an in-Canada-only cloud service hosted by AWS Canada, for the support of the Contact Centre solution, for the use of Cherwell, and Microsoft 365. The collection, use, and disclosure of any information, personal or otherwise, that Maximus is migrating remains the same; this update focuses on the migration to Cloud-hosting only.

2. Is any personal information stored outside of Canada?

No

3. Does your initiative involve sensitive personal information?

Yes

- If yes, go to question 4.
- If no, go to question 5

4. **Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)?**

No

- If yes, go to question 5
- If no, contact your MPO and go to Part 3

5. **Where are you storing the personal information involved in your initiative?**

If the change to your initiative is not related to sensitive personal information stored outside of Canada, and if you have already completed an Assessment of Disclosure for Storage Outside of Canada as part of your original PIA, go to Part 3.

After you answer this question go to Part 3.

PART 2: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section if you are storing sensitive personal information outside of Canada. You will likely need your MPO's help to complete this section.

6. **Is the sensitive personal information stored by a service provider?**

Type "yes" or "no" to indicate your response.

- If yes, fill in the table below (add more rows if necessary) and go to question 8
- If no, go to question 7

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?

7. **Provide details on the disclosure, including where the sensitive personal information is stored.**

8. Describe the contractual terms in place (if applicable).

If you wish to modify the Privacy Protection Schedule, email Privacy.Helpline@gov.bc.ca or call 250 356-1851 for approval.

For example, indicate if you have attached the Privacy Protection Schedule.

9. Are you relying on an existing contract, such as an enterprise offering from the Office of the Chief Information Officer (OCIO)?

Type "yes" or "no" to indicate your response.

- If yes, go to question 9.1
- If no, go to question 10

9.1 Which enterprise service are you accessing?

There may be a corporate PIA or other information to help you.

10. What controls are in place to prevent unauthorized access to sensitive personal information?

11. Provide details about how you will track access to sensitive personal information.

12. Describe the privacy risks for disclosures outside of Canada.

Use the table below to indicate the privacy risks, potential impacts and likelihood of occurrence and level of privacy risk. For each privacy risk identified, describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) that you outlined above.

Privacy risk	Impact to individuals	Likelihood of unauthorized collection, use, disclosure, or storage of the sensitive personal information (low, medium, high)	Level of privacy risk (low, medium, high, considering the impact and likelihood)	Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)	Is there any outstanding risk? If yes, please describe.

Outcome of Part 2

The outcome of Part 2 will be **a risk-based decision made by the head of the ministry on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 12.

PART 3: INITIATIVE CHANGES

13. Proposed changes to collection, use and disclosure

Use the table below to list each change to collection, use and disclosure of personal information.

Your MPO will help you identify whether each step represents collection, use or disclosure and make sure you have legal authority for what you want to do.

Describe each change to the way that your initiative involves personal information	MPO fills in collection, use and disclosure	MPO fills in FOIPPA authority	MPO fills in other legal authority
N/A			

Optional: Insert a drawing or flow diagram under this table or in an appendix if you think it will help to explain how each different part is connected.

14. Proposed changes to storage, security, accuracy, correction and retention

List each change you'll make to personal information in your initiative in the table below.

	Brief description of the change	MPO fills in FOIPPA authority (if applicable)	MPO fills in other legal authority (if applicable)
Storage	Services provided to Service BC by Maximus Canada will now be stored on Genesys	**S. 33.2(u)**	

	Cloud to meet operational services, and requirements. The only change being proposed is that of storage. Collection, use, and disclosure of any/all information remain the same.		
Physical security	s.15 s.21 s.21 s.21 s.21 s.21 s.21 https://help.mypurecloud.com/articles/genesys-cloud-security-policy/ s.21		
Technical security	Specific Genesys Cloud employees have access to customer data. Permissions are granted based on the principle of least privilege. This practice ensures that only authorized personnel have access to system administration or information security administration. Genesys Cloud operations have a formal account management process and perform quarterly audits on users with access to production data. Permission for access to Genesys Cloud must be granted at the s.21 Genesys will		

s.13

	create individual user accounts for each employee or contractor that has a business need to access the Genesys Cloud production environment. s.15 s.21 Genesys Cloud server instances are s.21 instead, s.21 s.21 s.21 It is required that all server instances be built on new virtual machines, and the old server instances terminated and deleted. s.21 Individual vulnerabilities are assessed for risk to Confidentiality, Integrity, and Availability and implemented accordingly. The Genesys Cloud suite of application services is based on a distributed cloud architecture built atop AWS. Genesys Cloud utilizes AWS services to provide highly available environments. Amazon also does not access Genesys Cloud customer data. https://help.mypurecloud.com/articles/genesys-cloud-security-policy/ *https://www.genesys.com/company/trust*		
Accuracy	All existing channels for client access to personal information are not changing and determined by contractual requirements. Any data requiring updates would occur in their normal course of service delivery and duties carried out by Maximus service providers in the context of a program, or initiative.		

s.13

9

Correction	Similar to concerns regarding information accuracy, a private citizen may request the updating of any personal information through the previously-established channels afforded through service deliveries and/or program initiatives.		
Retention	All information held by Maximus on behalf of SBC in Genesys is still subject to the contextually relevant retention schedules, as described by specific program requirements or as outlined in prior assessments.		

15. Is there a change to a personal information bank?

Beyond location of the data to the cloud, no.

Describe the type of information in the bank
N/A
Name of lead ministry or agency involved
N/A
Any other ministries, agencies, public bodies or organizations involved
N/A
Business contact title and phone number for person responsible for managing the PIB
N/A

16. Describe any additional risks that arise from the changes you described above.

Describe any additional risks that arise from collecting, using, storing, accessing or sharing personal information in your initiative that have not been addressed by the questions on the template. Add new rows if necessary.

Possible risk	Response
Risk 1:	
Risk 2:	
Risk 3:	
Risk 4:	

PART 4: SIGNATURES

PCT Summary

This section summarizes PCT's review of the PIA, identifies decisions made that are not otherwise noted.

PCT Comment:

PCT Signatures

This PIA is based on a review of the material provided to PCT as of the date below.

Role	Name	Electronic signature	Date signed
PCT Privacy Advisor			

Ministry Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored or disclosed, the program area will engage with their MPO and if necessary, complete a PIA update to submit to PCT. Your ministry may choose to add signatories.

Please ensure that you have reviewed the privacy risks and risk responses in Part 4: Assessment of Disclosures Outside of Canada.

Ministry Comments:

Role	Name	Electronic signature	Date signed
Initiative lead			
Assistant Deputy Minister or designate			

Privacy and Security Officers	Name	Electronic signature	Date signed
Ministry Privacy Officer			
Ministry Information Security Officer Only required if MISO was involved in the PIA			

Page 077 of 156 to/à Page 087 of 156

Withheld pursuant to/removed as

DUPLICATE

Privacy Impact Assessment Update Template for Ministries

Contents

Before you start..... **Error! Bookmark not defined.**

PART 1: GENERAL INFORMATION..... 1

PART 2: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA..... 3

PART 3: INITIATIVE CHANGES..... 7

PART 4: SIGNATURES..... 10

PART 1: GENERAL INFORMATION

CITZ22015

Initiative title:	Service BC_Maximus Cloud Migration_Update
Original PIA title:	Service BC Contact Service Centre Solution V4
Original PIA number:	MTICS16066
Ministry:	Citizen's Services
Branch or unit:	Service BC
Your name and title:	Pia Dewar, Senior Information Privacy Analyst
Your email:	Pia.Dewar@gov.bc.ca
Initiative Lead name and title:	Richard Harris, A/Manager, Business Development, Service Delivery
Initiative Lead email:	Richard.Harris@gov.bc.ca
Ministry Privacy Officer:	Shawna Lynch
MPO email:	Shawna.Lynch@gov.bc.ca

FOR MPO USE ONLY
Type of PIA (PI or non-PI):
PI
Is this a data-linking program under FOIPPA?
No
Is this a common or integrated program or activity?
No
Related PIAs, if any:
MTICS16066; CITZ17026; CITZ19072; CITZ21029
Would you describe this as a high-risk or complex initiative? If yes, why?
No
Briefly summarize the initiative to be published in the Personal Information Directory. This summary may be similar to the answer to question 1 below.
Maximus Canada is contracted by Service BC to carry out service delivery activities and responsibilities on SBC's behalf. Maximus is upgrading facilities, and frameworks to include use of a cloud solution in place of an on-premises solution. The only update occurring is that information holdings for service deliveries are being migrated to Genesys Cloud, off of Cisco Finesse (the previous on-premises solution).
Is there a new Information Sharing Agreement as part of this initiative? If yes, please have the Information Sharing Agreement Supplement attached to this PIA when submitting to PCT.
No

1. What is the update to your initiative?

This update assesses the migration of information holdings that Maximus Canada holds on behalf of Service BC as contracted service providers, from Cisco Finesse (an on-premises solution), to Genesys Cloud, an in-Canada-only cloud service hosted by AWS Canada, for the support of the Contact Centre solution, for the use of Cherwell, and Microsoft 365. The

collection, use, and disclosure of any information, personal or otherwise, that Maximus is migrating remains the same; this update focuses on the migration to Cloud-hosting only.

2. Is any personal information stored outside of Canada?

No

3. Does your initiative involve sensitive personal information?

Yes

- If yes, go to question 4.
- If no, go to question 5

4. Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)?

No

- If yes, go to question 5
- If no, contact your MPO and go to Part 3

5. Where are you storing the personal information involved in your initiative?

If the change to your initiative is not related to sensitive personal information stored outside of Canada, and if you have already completed an Assessment of Disclosure for Storage Outside of Canada as part of your original PIA, go to Part 3.

After you answer this question go to Part 3.

PART 2: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section if you are storing sensitive personal information outside of Canada. You will likely need your MPO's help to complete this section.

6. Is the sensitive personal information stored by a service provider?

Type "yes" or "no" to indicate your response.

- If yes, fill in the table below (add more rows if necessary) and go to question 8

- If no, go to question 7

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?

7. Provide details on the disclosure, including where the sensitive personal information is stored.

8. Describe the contractual terms in place (if applicable).

If you wish to modify the Privacy Protection Schedule, email Privacy.Helpline@gov.bc.ca or call 250 356-1851 for approval.

For example, indicate if you have attached the Privacy Protection Schedule.

9. Are you relying on an existing contract, such as an enterprise offering from the Office of the Chief Information Officer (OCIO)?

Type "yes" or "no" to indicate your response.

- If yes, go to question 9.1
- If no, go to question 10

9.1 Which enterprise service are you accessing?

There may be a corporate PIA or other information to help you.

10. What controls are in place to prevent unauthorized access to sensitive personal information?

11. Provide details about how you will track access to sensitive personal information.

12. Describe the privacy risks for disclosures outside of Canada.

Use the table below to indicate the privacy risks, potential impacts and likelihood of occurrence and level of privacy risk. For each privacy risk identified, describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) that you outlined above.

Privacy risk	Impact to individuals	Likelihood of unauthorized collection, use, disclosure, or storage of the sensitive personal information (low, medium, high)	Level of privacy risk (low, medium, high, considering the impact and likelihood)	Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)	Is there any outstanding risk? If yes, please describe.

Outcome of Part 2

The outcome of Part 2 will be **a risk-based decision made by the head of the ministry on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 12.

PART 3: INITIATIVE CHANGES

13. Proposed changes to collection, use and disclosure

Describe each change to the way that your initiative involves personal information	MPO fills in collection, use and disclosure	MPO fills in FOIPPA authority	MPO fills in other legal authority
No change			

14. Proposed changes to storage, security, accuracy, correction and retention

	Brief description of the change	MPO fills in FOIPPA authority (if applicable)	MPO fills in other legal authority (if applicable)
Storage	Services provided to Service BC by Maximus Canada will now be stored on Genesys Cloud to meet operational services, and requirements. The only change being proposed is that of storage. Collection, use, and disclosure of any/all information remain the same.	**S. 33.2(u)**	
Physical security	s.15 s.21 s.21		

	s.21 s.21 s.21 https://help.mypurecloud.com/articles/genesys-cloud-security-policy/ s.21		
Technical security	Specific Genesys Cloud employees have access to customer data. Permissions are granted based on the principle of least privilege. This practice ensures that only authorized personnel have access to system administration or information security administration. Genesys Cloud operations have a formal account management process and perform quarterly audits on users with access to production data. Permission for access to Genesys Cloud must be granted at the s.21 Genesys will create individual user accounts for each employee or contractor that has a business need to access the Genesys Cloud production environment. s.15 s.21 Genesys Cloud server instances are s.21 instead, s.21 s.21 s.21 It is required that all server instances be built on new virtual machines, and the old server instances terminated and deleted. s.21 Individual vulnerabilities are assessed for risk to Confidentiality, Integrity, and Availability and		

	implemented accordingly. The Genesys Cloud suite of application services is based on a distributed cloud architecture built atop AWS. Genesys Cloud utilizes AWS services to provide highly available environments. Amazon also does not access Genesys Cloud customer data. https://help.mypurecloud.com/articles/genesys-cloud-security-policy/ *https://www.genesys.com/company/trust*		
Accuracy	All existing channels for client access to personal information are not changing and determined by contractual requirements. Any data requiring updates would occur in their normal course of service delivery and duties carried out by Maximus service providers in the context of a program, or initiative.		
Correction	Similar to concerns regarding information accuracy, a private citizen may request the updating of any personal information through the previously-established channels afforded through service deliveries and/or program initiatives.		
Retention	All information held by Maximus on behalf of SBC in Genesys is still subject to the contextually relevant retention schedules, as described by specific program requirements or as outlined in prior assessments.		

15. Is there a change to a personal information bank?

Beyond location of the data to the AWS Canada cloud, no.

Describe the type of information in the bank
N/A
Name of lead ministry or agency involved
N/A
Any other ministries, agencies, public bodies or organizations involved
N/A
Business contact title and phone number for person responsible for managing the PIB

N/A

16. Describe any additional risks that arise from the changes you described above.

Describe any additional risks that arise from collecting, using, storing, accessing or sharing personal information in your initiative that have not been addressed by the questions on the template. Add new rows if necessary.

Possible risk	Response
Risk 1:	
Risk 2:	
Risk 3:	
Risk 4:	

PART 4: SIGNATURES

PCT Summary

PCT Comment:

PCT has reviewed the ministry's PIA update that details the migration of information holdings that Maximus Canada holds on behalf of Service BC as contracted service providers, from Cisco Finesse to Genesys Cloud (AWS Canada). The ministry has indicated appropriate FOIPPA authorities regarding the storage of personal information involved in this initiative update. PCT's review did not result in a recommendation to consult with the OIPC.

PCT Signatures

This PIA is based on a review of the material provided to PCT as of the date below.

Role	Name	Electronic signature	Date signed
PCT Privacy Advisor	Arun Lagah		May 20, 2022

Ministry Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored or disclosed, the program area will engage with their MPO and if necessary, complete a PIA update to submit to PCT. Your ministry may choose to add signatories.

Please ensure that you have reviewed the privacy risks and risk responses in Part 4: Assessment of Disclosures Outside of Canada.

Ministry Comments:

Role	Name	Electronic signature	Date signed
Initiative lead	Richard Harris	RH	2022-06-17
Assistant Deputy Minister or designate	Sheila Robinson, SBC		

Privacy and Security Officers	Name	Electronic signature	Date signed
Ministry Privacy Officer	Shawna Lynch	Shawna Lynch, MPO	July 13, 2022
Ministry Information Security Officer Only required if MISO was involved in the PIA	Garry Mierzuak		July 13, 2022

Privacy Impact Assessment Update Template for Ministries

Contents

Before you start..... **Error! Bookmark not defined.**

PART 1: GENERAL INFORMATION..... 1

PART 2: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA..... 3

PART 3: INITIATIVE CHANGES..... 7

PART 4: SIGNATURES..... 10

PART 1: GENERAL INFORMATION

CITZ22015

Initiative title:	Service BC_Maximus Cloud Migration_Update
Original PIA title:	Service BC Contact Service Centre Solution V4
Original PIA number:	MTICS16066
Ministry:	Citizen's Services
Branch or unit:	Service BC
Your name and title:	Pia Dewar, Senior Information Privacy Analyst
Your email:	Pia.Dewar@gov.bc.ca
Initiative Lead name and title:	Richard Harris, A/Manager, Business Development, Service Delivery
Initiative Lead email:	Richard.Harris@gov.bc.ca
Ministry Privacy Officer:	Shawna Lynch
MPO email:	Shawna.Lynch@gov.bc.ca

FOR MPO USE ONLY
Type of PIA (PI or non-PI):
PI
Is this a data-linking program under FOIPPA?
No
Is this a common or integrated program or activity?
No
Related PIAs, if any:
MTICS16066; CITZ17026; CITZ19072; CITZ21029
Would you describe this as a high-risk or complex initiative? If yes, why?
No
Briefly summarize the initiative to be published in the Personal Information Directory. This summary may be similar to the answer to question 1 below.
Maximus Canada is contracted by Service BC to carry out service delivery activities and responsibilities on SBC's behalf. Maximus is upgrading facilities, and frameworks to include use of a cloud solution in place of an on-premises solution. The only update occurring is that information holdings for service deliveries are being migrated to Genesys Cloud, off of Cisco Finesse (the previous on-premises solution).
Is there a new Information Sharing Agreement as part of this initiative? If yes, please have the Information Sharing Agreement Supplement attached to this PIA when submitting to PCT.
No

1. What is the update to your initiative?

This update assesses the migration of information holdings that Maximus Canada holds on behalf of Service BC as contracted service providers, from Cisco Finesse (an on-premises solution), to Genesys Cloud, an in-Canada-only cloud service hosted by AWS Canada, for the support of the Contact Centre solution, for the use of Cherwell, and Microsoft 365. The

collection, use, and disclosure of any information, personal or otherwise, that Maximus is migrating remains the same; this update focuses on the migration to Cloud-hosting only.

2. Is any personal information stored outside of Canada?

No

3. Does your initiative involve sensitive personal information?

Yes

- If yes, go to question 4.
- If no, go to question 5

4. Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)?

No

- If yes, go to question 5
- If no, contact your MPO and go to Part 3

5. Where are you storing the personal information involved in your initiative?

If the change to your initiative is not related to sensitive personal information stored outside of Canada, and if you have already completed an Assessment of Disclosure for Storage Outside of Canada as part of your original PIA, go to Part 3.

After you answer this question go to Part 3.

PART 2: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section if you are storing sensitive personal information outside of Canada. You will likely need your MPO's help to complete this section.

6. Is the sensitive personal information stored by a service provider?

Type "yes" or "no" to indicate your response.

- If yes, fill in the table below (add more rows if necessary) and go to question 8

- If no, go to question 7

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?

7. Provide details on the disclosure, including where the sensitive personal information is stored.

8. Describe the contractual terms in place (if applicable).

If you wish to modify the Privacy Protection Schedule, email Privacy.Helpline@gov.bc.ca or call 250 356-1851 for approval.

For example, indicate if you have attached the Privacy Protection Schedule.

9. Are you relying on an existing contract, such as an enterprise offering from the Office of the Chief Information Officer (OCIO)?

Type "yes" or "no" to indicate your response.

- If yes, go to question 9.1
- If no, go to question 10

9.1 Which enterprise service are you accessing?

There may be a corporate PIA or other information to help you.

10. What controls are in place to prevent unauthorized access to sensitive personal information?

11. Provide details about how you will track access to sensitive personal information.

12. Describe the privacy risks for disclosures outside of Canada.

Use the table below to indicate the privacy risks, potential impacts and likelihood of occurrence and level of privacy risk. For each privacy risk identified, describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) that you outlined above.

Privacy risk	Impact to individuals	Likelihood of unauthorized collection, use, disclosure, or storage of the sensitive personal information (low, medium, high)	Level of privacy risk (low, medium, high, considering the impact and likelihood)	Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)	Is there any outstanding risk? If yes, please describe.

Outcome of Part 2

The outcome of Part 2 will be **a risk-based decision made by the head of the ministry on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 12.

PART 3: INITIATIVE CHANGES

13. Proposed changes to collection, use and disclosure

Describe each change to the way that your initiative involves personal information	MPO fills in collection, use and disclosure	MPO fills in FOIPPA authority	MPO fills in other legal authority
No change			

14. Proposed changes to storage, security, accuracy, correction and retention

	Brief description of the change	MPO fills in FOIPPA authority (if applicable)	MPO fills in other legal authority (if applicable)
Storage	Services provided to Service BC by Maximus Canada will now be stored on Genesys Cloud to meet operational services, and requirements. The only change being proposed is that of storage. Collection, use, and disclosure of any/all information remain the same.	**S. 33.2(u)**	
Physical security	s.15 s.21 s.21		

	s.21 s.21 s.21 https://help.mypurecloud.com/articles/genesys-cloud-security-policy/ s.21		
Technical security	Specific Genesys Cloud employees have access to customer data. Permissions are granted based on the principle of least privilege. This practice ensures that only authorized personnel have access to system administration or information security administration. Genesys Cloud operations have a formal account management process and perform quarterly audits on users with access to production data. Permission for access to Genesys Cloud must be granted at the s.21 Genesys will create individual user accounts for each employee or contractor that has a business need to access the Genesys Cloud production environment. s.15 s.21 Genesys Cloud server instances are s.21 instead, s.21 s.21 s.21 It is required that all server instances be built on new virtual machines, and the old server instances terminated and deleted. s.21 Individual vulnerabilities are assessed for risk to Confidentiality, Integrity, and Availability and		

	implemented accordingly. The Genesys Cloud suite of application services is based on a distributed cloud architecture built atop AWS. Genesys Cloud utilizes AWS services to provide highly available environments. Amazon also does not access Genesys Cloud customer data. https://help.mypurecloud.com/articles/genesys-cloud-security-policy/ *https://www.genesys.com/company/trust*		
Accuracy	All existing channels for client access to personal information are not changing and determined by contractual requirements. Any data requiring updates would occur in their normal course of service delivery and duties carried out by Maximus service providers in the context of a program, or initiative.		
Correction	Similar to concerns regarding information accuracy, a private citizen may request the updating of any personal information through the previously-established channels afforded through service deliveries and/or program initiatives.		
Retention	All information held by Maximus on behalf of SBC in Genesys is still subject to the contextually relevant retention schedules, as described by specific program requirements or as outlined in prior assessments.		

15. Is there a change to a personal information bank?

Beyond location of the data to the AWS Canada cloud, no.

Describe the type of information in the bank
N/A
Name of lead ministry or agency involved
N/A
Any other ministries, agencies, public bodies or organizations involved
N/A
Business contact title and phone number for person responsible for managing the PIB

N/A

16. Describe any additional risks that arise from the changes you described above.

Describe any additional risks that arise from collecting, using, storing, accessing or sharing personal information in your initiative that have not been addressed by the questions on the template. Add new rows if necessary.

Possible risk	Response
Risk 1:	
Risk 2:	
Risk 3:	
Risk 4:	

PART 4: SIGNATURES

PCT Summary

PCT Comment:

PCT has reviewed the ministry's PIA update that details the migration of information holdings that Maximus Canada holds on behalf of Service BC as contracted service providers, from Cisco Finesse to Genesys Cloud (AWS Canada). The ministry has indicated appropriate FOIPPA authorities regarding the storage of personal information involved in this initiative update. PCT's review did not result in a recommendation to consult with the OIPC.

PCT Signatures

This PIA is based on a review of the material provided to PCT as of the date below.

Role	Name	Electronic signature	Date signed
PCT Privacy Advisor	Arun Lagah		May 20, 2022

Ministry Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored or disclosed, the program area will engage with their MPO and if necessary, complete a PIA update to submit to PCT. Your ministry may choose to add signatories.

Please ensure that you have reviewed the privacy risks and risk responses in Part 4: Assessment of Disclosures Outside of Canada.

Ministry Comments:

Role	Name	Electronic signature	Date signed
Initiative lead	Richard Harris	RH	2022-06-17
Assistant Deputy Minister or designate	Sheila Robinson, SBC		

Privacy and Security Officers	Name	Electronic signature	Date signed
Ministry Privacy Officer	N/A	N/A	N/A
Ministry Information Security Officer Only required if MISO was involved in the PIA	N/A	N/A	N/A

Page 110 of 156 to/à Page 120 of 156

Withheld pursuant to/removed as

DUPLICATE

ID: 25420, Title: SBC PCC Cloud Migration PIA - Final for Signature

Full Name:

Approval Route:

Richard Harris > Jeremy Moss > Stacey Sumners > Sheila Robinson > Stacey Sumners > Richard Harris

Assigned To: Dewar, Pia Rush: No Contracts - Service Contract Amendments Signature:

Assistant Deputy Minister

Branch: SBC-ISS Other Number: N/A

Link: N/A

Due Date: 7/25/2022 Date Completed: N/A Date Initiated: 6/17/2022 N/A

Item History

8/3/2022 02:53 PM

Harris, Richard CITZ:EX [Assignee] approved the item and forwarded it to Dewar, Pia for action

PIA fully signed-off by SBC business area. Closing the loop with IMB. Many thanks!

7/21/2022 11:36 AM

Van El, Wendy M CITZ:EX [Assignee] forwarded an eApprovals item to Harris, Richard CITZ:EX for action

Signed by S Robinson, thanks Wendy

7/21/2022 11:35 AM

Van El, Wendy M CITZ:EX added a document: CITZ22015 - PIA for Genesys with BH input_SigBlocksAltered.pdf

7/21/2022 11:00 AM

Sumners, Stacey CITZ:EX [Assignee] forwarded an eApprovals item to Van El, Wendy M CITZ:EX for action

Please add ADM signature, date and send back to branch

7/20/2022 05:47 PM

Robinson, Sheila A [Assignee] approved the item and forwarded it to Sumners, Stacey CITZ:EX for action

No Comment

7/20/2022 09:24 AM

Sumners, Stacey CITZ:EX [Assignee] forwarded an eApprovals item to Robinson, Sheila A for action

PCC Cloud Migration PIA for your review/approval. Edits made as per discussion by program area. Upon approval you esignature will be applied.

7/20/2022 09:23 AM

Sumners, Stacey CITZ:EX made some changes to this item's details

7/20/2022 08:54 AM

Moss, Jeremy [Assignee] approved the item and forwarded it to Sumners, Stacey CITZ:EX for action

Additional signatures added as per Sheila's request. Otherwise unchanged. Ready for Sheila's signature.

7/15/2022 09:47 AM

Harris, Richard CITZ:EX [Assignee] forwarded an eApprovals item to Moss, Jeremy for action

PIA updated to capture additional Information Management Branch signatures: Ministry Privacy Officer and Ministry Security Officer. PIA is otherwise unchanged, and fully approved by IMB and PCTB.

For clarity: this PIA addresses all four proposed Maximus cloud tools: Genesys contact centre platform, Cherwell service desk manager, Shelf knowledge base, and Microsoft Office 365.

7/15/2022 09:43 AM

Harris, Richard CITZ:EX added a document: CITZ22015 - PIA for Genesys with BH input_SigBlocksAltered.pdf

7/6/2022 01:49 PM

Sumners, Stacey CITZ:EX [Colleague of Robinson, Sheila A] forwarded an eApprovals item to Harris, Richard CITZ:EX for action

As requested

7/5/2022 04:16 PM

Sumners, Stacey CITZ:EX [Assignee] forwarded an eApprovals item to Robinson, Sheila A for action

PIA for ADM review/approval. Briefing scheduled in calendar July 6 @ 11:15am with Emily Eng

7/5/2022 12:30 PM
Eng, Emily CITZ:EX [Assignee] approved the item and forwarded it to Sumners, Stacey CITZ:EX for action

No Comment

7/5/2022 05:47 AM
Eng, Emily CITZ:EX made some changes to this item's details

6/23/2022 03:07 PM
Moss, Jeremy [Assignee] approved the item and forwarded it to Eng, Emily CITZ:EX for action

Approved from me, ready for A/E.D. approval and forwarding to ADM for signature.

6/23/2022 03:06 PM
Moss, Jeremy made some changes to this item's details

6/17/2022 09:48 AM
Harris, Richard CITZ:EX [Assignee] forwarded an eApprovals item to Moss, Jeremy for action

PIA Initiative Update reviewed and vetted by SBC business, IMB, and PCT. Privacy review confirms Canadian data residency and data sovereignty and compliance with FOIPPA. I endorse this document for further signature.

6/17/2022 09:44 AM
Harris, Richard CITZ:EX added a document: CITZ22015 - PIA for Genesys with BH input_SigBlocksAltered.pdf

6/17/2022 09:44 AM
Harris, Richard CITZ:EX deleted a document: CITZ22015 - PIA for Genesys with BH input_SigBlocksAltered.pdf

6/17/2022 09:42 AM
Harris, Richard CITZ:EX made some changes to this item's details

6/17/2022 09:42 AM
Harris, Richard CITZ:EX added a document: CITZ22015 - PIA for Genesys with BH input_SigBlocksAltered.pdf

6/17/2022 09:42 AM
Harris, Richard CITZ:EX created this item

Privacy Impact Assessment Update Template for Ministries

Contents

Before you start 1
PART 1: GENERAL INFORMATION 2
PART 2: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA 4
PART 3: INITIATIVE CHANGES 7
PART 4: SIGNATURES 11

Use this privacy impact assessment (PIA) update template if you work for or are a service provider to a ministry in the Government of B.C. and are significantly changing your initiative.

Before you start

- An initiative is an enactment, system, project, program or activity
- Contact your Ministry Privacy Officer (MPO) for help with your PIA
- Your MPO fills in the shaded areas
- Find information on the PIA review process and question-by-question help on PCT's website
- If you have any questions, email Privacy.Helpline@gov.bc.ca or call the Privacy and Access Helpline 250-346-1851
- If you are starting a new initiative and need to complete a new PIA or complete a PIA for an enactment, find the correct template to use
- Protecting privacy involves managing records and providing reasonable security for information throughout its lifecycle. Contact your Government Records Officer for questions about information management and your Ministry Information Security Officer for questions about information security.

PART 1: GENERAL INFORMATION

CITZ22015

Initiative title:	Service BC_Maximus Cloud Migration_Update
Original PIA title:	Service BC Contact Service Centre Solution V4
Original PIA number:	MTICS16066
Ministry:	Citizen's Services
Branch or unit:	Service BC
Your name and title:	Pia Dewar, Senior Information Privacy Analyst
Your email:	Pia.Dewar@gov.bc.ca
Initiative Lead name and title:	Richard Harris, A/Manager, Business Development, Service Delivery
Initiative Lead email:	Richard.Harris@gov.bc.ca
Ministry Privacy Officer:	Shawna Lynch
MPO email:	Shawna.Lynch@gov.bc.ca

Your MPO will complete the questions in the table below.

FOR MPO USE ONLY
Type of PIA (PI or non-PI):
PI
Is this a data-linking program under FOIPPA?
No
Is this a common or integrated program or activity?
No
Related PIAs, if any:
MTICS16066; CITZ17026; CITZ19072; CITZ21029
Would you describe this as a high-risk or complex initiative? If yes, why?
No

Briefly summarize the initiative to be published in the Personal Information Directory. This summary may be similar to the answer to question 1 below.
Maximus Canada is contracted by Service BC to carry out service delivery activities and responsibilities on SBC's behalf. Maximus is upgrading facilities, and frameworks to include use of a cloud solution in place of an on-premise solution. The only update occurring is that information holdings for service deliveries are being migrated to Genesys Cloud, off of Cisco Finesse (the previous on-premises solution).
Is there a new Information Sharing Agreement as part of this initiative? If yes, please have the Information Sharing Agreement Supplement attached to this PIA when submitting to PCT.
No

1. What is the update to your initiative?

This update assesses the migration of information holdings that Maximus Canada holds on behalf of Service BC as contracted service providers, from Cisco Finesse (an on-premises solution), to Genesys Cloud, an in-Canada-only cloud service hosted by AWS Canada, for the support of the Contact Centre solution, for the use of Cherwell, and Microsoft 365. The collection, use, and disclosure of any information, personal or otherwise, that Maximus is migrating remains the same; this update focuses on the migration to Cloud-hosting only.

2. Is any personal information stored outside of Canada?

No

3. Does your initiative involve sensitive personal information?

Yes

- If yes, go to question 4.
- If no, go to question 5

4. **Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)?**

No

- If yes, go to question 5
- If no, contact your MPO and go to Part 3

5. **Where are you storing the personal information involved in your initiative?**

If the change to your initiative is not related to sensitive personal information stored outside of Canada, and if you have already completed an Assessment of Disclosure for Storage Outside of Canada as part of your original PIA, go to Part 3.

After you answer this question go to Part 3.

PART 2: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section if you are storing sensitive personal information outside of Canada. You will likely need your MPO's help to complete this section.

6. **Is the sensitive personal information stored by a service provider?**

Type "yes" or "no" to indicate your response.

- If yes, fill in the table below (add more rows if necessary) and go to question 8
- If no, go to question 7

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?

7. **Provide details on the disclosure, including where the sensitive personal information is stored.**

8. Describe the contractual terms in place (if applicable).

If you wish to modify the Privacy Protection Schedule, email Privacy.Helpline@gov.bc.ca or call 250 356-1851 for approval.

For example, indicate if you have attached the Privacy Protection Schedule.

9. Are you relying on an existing contract, such as an enterprise offering from the Office of the Chief Information Officer (OCIO)?

Type "yes" or "no" to indicate your response.

- If yes, go to question 9.1
- If no, go to question 10

9.1 Which enterprise service are you accessing?

There may be a corporate PIA or other information to help you.

10. What controls are in place to prevent unauthorized access to sensitive personal information?

11. Provide details about how you will track access to sensitive personal information.

12. Describe the privacy risks for disclosures outside of Canada.

Use the table below to indicate the privacy risks, potential impacts and likelihood of occurrence and level of privacy risk. For each privacy risk identified, describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) that you outlined above.

Privacy risk	Impact to individuals	Likelihood of unauthorized collection, use, disclosure, or storage of the sensitive personal information (low, medium, high)	Level of privacy risk (low, medium, high, considering the impact and likelihood)	Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)	Is there any outstanding risk? If yes, please describe.

Outcome of Part 2

The outcome of Part 2 will be **a risk-based decision made by the head of the ministry on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 12.

PART 3: INITIATIVE CHANGES

13. Proposed changes to collection, use and disclosure

Use the table below to list each change to collection, use and disclosure of personal information.

Your MPO will help you identify whether each step represents collection, use or disclosure and make sure you have legal authority for what you want to do.

Describe each change to the way that your initiative involves personal information	**MPO fills in collection, use and disclosure**	**MPO fills in FOIPPA authority**	**MPO fills in other legal authority**
N/A			

Optional: Insert a drawing or flow diagram under this table or in an appendix if you think it will help to explain how each different part is connected.

14. Proposed changes to storage, security, accuracy, correction and retention

List each change you'll make to personal information in your initiative in the table below.

	Brief description of the change	**MPO fills in FOIPPA authority (if applicable)**	**MPO fills in other legal authority (if applicable)**
Storage	Services provided to Service BC by Maximus Canada will now be stored on Genesys	**S. 33.2(u)**	

	Cloud to meet operational services, and requirements. The only change being proposed is that of storage. Collection, use, and disclosure of any/all information remain the same.		
Physical security	s.15 s.21 s.21 s.21 s.21 s.21 https://help.mypurecloud.com/articles/genesys-cloud-security-policy/ s.21		
Technical security	Specific Genesys Cloud employees have access to customer data. Permissions are granted based on the principle of least privilege. This practice ensures that only authorized personnel have access to system administration or information security administration. Genesys Cloud operations have a formal account management process and perform quarterly audits on users with access to production data. Permission for access to Genesys Cloud must be granted at thes.21 Genesys will		

s.13

	create individual user accounts for each employee or contractor that has a business need to access the Genesys Cloud production environment. s.15 s.21 Genesys Cloud server instances are s.21 instead, s.21 s.21 s.21 It is required that all server instances be built on new virtual machines, and the old server instances terminated and deleted. s.21 Individual vulnerabilities are assessed for risk to Confidentiality, Integrity, and Availability and implemented accordingly. The Genesys Cloud suite of application services is based on a distributed cloud architecture built atop AWS. Genesys Cloud utilizes AWS services to provide highly available environments. Amazon also does not access Genesys Cloud customer data. https://help.mypurecloud.com/articles/genesys-cloud-security-policy/ *https://www.genesys.com/company/trust*		
Accuracy	All existing channels for client access to personal information are not changing and determined by contractual requirements. Any data requiring updates would occur in their normal course of service delivery and duties carried out by Maximus service providers in the context of a program, or initiative.		

s.13

Correction	Similar to concerns regarding information accuracy, a private citizen may request the updating of any personal information through the previously-established channels afforded through service deliveries and/or program initiatives.		
Retention	All information held by Maximus on behalf of SBC in Genesys is still subject to the contextually relevant retention schedules, as described by specific program requirements or as outlined in prior assessments.		

15. Is there a change to a personal information bank?

Beyond location of the data to the cloud, no.

Describe the type of information in the bank
N/A
Name of lead ministry or agency involved
N/A
Any other ministries, agencies, public bodies or organizations involved
N/A
Business contact title and phone number for person responsible for managing the PIB
N/A

16. Describe any additional risks that arise from the changes you described above.

Describe any additional risks that arise from collecting, using, storing, accessing or sharing personal information in your initiative that have not been addressed by the questions on the template. Add new rows if necessary.

Possible risk	Response
Risk 1:	
Risk 2:	
Risk 3:	
Risk 4:	

PART 4: SIGNATURES

PCT Summary

This section summarizes PCT's review of the PIA, identifies decisions made that are not otherwise noted.

PCT Comment:

PCT Signatures

This PIA is based on a review of the material provided to PCT as of the date below.

Role	Name	Electronic signature	Date signed
PCT Privacy Advisor			

Ministry Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored or disclosed, the program area will engage with their MPO and if necessary, complete a PIA update to submit to PCT. Your ministry may choose to add signatories.

Please ensure that you have reviewed the privacy risks and risk responses in Part 4: Assessment of Disclosures Outside of Canada.

Ministry Comments:

Role	Name	Electronic signature	Date signed
Initiative lead			
Assistant Deputy Minister or designate			

Privacy and Security Officers	Name	Electronic signature	Date signed
Ministry Privacy Officer			
Ministry Information Security Officer Only required if MISO was involved in the PIA			

Privacy Impact Assessment Update Template for Ministries

Contents

Before you start..... **Error! Bookmark not defined.**
PART 1: GENERAL INFORMATION..... 1
PART 2: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA..... 3
PART 3: INITIATIVE CHANGES..... 7
PART 4: SIGNATURES..... 10

PART 1: GENERAL INFORMATION

CITZ22015

Initiative title:	Service BC_Maximus Cloud Migration_Update
Original PIA title:	Service BC Contact Service Centre Solution V4
Original PIA number:	MTICS16066
Ministry:	Citizen's Services
Branch or unit:	Service BC
Your name and title:	Pia Dewar, Senior Information Privacy Analyst
Your email:	Pia.Dewar@gov.bc.ca
Initiative Lead name and title:	Richard Harris, A/Manager, Business Development, Service Delivery
Initiative Lead email:	Richard.Harris@gov.bc.ca
Ministry Privacy Officer:	Shawna Lynch
MPO email:	Shawna.Lynch@gov.bc.ca

FOR MPO USE ONLY
Type of PIA (PI or non-PI):
PI
Is this a data-linking program under FOIPPA?
No
Is this a common or integrated program or activity?
No
Related PIAs, if any:
MTICS16066; CITZ17026; CITZ19072; CITZ21029
Would you describe this as a high-risk or complex initiative? If yes, why?
No
Briefly summarize the initiative to be published in the Personal Information Directory. This summary may be similar to the answer to question 1 below.
Maximus Canada is contracted by Service BC to carry out service delivery activities and responsibilities on SBC's behalf. Maximus is upgrading facilities, and frameworks to include use of a cloud solution in place of an on-premises solution. The only update occurring is that information holdings for service deliveries are being migrated to Genesys Cloud, off of Cisco Finesse (the previous on-premises solution).
Is there a new Information Sharing Agreement as part of this initiative? If yes, please have the Information Sharing Agreement Supplement attached to this PIA when submitting to PCT.
No

1. What is the update to your initiative?

This update assesses the migration of information holdings that Maximus Canada holds on behalf of Service BC as contracted service providers, from Cisco Finesse (an on-premises solution), to Genesys Cloud, an in-Canada-only cloud service hosted by AWS Canada, for the support of the Contact Centre solution, for the use of Cherwell, and Microsoft 365. The

collection, use, and disclosure of any information, personal or otherwise, that Maximus is migrating remains the same; this update focuses on the migration to Cloud-hosting only.

2. Is any personal information stored outside of Canada?

No

3. Does your initiative involve sensitive personal information?

Yes

- If yes, go to question 4.
- If no, go to question 5

4. Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)?

No

- If yes, go to question 5
- If no, contact your MPO and go to Part 3

5. Where are you storing the personal information involved in your initiative?

If the change to your initiative is not related to sensitive personal information stored outside of Canada, and if you have already completed an Assessment of Disclosure for Storage Outside of Canada as part of your original PIA, go to Part 3.

After you answer this question go to Part 3.

PART 2: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section if you are storing sensitive personal information outside of Canada. You will likely need your MPO's help to complete this section.

6. Is the sensitive personal information stored by a service provider?

Type "yes" or "no" to indicate your response.

- If yes, fill in the table below (add more rows if necessary) and go to question 8

- If no, go to question 7

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?

7. Provide details on the disclosure, including where the sensitive personal information is stored.

8. Describe the contractual terms in place (if applicable).

If you wish to modify the Privacy Protection Schedule, email Privacy.Helpline@gov.bc.ca or call 250 356-1851 for approval.

For example, indicate if you have attached the Privacy Protection Schedule.

9. Are you relying on an existing contract, such as an enterprise offering from the Office of the Chief Information Officer (OCIO)?

Type "yes" or "no" to indicate your response.

- If yes, go to question 9.1
- If no, go to question 10

9.1 Which enterprise service are you accessing?

There may be a corporate PIA or other information to help you.

10. What controls are in place to prevent unauthorized access to sensitive personal information?

11. Provide details about how you will track access to sensitive personal information.

12. Describe the privacy risks for disclosures outside of Canada.

Use the table below to indicate the privacy risks, potential impacts and likelihood of occurrence and level of privacy risk. For each privacy risk identified, describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) that you outlined above.

Privacy risk	Impact to individuals	Likelihood of unauthorized collection, use, disclosure, or storage of the sensitive personal information (low, medium, high)	Level of privacy risk (low, medium, high, considering the impact and likelihood)	Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)	Is there any outstanding risk? If yes, please describe.

Outcome of Part 2

The outcome of Part 2 will be **a risk-based decision made by the head of the ministry on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 12.

PART 3: INITIATIVE CHANGES

13. Proposed changes to collection, use and disclosure

Describe each change to the way that your initiative involves personal information	MPO fills in collection, use and disclosure	MPO fills in FOIPPA authority	MPO fills in other legal authority
No change			

14. Proposed changes to storage, security, accuracy, correction and retention

	Brief description of the change	MPO fills in FOIPPA authority (if applicable)	MPO fills in other legal authority (if applicable)
Storage	Services provided to Service BC by Maximus Canada will now be stored on Genesys Cloud to meet operational services, and requirements. The only change being proposed is that of storage. Collection, use, and disclosure of any/all information remain the same.	**S. 33.2(u)**	
Physical security	s.15 s.21 s.21		

	s.15 s.21 s.21 s.21 https://help.mypurecloud.com/articles/genesys-cloud-security-policy/ s.21		
Technical security	Specific Genesys Cloud employees have access to customer data. Permissions are granted based on the principle of least privilege. This practice ensures that only authorized personnel have access to system administration or information security administration. Genesys Cloud operations have a formal account management process and perform quarterly audits on users with access to production data. Permission for access to Genesys Cloud must be granted at the s.21 Genesys will create individual user accounts for each employee or contractor that has a business need to access the Genesys Cloud production environment. s.15 s.21 Genesys Cloud server instances are s.21 instead, s.21 s.21 and updates. It is required that all server instances be built on new virtual machines, and the old server instances terminated and deleted. s.21 Individual vulnerabilities are assessed for risk to Confidentiality, Integrity, and Availability and		

s.13

s.13

	implemented accordingly. The Genesys Cloud suite of application services is based on a distributed cloud architecture built atop AWS. Genesys Cloud utilizes AWS services to provide highly available environments. Amazon also does not access Genesys Cloud customer data. https://help.mypurecloud.com/articles/genesys-cloud-security-policy/ *https://www.genesys.com/company/trust*		
Accuracy	All existing channels for client access to personal information are not changing and determined by contractual requirements. Any data requiring updates would occur in their normal course of service delivery and duties carried out by Maximus service providers in the context of a program, or initiative.		
Correction	Similar to concerns regarding information accuracy, a private citizen may request the updating of any personal information through the previously-established channels afforded through service deliveries and/or program initiatives.		
Retention	All information held by Maximus on behalf of SBC in Genesys is still subject to the contextually relevant retention schedules, as described by specific program requirements or as outlined in prior assessments.		

15. Is there a change to a personal information bank?

Beyond location of the data to the AWS Canada cloud, no.

Describe the type of information in the bank
N/A
Name of lead ministry or agency involved
N/A
Any other ministries, agencies, public bodies or organizations involved
N/A
Business contact title and phone number for person responsible for managing the PIB

N/A

16. Describe any additional risks that arise from the changes you described above.

Describe any additional risks that arise from collecting, using, storing, accessing or sharing personal information in your initiative that have not been addressed by the questions on the template. Add new rows if necessary.

Possible risk	Response
Risk 1:	
Risk 2:	
Risk 3:	
Risk 4:	

PART 4: SIGNATURES

PCT Summary

PCT Comment:

PCT has reviewed the ministry's PIA update that details the migration of information holdings that Maximus Canada holds on behalf of Service BC as contracted service providers, from Cisco Finesse to Genesys Cloud (AWS Canada). The ministry has indicated appropriate FOIPPA authorities regarding the storage of personal information involved in this initiative update. PCT's review did not result in a recommendation to consult with the OIPC.

PCT Signatures

This PIA is based on a review of the material provided to PCT as of the date below.

Role	Name	Electronic signature	Date signed
PCT Privacy Advisor	Arun Lagah		May 20, 2022

Ministry Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored or disclosed, the program area will engage with their MPO and if necessary, complete a PIA update to submit to PCT. Your ministry may choose to add signatories.

Please ensure that you have reviewed the privacy risks and risk responses in Part 4: Assessment of Disclosures Outside of Canada.

Ministry Comments:

Role	Name	Electronic signature	Date signed
Initiative lead			
Assistant Deputy Minister or designate			

Privacy and Security Officers	Name	Electronic signature	Date signed
Ministry Privacy Officer			
Ministry Information Security Officer Only required if MISO was involved in the PIA			

Page 146 of 156 to/à Page 156 of 156

Withheld pursuant to/removed as

DUPLICATE