GC Notify

Privacy and Data Protection Division
Privacy Analysis
Date: January 2024

This page is left blank

Note: This privacy analysis was conducted in collaboration with the Treasury Board Secretariat Privacy and Responsible Data Division (PRDD) prior to CDS's transition to the Department of Employment and Social Development Canada in August 2023. The risks outlined in the Privacy Considerations and Risks, Recommendations, and Mitigations sections, and CDS's response, were identified and reviewed by PRDD prior to the transition.

Table of Contents

Purpose

This Privacy Analysis is a customized assessment focused on an IT solution, tool, service or system. The purpose is to assess the impacts to privacy and identify privacy considerations in departments' use of an enterprise solution. It will also serve as an input/tool for other government departments using GC Notify to inform their privacy analyses and impact assessments.

Introduction

GC Notify is a government platform developed by the Canadian Digital Service (CDS) that provides a simple and efficient way for departments to integrate various channels of notifications into their services. GC Notify has been built using open-source code from CDS's counterparts at the Government Digital Service (GDS) in the United Kingdom.

The primary purpose of GC Notify is to connect other government departments' web services to people and inform them of where they need to go or what they need to do to complete a task, update a file, and/or review or approve a change.

GC Notify lets developers in government integrate notifications into their services easily with a web application programming interface (API). To send an email or text message with GC Notify, you need to create a message template first. Templates are used so that you can call on the same message repeatedly based on different variables.

The templates allow government departments to integrate the GC Notify API into the web applications they are building. For example, GC Notify could be built into authentication management. A service can use GC Notify to help clients reset or change their passwords. This is done by triggering a notification to the user's email on file with an expiring link that corresponds to a template variable filled in by the department's data platform. User login to the department's service could also be augmented by sending two-factor authentication codes via an email or text message generated by the system and delivered by GC Notify.

GC Notify allows departments to make use of a robust, extensible notification system without having to build a one-off solution each time. This saves both costs and time associated with procuring, building, or supporting individual notification systems for each and every government department and/or service.

GC Notify is not a subscriber list management system, and by design does not include the functionality to permanently store or manage recipient information. GC Notify is not the system of record for any personal information transmitted through it, and it is not used to determine administrative decisions.

As with all CDS products, GC Notify is designed for self-serve use by departmental teams to enable adoption and proactively provide prospective clients with the information they need. GC Notify has a suite of documents that together serve as the information sharing arrangement and other information on the product's security, privacy, availability, and operations. These documents are also made available to the general public and end users or recipients of notifications.

The Terms of Use outlines the responsibilities of departmental teams that use the GC Notify platform (e.g. sending Protected A and under notifications to users, getting user consent to send messages, and handling user data with your applicable policies and securities).

The Service Level Agreement (SLA) outlines the responsibilities that GC Notify has to its clients around security, availability of the product, known constraints, and providing support (e.g. uptime guarantees, providing support, and patching vulnerabilities).

The Privacy Statement outlines the privacy rights and considerations of a Notify client. It provides information on what information we collect, use, and share, as well as relevant authorities.

The Security Statement outlines key security information from GC Notify's Authority to Operate, as well as security measures to minimize risks (e.g. automated alarms and scanning, external audits and penetration testing). Additionally, it provides information on GC Notify's Security profile, summary of access controls for clients, concepts of continuous security and confidentiality.

Scope

This assessment specifically covers the GC Notify platform itself and CDS' handling of personal information. It does not cover the departmental programs/activities/services that use GC Notify. Per the Terms of Use, each department is responsible for ensuring that their use of the service and handling of personal information complies with the department's applicable privacy laws and policies. A separate privacy analysis may be required by the onboarding department.

Authority

CDS has the authority to collect personal information for this purpose under section 5.1 of the *Department of Employment and Social Development Canada*, which states:

The Minister may provide support for service delivery to the public and, in doing so, he or she may (b) provide (...) services to any department or body listed in Schedule I, I.1 or II to the *Financial Administration Act* and to any other partner entity authorized by the Governor in Council and perform activities related to those services.

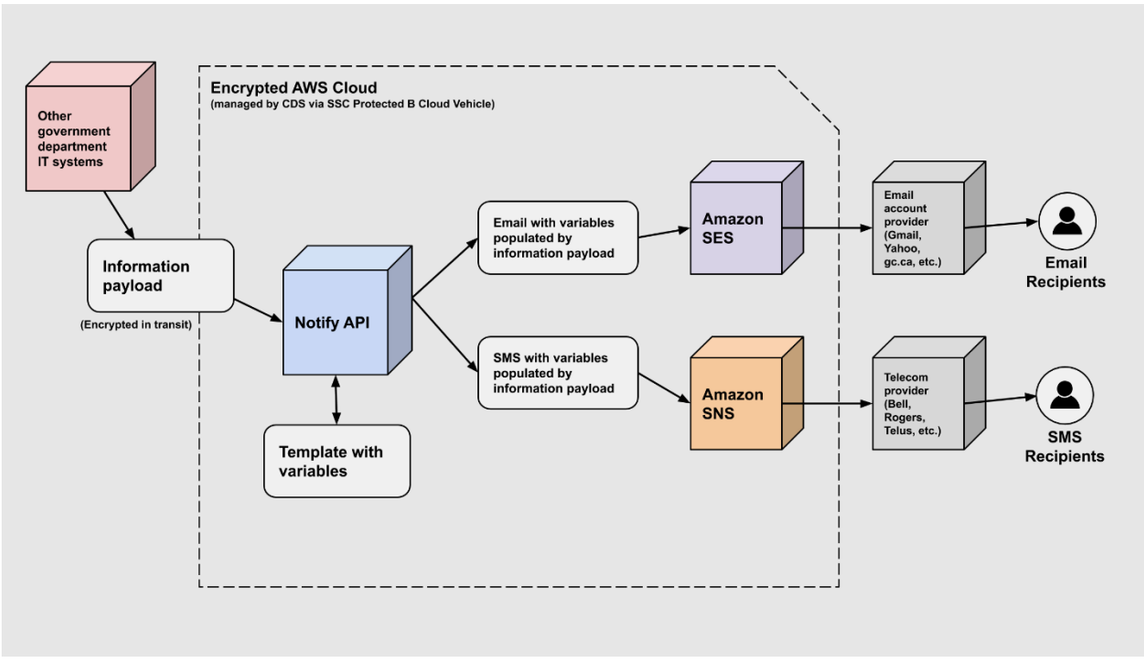
Personal Information Elements

See **Annex B**- Data Flow Table

Overview of Personal Information Flows

The diagram below illustrates the flow of information from other government departments' IT systems to the Notify API, and through to the underlying email and SMS infrastructure that delivers notifications to the email and telecom service providers used by each recipient.

Diagram 1: High-level flow



The information payload (sent via encrypted request from the departmental IT system to the Notify API) includes the recipients' contact information (email address or phone number) along with the identifier of the selected template (each template and version has a unique ID), and any

personalized variables (e.g. recipient-specific variables that the client uses; such as names, or dates specific to the recipient).

Templates include the structure of a notification, with placeholder variables that are replaced by the personalized variables (if any) included in the information payload.

- For example, a template with variables could be: “Hello [name], your file was successfully processed on [date].”
- The information payload sent from the departmental IT system could include, in this example, the email address of the recipient (used to send the notification) and the actual name and date to insert into the variable placeholders in the template.
- These variables are optional; in some cases, the template might only have pre-written text. For example, “Your password has successfully been reset.”

After an information payload is received by the Notify API, it is populated with the provided variables and sent to the underlying message delivery infrastructure. This message delivery infrastructure is one of two Amazon Web Services (AWS) products, depending on the message type: Simple Email Service (SES), to deliver email messages, and Simple Notification Service (SNS) to deliver SMS text messages. This infrastructure sends the relevant messages to the service providers for the recipients, using standard protocols by AWS such as SMTP. Emails are sent to the email account providers based on the recipients’ domain name (for example, Gmail, Yahoo, gc.ca, etc.) and SMS text messages are sent to the applicable telecom provider (Bell, Rogers, Telus, etc.) based on nationwide SMS handling. These providers receive the notification and deliver or display it to the recipient. This process is out of scope for this assessment.

The Notify API software, associated database, and message delivery infrastructure are all housed on an Amazon Web Services (AWS) cloud instance, established via SSC’s Protected B cloud vehicle and located in AWS’s Montreal region.

Connectivity

- *Identify all instances of connectivity with other systems and the technologies used to establish the connection and communications.*
- *Are the connections limited to technical functions with no further or residual uses / data matching or other activities?*
- *If personal information will be transmitted through an electronic system, application/software (including collaborative software), select the option that best applies*.

See diagram and corresponding explanation above- **Overview of Personal Information Flows**, for further details. The diagram illustrates the flow of information from other government departments’ IT systems to the Notify API, and through to the underlying email and SMS infrastructure that delivers notifications to the email and telecom service providers used by each recipient.

The information payload is sent via encrypted request from the departmental IT system to the Notify API. After an information payload is received by the Notify API, it is populated with the provided variables and sent to the underlying message delivery infrastructure. This message delivery infrastructure is one of two Amazon Web Services (AWS) products, depending on the message type: Simple Email Service (SES), to deliver email messages, and Simple Notification Service (SNS) to deliver SMS text messages. This infrastructure sends the relevant messages to the service providers for the recipients, using standard protocols.

The Notify API software, associated database, and message delivery infrastructure are all housed on an Amazon Web Services (AWS) cloud instance, established via SSC’s Protected B cloud vehicle, and located in AWS’s Montreal region.

GC Notify does not have (and does not require) any outbound connections back to other departmental IT systems. These departmental IT systems can optionally use the same API connection to query GC Notify for status updates (e.g., if the notifications were sent successfully). The API can also be used to query the status of individual notifications. A user can also set up call-backs so that Notify actually tells another system when there are status updates.

Security and Safeguards

The following applies to the new activity:

Cloud Services:

- Does the solution involve cloud services?
  ☒ Yes ☐ No

- Cloud Deployment Models:
  ☐ Public cloud ☒ Private cloud ☐ Hybrid cloud ☐ Non-cloud

- Cloud Service Models:
  ☒ Software as a Service (SaaS)
  ☐ Platform as a Service (PaaS)
  ☐ Infrastructure as a Service (IaaS)

Encryption:

- *Is there a clear plan for the secure transmission of personal information? The use of encryption for personal information both in transit and at rests: SFTP or FTP*

See diagram and corresponding explanation above- **Overview of Personal Information Flows**, for further details.

All personalized data found in notifications that might contain sensitive information are encrypted on transport to AWS and crypto-signed when stored within AWS to ensure data integrity. When email notifications leave our system, they may be encrypted, subject to routing infrastructure (e.g., email messages sent to a standard provider such as Google should be encrypted though likely routed through the US). On the other hand, SMS notifications are unlikely to be sent via an encrypted route.
Notify leverages AWS fast SMS sending, which picks random numbers among Canadian and sometimes American long codes if we send a message to a US number. If a US long code is chosen, it would likely go through an American carrier. SMS was never intended to be used to transmit high risk content. SMS messages are unencrypted. There are many inherent weaknesses in the SMS ecosystem.

In general, IT routing infrastructure does not respect borders. An email from Ottawa to Toronto can go through New York. SMS are unencrypted and broadcast through the air, they are not secure.

The connection will encrypt and carry the data between the servers (encrypted at the transport layer) but not at the application layer. Email servers and AWS and intermediate servers do encrypt on the wire but once it reaches the servers, everyone with access to these can read it (this is why an email client can parse content and show you ads about Notify).

However, what government clients do within Notify is secured and the infrastructure can handle up to protected B information (e.g. if someone creates a template, uploads an email list with variables, etc.), but once an email or text goes out of Notify to a recipient, we cannot guarantee what happens to it because anyone else could access this (e.g. email provider servers, telecommunications companies routing the msg, etc.). This is why our Terms of Use state that service owners only send messages designated up to and including “Protected A” per the Security levels for sensitive government information and assets.

Access controls

Notify has an access control document that was prepared for our Authority to Operate. Employees have role-based access and the document is updated whenever personnel onboards, offboards, or is granted new access.

Procedures regarding access controls and audit log are outlined in GC Notify’s Authority to Operate and Security Assessment. All administrator access activities are logged and audited if an alarm is triggered. In case of malicious activity, these alarms and logs provide context for the Notify Team to mitigate security risks.

Notify has automated monitoring through AWS Cloud Watch, as well as the monitoring that happens from the Canadian Centre for Cybersecurity (CCCS) to detect malicious activity and patterns. We have also set up WAF rules to block illegitimate activity and rate limit activity on our admin and API. In addition, only US and Canadian traffic is allowed to be transmitted through the API. For our own admin activity we only check audit logs in the event of an incident.

Portable storage devices and personal information

- *Does the solution involve or permit the use of portable storage devices, if yes please list approved devices.*
- *For non-approved devices, how have these prohibitions been communicated policies / procedures in place?*

Not applicable.

Automated Decision System[1]

- *Will the system or solution use personal information as part of an automated decision-making process, as part of personal information matching and/or knowledge discovery techniques?*
    - *If so, please explain (i.e., what personal information elements, what does the decision-making process involve, etc.).*
- *If yes, is an Algorithmic Impact Assessment being completed? Please provide details.*

Not applicable.

Status of Security Assessment and Authorization

- *Report on the status of any relevant SA&A whether completed, in progress or scheduled to be conducted.*
- *Where no SA&A will be conducted explain why.*
- *Describe any other security assessments.*

An SA&A of GC Notify was performed. The security assessment assessed the Notify service including application configuration and Amazon hosting environment. The report scope included the products, services and related processes that make up the Notification Service. The service was categorized at the Protected B, Medium Integrity, Medium Availability (PBMM) level. An authority to operate (ATO) was granted on March 11, 2022 for three (3) years or until significant change occurs. Eight (8) medium risks were identified which were grouped into four (4) risk mitigation tasks.

Inventory of Individuals

Table 1: Access

Within the scope of the assessment- the following have access who will be handling the relevant personal information. Permissions are ranked by most access/ critical to least.				
CDS Branch/Divisions	Positions/titles of individuals who access and handle personal information	Rationale or access	# Users	Geographical location
CDS, Internal Site Reliability Engineering (SRE) Team	Security Developer, Infrastructure Developer	Backend AWS Access, full read/write access to Notify Staging/ Production	5 users	Canada
CDS, GC Notify Team	Developer	Backend AWS Access, full read/write access to Notify Staging/ Production	8 users	Canada

[1] Includes any technology that either assists or replaces the judgement of human decision-makers. These systems draw from fields like statistics, linguistics, and computer science, and use techniques such as rules-based systems, regression, predictive analytics, machine learning, deep learning, and neural nets (TBS Directive on Automated Decision-Making, 2019).

CDS, GC Notify Team	Head of Notify, Product Manager, Researcher, Senior Designer Interaction, Tech Support Lead Developer	Backend AWS Access, lesser permissions: Read/write access to Notify Staging/Production support centre to create and resolve issues Write access to Notify SMS suppression lists Write access to Notify Staging/Production Pinpoint SMS and read access of Pinpoint console Read access to Notify Staging/Production	5 users	Canada
CDS	GC Notify Team	Front-end Notify Administrators	18 total users: - 10 GC Notify Team 5 SRE Team 2 Platform CORE Team 1 GC Articles Lead	Canada

Privacy Considerations

Accountability:

A government institution is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with privacy legislative and policy requirements. A government institution is also responsible for personal information under its control that is transferred to a third party.

As per the TB Directive on Security Management, the CEO / Assistant Deputy Minister has ultimate accountability for CDS products. Internal CDS guidance on this is outlined in the "Authority to Operate" process documentation.

Although GC Notify handles personal information, and has custody of it for a specified time, it is not the initial point of collection for any personal information. Section 4.2.23 of the Directive on Privacy Practices requires that government institutions establish agreements or arrangements with appropriate safeguards when disclosing personal information to another public sector entity. When sharing personal information, government institutions must prepare an Information Sharing Arrangement (ISA): a written record of understanding between government parties that outlines the terms and conditions under which personal information is shared between the parties. “Information sharing" may mean that one party is disclosing information while the other party is collecting information. It can also refer to situations where information is exchanged, that is, where both parties are disclosing and collecting information.

The purpose of an ISA is to establish a service delivery arrangement to govern the relationship between the Parties and articulate the respective roles and responsibilities of the Parties in relation to the delivery of the Program. Language should be included to clearly outline the exact roles and responsibilities in the event of a privacy breach or security incident, and ultimate responsibility for responding to any *Access to Information Act* and *Privacy Act* requests.

GC Notify has a suite of documents that together serve as an ISA and provide other information on the product’s security, privacy, availability, and operations. To be transparent, these documents are also made available to the public and end users or recipients of notifications. It is important to note that this documentation does not include signatures from the responsible parties.

Risk: Although language was included in the Terms of Use and Service Level Agreement around roles and responsibilities, there is a low risk that in the absence of a signed agreement, the roles and responsibilities in the event of a security incident, privacy breach complaint or other related issue may be unclear and potentially lead to a longer response time.

Recommendation: PRD recommended that the documents be signed by onboarding institutions.

Compliance Issue: No issue identified.

Institutions’ Considerations: Ensure that the accountability for the protection of personal information used for the service is clear and documented.

Consider drafting operational guidance (processes and procedures) to ensure the roles and responsibilities at the working level are clearly understood.

Collection:

Once an institution has determined the purpose and the need to share personal information, as per section 4 of the *Privacy Act*, it must verify that it has the legal authority to collect the personal information. Authority to collect personal information will usually be found in an Act of Parliament or subsequent regulations.

CDS has the authority to collect personal information for this purpose under section 5.1 of the *Department of Employment and Social Development Canada*, which states:

(1) The Minister may provide support for service delivery to the public and, in doing so, he or she may (b) provide (...) services to any department or body listed in Schedule I, I.1 or II

to the *Financial Administration Act* and to any other partner entity authorized by the Governor in Council and perform activities related to those services.

Although GC Notify handles personal information (i.e., has custody of it for a specified time), it is not the initial point of collection for any personal information.

Notwithstanding CDS's authority to provide the service, the government institution to which the service is being provided must verify that it has the legal authority to collect the personal information.

Risk: No risk identified.

Issue: No issue identified.

Institutions' Considerations:

Ensure the collection authority for the program/activity using the service.

Use:

The Terms of Use outlines the responsibilities of departmental teams that use the GC Notify platform (e.g. sending Protected A and under notifications to users, getting user consent to send messages, and handling user data with your applicable policies and securities).

The Service Level Agreement (SLA) outlines the responsibilities that GC Notify has to its clients around security, availability of the product, known constraints, and providing support (e.g. uptime guarantees, providing support, and patching vulnerabilities).

The Privacy Statement outlines the privacy rights and considerations of a Notify client. It provides information on what information we collect, use, and share, as well as relevant authorities

Risk: No risk identified.

Issue: No issue identified.

Institutions' Considerations: As per section 6.3.1. of the Directive on Privacy Impact Assessment, a PIA should be initiated when personal information is used as part of a decision-making process; upon substantial modification to an existing program or activity; and when contracting out to another level of government or the private sector.

Determine whether the use of Notify accounts for a substantial modification to their program/activity and warrants the initiation of a PIA.

Disclosure:

Once an institution has determined the purpose and the need to share personal information, as per section 4 of the *Privacy Act*, it must verify that it has the legal authority both to have the personal information with other institutions. Authority to disclose personal information will usually be found in an Act of Parliament or subsequent regulations.

Notwithstanding CDS's authority to provide the service, the government institution to which the service is being provided must verify that it has the legal authority to share the personal information with other institutions.

Risk: No risk identified.

Compliance Issue: No issue identified.

Institutions' Considerations:

As per section 8(2) of the *Privacy Act*, personal information under the control of a government institution may be disclosed for specific purposes and under certain circumstances.

Ensure that the personal information of the program/activity may be disclosed for the use of Notify.

Accuracy:

As per the Terms of Use, each department is responsible to provide CDS with the most up-to-date information, as per their records.

Risk: No risk identified.

Compliance Issue: No issue identified.

Institutions' Considerations:

Ensure the maintenance of accurate program/activity personal information.

Retention:

Although GC Notify handles personal information, and has custody of it, it is not the initial point of collection for any personal information. GC Notify does not permanently store any personal information and all personal information handled by GC Notify is automatically deleted after a retention period (7 days by default, but configurable).

Notify retains information needed to send notifications for 7 days such as emails, phone number, template personalization, and the csv file used to facilitate sending. After the 7 days, Notify retains non-identifying information, such as time and method of sending, and number of messages sent for statistical purposes.

Clients can upload an attachment to their email notification through the API. Notify retains the file for 7 days and permanently deletes the file from Notify (API documentation).

Clients can upload an attachment to their email notification *as a link that can be downloaded* through the API. The client uploads the file to Notify and we generate a unique link for the recipient to click and download the file. The file and the unique link is open for 7 days for the recipient to download, after 7 days permanently deletes the file from Notify (API documentation).

Storing this information for 7 days allows for technical troubleshooting (in cases where messages could not be sent successfully, for example because an email address was misspelled when a department originally collected it). It also provides a time window for handling any complaints from recipients about a notification they received or about the handling of their personal information.

Institutions may request a retention reduction for information used to send notifications down to 3 days if they find that the need for privacy protection is greater than the need for support and technical troubleshooting (e.g. use cases involving health).

GC Notify sends firewall and access logs to the Canadian Centre for Cyber Security (CCCS) for threat monitoring and is collected under their PIB for Cyber Defence (CSE PPU 007). Data shared includes:

- Recipient IP address (or internal IP address if using a VPN)
- Approximate location, and timestamp of when a message was sent out

Browser information (type of browser and version), and operating system

Risk: No risk identified.

Compliance Issue: No issue identified.

Institutions' Considerations:

Ensure that established retention and disposition are followed accordingly and are modified to reflect any changes.

Safeguards:

An SA&A has been conducted and an Authority to Operate has been granted. See section above **Status of Security Assessment and Authorization** for further details.

CDS uses a continuous security approach. GC Notify embeds security specialists on the team and treat security priorities as design constraints. This involves automated security tools, such as AWS Cloud Watch and the CCCS Cloud-Based Sensor, to monitor for suspicious activity and a set of CDS-wide policies such as Patch Management and Security guidelines.

Risk: There is a risk that, in the absence of a clear monitoring schedule, the impact of a breach (inappropriate access) may be increased.

Recommendation: PRDD recommended that a monitoring schedule be put in place.

Compliance Issue: No issue identified.

Institutions' Considerations:

Ensure to maintain implemented institutional safeguards and modify accordingly, if required.

Openness:

This Privacy Analysis will be available to current and prospective clients by request.

The Privacy Statement outlines the privacy rights and considerations of a Notify client. It provides information on what information we collect, use, and share, as well as relevant authorities.

Risk: No risk identified.

Compliance Issue: No issue identified.

Institutions' Considerations:

If a PIA is required, that the summary be posted on the departmental website.

As per section 4.2.10 of the Directive on Privacy Practices government institutions are required to notify the individual whose personal information is collected directly, including any uses or disclosure that are consistent with the original purpose.

Whether the current privacy notice meets the policy requirements, in accordance with section 4.2.10 of the Directive on Privacy Practices, which requires government institutions to notify the individual whose personal information is collected directly, including any uses or disclosure that are consistent with the original purpose.

Ensure privacy notice statement(s) are modified to reflect consistent uses and/or disclosures.

Individual Access:

As stated in the Terms of Use, responding to requests under the *Access to Information* and *Privacy Act* about information entered in GCNotify by the client is the responsibility of the client. Upon being contacted, CDS will support such requests.

As per section 10 of the *Privacy Act*, government institutions are required to include in personal information banks, all personal information under control of the institution that is used for an administrative purpose or intended to be retrieved by the name or other identifier of an individual. As per the Directive on Privacy Practices, under the *Privacy Act*, heads of all government institutions are required to identify, describe and publicly report their institutions' personal information banks (PIBs) and classes of personal information. The activities undertaken by CDS do not require the development of a PIB, as the personal information in Notify is not used for an administrative purpose and is not intended to be retrieved by personal identifier. However, CDS is a custodian of personal information and fall within the parameter of a classes of personal information, being personal information that is not intended to be used for an administrative purpose or that it is not intended to be retrieved by the name of the individual or another personal identifier (e.g., unsolicited opinions and general correspondence).

As per section 11 (1) (b) of the *Privacy Act*, designated Minister shall cause to be published an index of all classes of personal information under the control of the government institution that are not contained in PIBs.

Risk: No risk identified.

Compliance Issue: No issue identified.

Institutions' Considerations:

As per section 12(1) of the *Privacy Act*, every Canadian has the right to request access to their personal information under control of a government institution.

Ensure the party responsible for responding to ATIA and PA requests is made explicitly clear.

As per the Directive on Privacy Practices government institutions are required to establish procedures for maintaining a record of new uses or disclosures, as well as any consistent uses that are not reflected in the PIB.

As per section 4.1.7 of the Directive on Privacy Practices they are also required to ensure the development process for new or substantially modified PIBs is aligned with the process for the development and approval of the PIA (see **Use** section above).

If required, ensure the modification of the existing PIB or PIBs to accurately reflect the disclosure and consistent use.

Challenging Compliance:

CDS will direct complaints to the onboarding institution and work with them, when required, to resolve any issues.

Risk: No risk identified.

Compliance Issue: No compliance issue identified.

Institutions' Considerations:

Ensure there is clear guidance on how to manage (where to direct) Notify related complaints.

Risks, Recommendations and Mitigation

a) Privacy Risks and Mitigation Action Plan Table

Risk #	Privacy Principle	Nature of privacy risk	Risk Rating Insignificant, Low, Medium, High, Severe	PMD Recommendation	Management Response (Mitigation Action)	Lead	Planned Completion
1	**Accountability**	Although language was included in the Terms of Use and Service Level Agreement around roles and responsibilities, there is a risk that in the absence of a signed agreement the roles and responsibilities in the event of a security incident, privacy breach complaint or other related issue may be unclear and lead to a longer response time.	2 (likelihood) x 2 (impact) **= 4 (Low)**	PRDD recommended that the documents be signed by onboarding institutions to ensure compliance.	CDS has decided to accept this low risk. Signed documentation with every service owner or central departmental body could create bottlenecks for onboarding services to a platform that CDS has designed and marketed to be as frictionless as possible, with direct communication between the departmental user and CDS. Our user research suggests that requiring signatures and additional upfront paperwork could discourage uptake and does not guarantee compliance. This risk is mitigated by the requirements set out in the GC Notify Security Statement and TOU that organizations agree to follow when they onboard. This includes reporting breaches to CDS and following our process, which are clearly documented on our website. The GC Notify team is also planning to implement a feature that would require users to indicate (e.g., check a box) that they have read the TOU. For non-federal jurisdictions, CDS will be entering into memoranda of understanding to outline the terms for the administration and use of GC Notify, including roles and responsibilities in responding to security incidents and privacy breaches.	CDS	No action required.
2	**Safeguards**	There is a risk that, in the absence of a clear monitoring schedule, the impact of a breach (inappropriate access) may be increased.	2 (likelihood) x 2 (impact) **= 4 (Low)**	PRDD recommended that CDS develop and implement a clear audit log monitoring schedule, in addition to the current alarms system which are triggered in the event of suspected malicious activity.	CDS has decided to accept this low risk and rely on the current alarm system in place.	CDS	No action required.

Conclusion: There are 2 residual low risks and no compliance issues.

ANNEX A – Data Flow Table

Collection					Uses	Disclosure		Retention	
1- Element of Personal Information Collected	**2- Method of collection**	**3- Initially collected by**	**4- Format of the collection**	**5- Purpose of the collection**	**6- Uses of personal information**	**7- Disclosure of personal information**	**8- Transmission method**	**9- Access**	**10-Disposal**
Contact information: Email or phone number	Spreadsheet file (e.g. csv, tsv, ods, xlsx), or API	Department using service (GC Notify Client)	GC Notify collects this data electronically	To send a notification to a recipient's phone number or email address	To send a notification to a recipient's phone or email address To track notification delivery status or investigate an issue	With AWS delivery infrastructure and with the recipient's service provider(s)	Either sent via encrypted request from the departmental IT system to the Notify API or uploaded via spreadsheet to the Notify system, then to AWS, and onward to the recipient's service provider(s)	Specific Notify clients who have permissions to send notifications, to see dashboard statistics, or to manage the API integration on a service. Notify Admins with access to the database and front-end website AWS and Service Provider(s)	In the database, after 7 days or less. Clients can request retention down to 3 days. AWS SNS/SMS is 4 days, regarding status of SMS sent
Template variable data: Clients can voluntarily create recipient-specific variables (e.g., names, appointment date, etc.) to customize content of notifications for recipients	Spreadsheet file (e.g., csv, tsv, ods, xlsx), or API	Department using service (GC Notify Client)	GC Notify collects this data electronically	To personalize a notification to a recipient	To fill out the notification template with custom content for the specific recipient	With AWS delivery infrastructure and with the recipient's service provider(s)	Either sent via encrypted request from the departmental IT system to the Notify API or uploaded via spreadsheet to the Notify system, then to AWS, and onward to the recipient's service provider(s)	Specific Notify clients who have permissions to send notifications, or to manage the API integration on a service. Notify Admins with access to the database AWS and Service Provider(s)	After 7 days or less. Clients can request retention down to 3 days. Clients can also redact template variable data on their own templates so that it cannot be viewed on the dashboard
Networking monitoring and security logs contain IP addresses related to	Infrastructure logs	Notify Admin and sent to AWS Web application for the	Electronic	For logging and auditing, to ensure the security and	Security incidents, events, or breach, or to investigate	AWS and CCCS, Authorities if by court order	AWS: Encrypted, automated logging	AWS, CCCS, Notify Admins with access to the dev environment	Indefinitely (only PII is the IP address of the

GC Notify clients (not recipients). GC Notify users are public servants and not members of the public.		(for the requests sent to the API), CCCS		integrity of the Notify service and infrastructure	malicious activity of the Notify system (IP addresses)		CCCS: Encrypted and automated		sender who is a public servant)
Email address and/or contact information of support ticket requests Voluntarily-provided support ticket details	Contact us form on our website, sent to Freshdesk through API	Notify Website and Freshdesk	Electronic	To answer client questions and provide support	To respond to client questions and provide timely support	Full access: Notify team, CDS Support Team, On call rotation Slack support channel: CDS can preview an email address before the domain and a preview of the ticket	Via Freshdesk, and Notify Support Channel on Slack	Full access: Notify team, CDS Support Team, On-call rotation Slack support channel: CDS can preview an email address before the domain and a preview of the ticket	Freshdesk is indefinitely unless admins delete specific tickets or redact information Slack retention is 1 year unless ticket has PII in which case it is redacted as soon as possible and deleted from Slack

ANNEX B – Privacy Risk Assessment Grid and Non-Compliance Grid

Impact scale

Impacts on individuals / Impacts on the Department		Insignificant	Low	Medium	High	Severe	Definitions of Impact Types
Impacts on individuals	***Physical Security and Financial Harm***	Inconvenience	Short-term injury and/or financial losses that would have **negligible** impact on the individuals	Long-term injury and/or financial losses that would have a **short term** impact on the individuals	Grave and irreversible injury and/or financial losses that would have a **long term** impact on the individuals	Fatalities, significant risk of death or inevitable bankruptcy	Harm to the security of individuals can be in the form of personal injury (physical). Financial harm can be in the form of non-recoverable financial losses or assets losses.
	Psychological Harm	Discomfort	Negligible psychological distress, not requiring professional attention	Short-term psychological distress interfering with the daily activities of an individual which could be addressed with professional attention	Long term psychological distress interfering with the daily activities of an individual and would require long-term professional attention	Permanent and irreversible mental health issues	Psychological harm can be experienced in different forms such as difficulty concentrating, sadness, anxiety, depression, etc.
	Reputational Harm	Inconvenience	Reputational harm that would have negligible impact on the individual	Short-term reputational harm that would have a noticeable impact on the individual	Long term reputational harm that would have serious impacts on the individual	Severe and permanent harm to the reputation of the individual	Reputational harm to an individual can be in the form of public discomfort, embarrassment, loss of respect, social dilemma, character degradation, ignominy and/or social isolation
Impacts on the Department	***Financial Resources or Assets Loss***	up to $100K	$100K - $1M e.g.	$1M - $50M	$50M - $335M	($335M+)	Financial harm can be in the form of non-recoverable financial losses or assets losses. The financial impact scale is in keeping with the Materiality threshold established by CFOB for the purposes of financial reporting.
	Program operations and the delivery of services	Consequences can be absorbed through normal activity	Consequences can be absorbed with managed effort	Consequences could cause significant review on the administration of operations. Impacts to the delivery functions can be minimized by proper management.	Consequences to operations require the intervention of Senior Management or elected representatives. The effective delivery function of the Program is also threatened.	The survival of the program is threatened or a catastrophic failure resulting in a long term service interruption. Event consequences require the Department to make large-scale, long-term realignment of operations.	Impact to the program operations could be in the form of disruptions, delays or interruptions in the delivery of services to client.
	Reputation and Relationships with stakeholders	No effects on the relationship; dissatisfaction from clients and/or the public	Unfavorable media attention **for less than a week**; Noticeable increase in client complaints	Public trust and confidence in the program or service is negatively affected **for up to one month**; potentially subject to negative criticism by the OPC	Embarrassment for the Department ; Subject to an audit and/or investigation by the OPC; strong criticism by government partners/stakeholders **for more than a month up to three months**	Loss of public trust and confidence in the Government **for more than 3 months** that could result in an outcry for the removal of a minister or departmental officials	Reputational impacts could be in the form of criticism, unfavorable media attention or loss of public trust towards government entities, public embarrassment of ministers or senior officials.
	Legal	Legal impacts attributed to legal actions against the department and possible financial settlements. (Legal impacts are a result of other risk events occurring and their associated impacts i.e. harm to individuals or service disruptions.)					Legal Services' risk assessment methodology focusses on the strength of a legal position if challenged in court.

Likelihood scale		1	2	3	4	5
Almost Certain Event is expected; should occur under typical circumstances	5	5	10	15	20	25
Likely Event can be anticipated; could occur under standard circumstances	4	4	8	12	16	20
Plausible Event is deemed plausible; could occur under limited circumstances	3	3	6	9	12	15
Unlikely Event is deemed improbable; could occur under exceptional circumstances	2	2	4	6	8	10
Rare Event is deemed highly improbable; could occur under unique circumstances	1	1	2	3	4	5

Risk rating	
Severe (20-25)	
High (15-16)	
Medium (6-12)	
Low (3-5)	
Insignificant (1-2)	

NON-COMPLIANCE GRID		
Non-compliance with Government of Canada Law or regulation	Non-compliance with Government of Canada directive, policy instruments or procedural documents	Non-compliance with TBS internal directive/policy instruments or procedural documents