PROTECTED B

Privacy Impact Assessment Report for

ESDC Virtual Assistant Chat (EVA)

09/2025

PMD CMS FILE NO. 2025-0248

Table of Contents

Privacy Impact Assessment Template

Section A: Program or activity information

1. Institution and program or activity

Name of institution:
Employment and Social Development Canada, Innovation, Information, and Technology Branch

Name of program or activity: **ESDC Virtual Assistant Foundation - EVA Foundation Branch Initiative PMIS 2024-IITB-134**

2. Multi-institutional program or activity (if applicable)

Appoint a lead institution with overall responsibility for privacy considerations to help reduce gaps and inconsistencies.

Lead institution:	N/A
Branch:	N/A
Directorate:	N/A

3. Officials responsible for completion of the assessment

Identify the executive responsible for the program or activity.

Name:	Mathieu Bergeron
Title:	Director General, Enterprise Digital Solution
Email:	mathieu.bergeron@hrsdc-rhdcc.gc.ca
Telephone:	1-819-654-2708

Delegated privacy official

Name:	Sally Thorpe
Title:	Corporate Secretary and Chief Privacy Officer, Corporate Secretariat Branch
Email:	Sally.Thorpe@hrsdc-rhdcc.gc.ca

4. Program or activity description

Response:

The ESDC Virtual Assistant (EVA) aims to provide a state-of-the-art generative AI service tailored for Employment and Social Development Canada (ESDC) employees.

Employees, as users, will input questions into EVA Chat, the question is then sent to the model, which has been trained on a vast range of text data. The model has been trained by the vendor and will not be trained with ESDC input. The model analyzes the context and semantics of the question based on the patterns it has learned. The model generates a reply by predicting the most likely sequence of words that would complete the interaction, drawing from its training on diverse datasets. While the model leverages advanced algorithms for this process, it's important to note that it produces responses based on probabilities derived from previous data and does not make decisions as a human would.

Moreover, for compliance and auditing purposes, all chat interactions are securely saved in a PostgreSQL database. This chat history can be used for audit purposes and is currently retained for a period of 90 days. If the system's content filter, monitored by Microsoft via their v2 content filter, is triggered, we can review the messages at that time. While there is currently no access to the PostgreSQL database for this purpose, it remains intact for audits or investigations if required.

EVA leverages Azure OpenAI services within a Protected B environment, ensuring compliance with ESDC, Canadian Centre for Cyber Security (CCCS), and Government of Canada standards for accessibility, privacy, and security. Microsoft adheres to privacy standards in compiling their datasets used to train the algorithm, please see Annex F: List of References under the heading ‘References for Microsoft standards and practices’. Unlike existing tools such as OpenAI’s ChatGPT, which have been found to have accessibility, privacy, and security issues by IITB pillars, EVA will adhere strictly to these standards.

EVA is designed to augment and support ESDC employees in their work, enhancing productivity without replacing the essential human elements of workplace culture and ethics. The virtual assistant will offer a comprehensive suite of language services, including advanced text analysis, language detection, text translation, speech-to-text and text-to-speech conversion, and computer vision capabilities for image analysis and interpretation. Support for both official languages, English and French, is integral to EVA’s functionality.

EVA represents a significant advancement in the use of generative AI within ESDC, providing a secure, accessible, and highly functional tool to enhance employee productivity and service delivery, and support employees in their vital roles.

EVA is a new initiative and does not have any dependencies on existing data or systems. EVA Chat is hosted on Microsoft Azure utilizing Azure OpenAI Service and Azure AI Foundry which allows to customize the safety and security of the application.

Content will be annotated by category and blocked according to a set threshold determined by IT security. A slider can be adjusted for violence, hate, sexual, and self-harm categories, to be set at a ‘high’, ‘medium’, and/or ‘low’. The Azure service will generate alerts and send emails to designated groups in charge of chat history. (Please see Annex G fig. 1 for a sample daily prompt progress alert metrics, fig. 2 for a sample blocked prompt error message from EVA Chat and fig. 3 for a sample alert generated by a blocked prompt).

EVA Chat has two distinct collection/usages of personal information:

1. Input data: data, which may include personal information, which a user inputs into the tool in order to generate a response or output. Input data, as well as the accompanying output, is stored in (Microsoft Azure) logs, accessible only by the Automated Infrastructure Team. This information is considered transitory, kept only for 90 days, and not organized in a way so as to be easily retrievable. Input data is not meant to replace primary program collection or storage of personal information, but is meant to facilitate user interaction with the tool.

2. User data: limited personal information collected about users (ESDC employees) for the function of the tool

5. Program or activity scope

The following is in-scope for this assessment of EVA Chat:

- The EVA Chat generative AI tool, its general use by ESDC employees, and its handling and storage of information, including personal information;
- Processes and procedures for logging and monitoring of input and output from EVA Chat;
- Training, Terms of Use, Privacy Notice Statement, user guidance and other EVA Chat-related documentation and communications which advises users on the use and handling of personal information in EVA Chat.

The following is out of scope for this assessment of EVA Chat:

- The use of any other generative AI tool at ESDC, regardless of purpose or function.

6. Requirement for a PIA

Although EVA Chat does not fall under the *Directive on Automated Decision-Making*, and administrative decisions are not directly implicated in EVA Chat's functions or Azure AI Foundry| Azure OpenAI Service's content filtering/monitoring, the use of personal information in EVA Chat, including storage in the logs, is a substantial modification to the handling of personal information. EVA Chat could also represent a substantial modification to the handling of personal information for many ESDC programs. The potential for employees to misuse the tool to assist with or make administrative decisions using personal information in EVA Chat was identified as a potential risk to privacy.

A Privacy Impact Assessment (PIA) is required as per subsection C.2.2.9.3 of Appendix C: Standard on Privacy Impact Assessment of the Treasury Board's *Directive on Privacy Practices* which states that a PIA is necessary "When the official responsible for section 10 of the *Privacy Act* determines that a PIA is warranted given the potential risks associated with any administrative or non-administrative use of personal information" to assess any risks to privacy in the EVA Chat tool.

It is acknowledged that generative AI is developing rapidly at the time of the writing of this PIA, and that evolutions and upgrades to EVA Chat, both planned and unplanned are inevitable. This PIA is intended to remain 'evergreen': to be updated, renewed, revised, rewritten, and reassessed as evolution, changes, updates and upgrades happen to EVA Chat. The AI CoE will keep regular contact with PMD to apprise them of changes to EVA Chat, so that PMD can determine whether a new or revised assessment is necessary.

Section B: Notification and personal information

1. Notification

Response:

A copy of this PIA will be submitted to the Office of the Privacy Commissioner and the Treasury Board Secretariat upon signature. OPC and TBS were notified prior to submission on May 15, 2025, to meet requirements under subsection 4.2.13.2 of the *Directive on Privacy Practices*.

2. Legal authority

1. *List the legal authority to collect personal information, citing the relevant clause(s):*

Response:

In the context of personal information entered as part of input data into EVA Chat by users, EVA's collection, handling, and use of personal information does not fall under a specific legal authority, as it is not a program with a specified goal, but rather a tool that collects, handles, and uses personal as incidental to its primary function of assisting employees with work-related tasks.

Legal authority for the use, handling and storage of personal information from various ESDC programs in EVA Chat is the responsibility of the executives and senior officials who act as the program authorities for each individual program or activity. EVA Chat serves as a technical tool to enable these programs.

Program authorities must ensure that the use, handling, and storage of personal information from the program(s) in their respective charge in EVA Chat is in accordance with Part 4 of the *Department of Employment and Social Development Act* and the *Privacy Act*.

EVA collects user data which is limited personal information collected directly from users in the form of username and date and time of visit. The collection is demonstrably necessary to support security and compliance processes, as described in subsection 4.2.9 of the TBS *Directive on Privacy Practices* and directly relates to the operating of an activity of the institution as described in Section 4 of the *Privacy Act*.

2. *If personal information for your program or programs is collected by another government institution, another jurisdiction, or private sector third party and subsequently disclosed to your institution:*

Response:

EVA Chat may collect personal information initially collected by other institutions incidentally as input data as part of its function to support work-related employee tasks.

The *Directive on Privacy Practices* specifies the responsibilities of executives and senior officials who manage programs or activities involving the creation, collection or handling of personal information. It is the responsibility of individual users and executives and senior officials who manage programs or activities to use personal information collected by other institutions in EVA Chat in accordance with Information Sharing Agreements and Arrangements or other guardrails which would restrict or limit the use, handling and storage of personal information in a tool such as EVA Chat.

In accordance with Section 4.2 of the *Directive on Privacy Practices*, program executives and senior officials are responsible for ensuring that any administrative use of personal information within EVA Chat, especially involving data from other institutions, is authorized, safeguarded, and assessed through a PIA and associated governance structures. This includes ensuring that inter-institutional data sharing complies with existing information-sharing agreements and is properly documented.

Ref.: Directive on Privacy Practices- Canada.ca

3. If the social insurance number (SIN) is collected:

Response:

EVA may collect SIN incidentally as part of input data to support work-related employee tasks. Feasibility analysis is underway to additionally assess options to mask potential SINs before log storage. If adopted, masking would occur at ingestion, preventing cleartext persistence in the PostgreSQL database. Individual users and programs are responsible for ensuring that SIN entered into EVA Chat is entered and used in accordance with prescribed guidelines and legal requirements for that program.

3. Personal information banks (PIBs)

1. Do one or more PIBs already exist for this program?

Response:

Electronic Network Monitoring Logs Bank Number: PSU 905

From EVA's Privacy Notice Statement:

"Any personal information will be managed in accordance with the *Privacy Act* and related policies. You have the right to the protection of, access to, and correction of your personal information, which is described in Personal Information Bank Electronic Network Monitoring Logs (PSU 905). Instructions for obtaining this information is outlined in the following government publication entitled Info Source."

2. *Does a PIB needs to be substantially modified or edited for this program?*

Response:

No, a PIB does not need to be established for EVA Chat as it is not intended to be used for administrative purposes, nor does it make personal information in the logs organized and retrievable by name, number or other identifier assigned to an individual which would create the need to establish one under 4.1.8 of the *Directive on Privacy Practices*.

However, 4.1.9 states that "Heads of government institutions or their delegates are responsible for the following:…Ensuring that a class of personal information is established for any personal information that is under the control of a government institution but that is not intended to be used for an administrative purpose and that cannot be retrieved by the name of the individual or another personal identifier;". Therefore, a class of personal information will be established and registered in Info Source for the use of personal information in EVA Chat and similar tools used in the department.

3. Does a new PIB need to be prepared for this program?

Response:

No, as stated above, a PIB is not required but a class of personal information will be established and registered in Info Source to describe the non-administrative use of personal information in EVA Chat and similar tools used in the department.

4. Handling of personal information

Use the table below to describe the handling of the personal information for both administrative and non-administrative purposes. Describe:

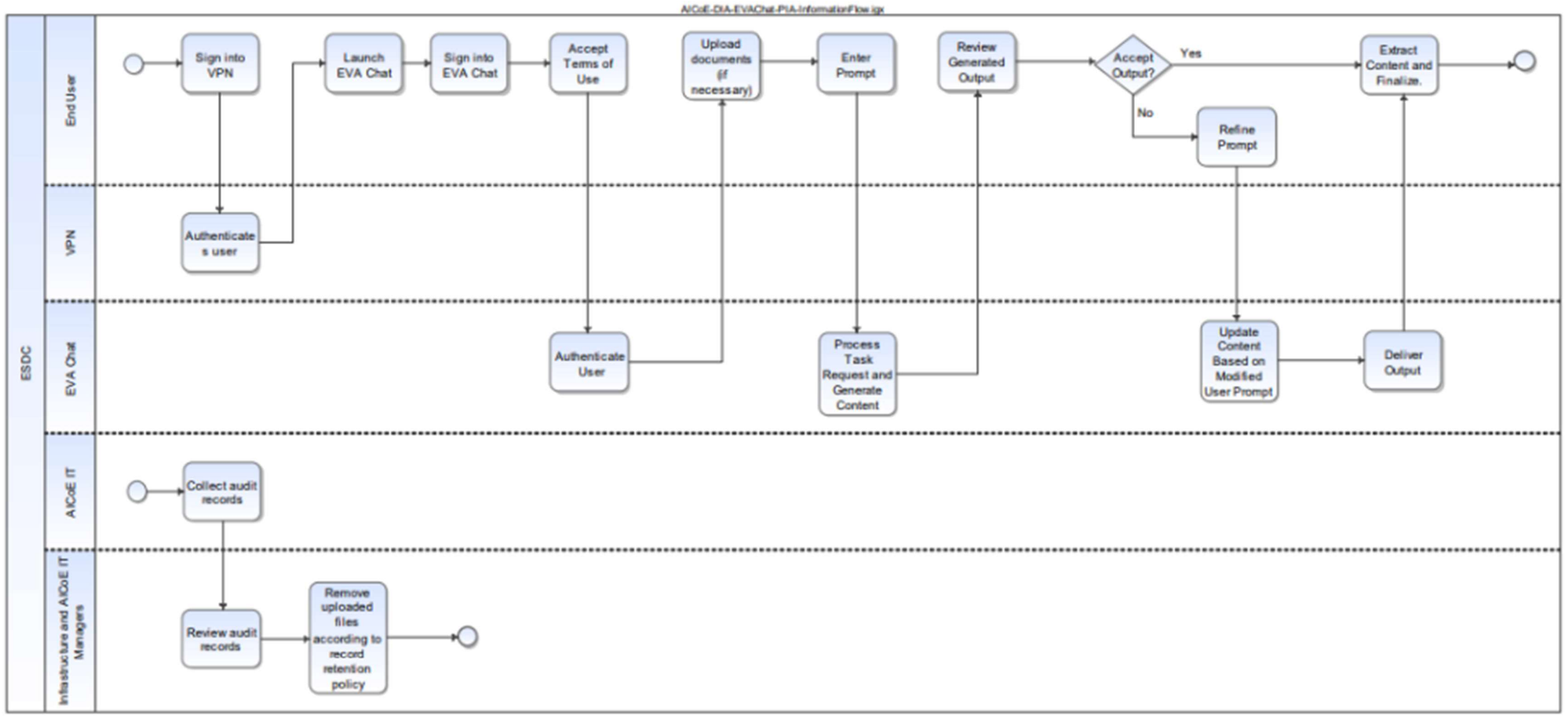
- *how the personal information is being created (includes data linking) or collected (directly from the individual, indirectly from another source, or a combination of the two)*
- *how the personal information will be disclosed: list the entities to whom it will be disclosed and link the disclosure to the purpose of the program*
- *how the personal information will be used and who will use the information: link the use to the purpose of the program*
- *how the personal information will be stored and the retention period for the elements of personal information*
- *how the personal information will be disposed of*

This section should also include the identification of partners that handle the personal information during the administration of your program.

1. Categories of personal information	2. Data Elements	3. Created or collected from (source)	4. Created or collected by	5. Method and format of collection	6. Purpose of the collection	7. Used by	8. Consistent uses*	9. Accessed by	10. Disclosed to*	11. Transmission method (how it is disclosed)	12. Location of storage and retention period	13. Disposed of
AD group members	List of Users	EVA Chat	(Entra ID)	Active Directory Module. Group Identity	Audit trail	Cloud Infrastructure ADmin	Yes	EVA cloud infrastructure Admin	AICoE Director, Manager	SQL	Postgres SQL	90 days (minimum)
Entra ID	Email	EVA Chat	(Entra ID)	Azure AD Group Member	Audit trail	Cloud Infrastructure ADmin	Yes	EVA cloud infrastructure Admin	AICoE Director, Manager	HTTPS	Postgres SQL a	90 days (minimum)
Microsoft Authentication	OAuth Sub	EVA Chat	(Entra ID)	Encrypted Authentication of signings	Audit trail	Cloud Infrastructure ADmin	Yes	EVA cloud infrastructure Admin	AICoE Director, Manager	HTTPS	Postgres SQL	90 days (minimum)
Login/Logout Time	Timestamp	EVA Chat	(Entra ID)	Security Event Logs	Audit trail	Cloud Infrastructure ADmin	Yes	EVA cloud infrastructure Admin	AICoE Director, Manager	HTTPS	Postgres SQL	90 days (minimum)
Network IP	IP Address	EVA Chat	ESDC Cloud Ops	Sign in Logs, Microsoft Defender Endpoint.	Audit trail	Cloud Infrastructure ADmin	Yes	EVA cloud infrastructure Admin	AICoE Director, Manager	HTTPS	Microsoft Azure Logs	90 days (minimum)

* Can include disaggregated data used for program monitoring, evaluation and reporting purposes.

5. Process flow description



Narrative (required): Describe each step of the flow of personal information within the program.

Step number	Description
1. **Accessing EVA Chat**	EDSC employees with a valid government email and VPN connection can access EVA Chat.
2. **Initial Login**	During their initial login to EVA Chat, users must accept the Terms of Use (ToU), which details their responsibilities for handling personal information including ensuring that the information they enter/upload is not above Protected B and that the user has the authority to access and use any personal information they enter into the tool and that they will handle this information in a manner consistent with the original purpose for which the information was collected. This acceptance is also required daily upon each login to the application. Once implemented, users will also asked to certify that they have completed mandatory training on Generative AI which includes a module on EVA.
3. **Data Input and Retention**	After logging in, the user interacts with EVA Chat by inputting queries or uploading documents. The system allows access to chat history which is retained 30 days for chat continuity, with input, output and uploaded documents retained for 90 days. Access to this data is restricted to the individual user and authorized IT personnel. The application does not share input or output between users.
4. **Interaction with the System**	EVA Chat processes user inputs and generates responses based on ungrounded data from the language model, as well as information provided directly by the user.
5. **Use of Information Tool for Insights**	Users leverage the outputs generated by EVA Chat for work-related inquiries and to complete general work tasks such as draft emails. The tool is intended for informational purposes only.
6. **Quarterly Reviews with Stakeholder Groups**	Quarterly reviews are conducted with relevant stakeholder groups - Infrastructure and AICoE IT Managers. These meetings assess usage patterns, audit logs, and compliance measures related to EVA Chat. The collaborative review ensures alignment on best practices for managing personal information.

Section C: Privacy analysis

Rationale and Reasonableness for the use of Personal Information in EVA Chat

Four-Part Test for Necessity and Proportionality

When a new or novel tool processes personal information – especially one using emerging technologies like generative AI – it often raises unprecedented privacy risks (i.e., secondary uses of data, inferences about individuals or repurposing beyond the original collection). The Four-part test is critical because it forces a structed justification for any possible intrusions.

The “Four-Part Test” provides a structured, court-recognized framework for balancing individual privacy rights against the Government’s operational objectives. By applying this Four-part analysis, ESDC ensures that: 1) the use of AI tools serves pressing and substantial public purpose, 2) there is a rational connection between the data used and the stated objective, 3) any privacy impact is minimally impairing and does not exceed what is necessary, and 4) the overall benefits of deploying the tool permitting the use of the personal information outweigh the adverse effects on individual privacy. Embedding this framework into this Privacy Impact Assessment strengthens transparency, supports defensible decision-making and aligns with privacy law and policy requirements.

Necessity

1. Is the measure demonstrably necessary to meet a specific, pressing, and substantial purpose?

Yes.

EVA Chat supports employees in performing their day-to-day tasks more efficiently by allowing them to interact with a secure generative AI assistant that can help draft text, summarize content, translate information, and provide structured answers based on curated prompts. It is a productivity-enhancing tool aligned with ESDC’s digital strategy and mandate to deliver high-quality, timely public services and manage complex internal operations.

The use of personal information in input data is necessary because many ESDC program tasks—such as preparing case summaries, drafting correspondence, and translating client communications—require employees to work directly with personal information that they are already authorized to handle. Prohibiting this would make the tool ineffective for a large portion of real operational needs.

Employees have turned to external chatbots to accomplish this type of work. Without an internal tool that permits the use of authorized personal information, staff are more likely to resort to unapproved platforms that have no safeguards, monitoring, or audit capabilities, thereby creating significant privacy and security risks. Allowing personal information within EVA Chat ensures that this work takes place in a secure, monitored, and compliant environment.

Finally, the collection of limited personal information (e.g., usernames, timestamps, IP logs) as part of user data is demonstrably necessary to enable system security, compliance monitoring, and responsible use auditing. These safeguards provide oversight that do not exist with external tools.

Effectiveness

2. Is the measure rationally connected to the stated purpose?

Yes.

The minimal personal information collected supports user authentication, usage accountability, system performance analysis, and audit functions. This ensures traceability and enables an investigatory response in the event of policy breaches or incidents involving sensitive information. These functions are directly aligned with guidance from the Office of the Privacy Commissioner (OPC), which stresses that AI-enabled systems must include accountability and traceability in their design.

Allowing employees to use personal information they are authorized to handle within EVA Chat has proven effective in shifting work away from unsanctioned, external chatbot platforms. Since launch, over **10,000 employees—more than one quarter of the ESDC workforce—have tried EVA Chat** (in addition to those using Copilot). This uptake demonstrates that EVA Chat is reaching critical mass as a trusted, secure alternative, and is reducing the incentive for staff to risk using uncontrolled AI services.

The public benefit is clear: by giving employees an effective, internally governed tool that can process authorized personal information, ESDC reduces the risk of privacy breaches while improving the timeliness and quality of service delivery. This strengthens trust in government operations and protects Canadians' personal data by ensuring it stays within departmental controls.

Proportionality

3. Is the privacy intrusion minimal and proportionate to the benefits?

Yes.

EVA Chat collects and retains only the personal information needed for core functionality and oversight. Employee-entered input data is ephemeral (retained for 90 days), access-controlled, and subject to Terms of Use. Chat logs are stored only for security monitoring and compliance purposes, with no automated decision-making or profiling of users.

Privacy is preserved by:

- **Requiring** daily acceptance of Terms of Use and adherence to its terms, policies, notices, guidelines and restrictions**.Providing** supplemental training (ETC mandatory training being updated, ETA April 1, 2026).
- **Restricting** log use to compliance and investigation of misuse.

While the potential for privacy intrusion exists through user misuse (e.g., entering unapproved PI or attempting to rely on AI outputs for administrative decision-making), safeguards are in place to minimize this risk, and any such misuse would contravene internal policy.

When viewed from the client perspective, the allowance for limited PI in EVA Chat is proportionate because it **reduces a greater public risk**: the likelihood that employees will expose personal data to uncontrolled external chatbots. Enabling authorized use within EVA Chat—with monitoring, safeguards, and auditability—better protects the public interest than forcing employees to work around restrictions.

Minimization

4. Is there a balance between the benefits of the measure and the impact on privacy rights?

Yes

The operational benefits of EVA Chat—improving efficiency, reducing workload, and enhancing internal service delivery—outweigh the limited and well-managed privacy impacts. EVA Chat does not replace authoritative program systems or hold official records. Instead, it complements existing systems by providing employees with a secure drafting and productivity aid, reinforced with guardrails and oversight mechanisms.

The risk of incidental collection of personal information is addressed through:

- **User accountability** via daily Terms of Use acceptance.
- **Compliance monitoring** and audit logging.
- **Targeted training** (mandatory ETC modules, updated by April 1, 2026) to reinforce what is and is not appropriate for input.
- **Governance alignment** with evolving TBS and OPC guidance, supported by updated PIBs and privacy audits.

Alternatives considered:

- **Prohibiting personal information entirely.** This was rejected because it would make EVA Chat ineffective for real ESDC program tasks, leading employees to either bypass the tool or turn to external chatbots without safeguards.
- **Restricting use only to dedicated "EVA Domains."** While EVA Domains support specific program use cases, employees require a general productivity assistant across diverse tasks. EVA Chat allows this in a secure, controlled environment, minimizing risk.

When compared to the alternative of employees using uncontrolled external AI services, the use of personal information within EVA Chat is clearly the **least intrusive option**. Programs use only the information they are already authorized to handle, within an internal tool that is monitored, auditable, and governed.

Section C.1 – Privacy Principles

1. 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.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
1. Have you documented who within ESDC (senior officials) is/are ultimately accountable for the proper use of the tool?	Yes	The accountability for the proper use of EVA Chat is shared across multiple senior officials depending on their roles and responsibilities. From a **program governance perspective**, each **Assistant Deputy Minister (ADM)** or **Program Authority** is ultimately accountable for ensuring that employees under their authority use EVA Chat in a manner that respects the privacy and security requirements of their respective programs. This includes ensuring that any personal information used within EVA Chat aligns with the legal authority for its collection and use, and that users understand and follow ESDC's policies. From a **technical and operational perspective**, the **Chief Information Officer (CIO)** is accountable for ensuring that the EVA Chat system is developed and deployed in accordance with privacy laws, departmental policies, and guidance from the Treasury Board Secretariat and Office of the Privacy Commissioner. The CIO is responsible for ensuring the system supports auditability, logging, and oversight capabilities to monitor privacy compliance and respond to incidents. Within the CIO organization, the **Director of the Artificial Intelligence Centre of Enablement (AI CoE)** is responsible for the day-to-day oversight of EVA Chat's	As accountability for the use of personal information in the EVA solution lies with the user, and executives and senior officials who have legal authority and bear ultimate accountability for their program or activity's use of personal information, it is essential that all users and officials receive verified, mandatory training to adequately inform them of their responsibilities when using personal information in EVA Chat. There is a risk to privacy that mandatory training has not yet been implemented for EVA Chat. Users are currently able to access EVA Chat without completing training, therefore, they may not understand all responsibilities and limitations to their use of personal information in the tool. Furthermore, there is a second risk that the currently available, optional training is inadequate to inform users and executives and senior officials of their responsibilities when it comes to privacy and the use and handling of personal information in the tool. In the Office of the Privacy Commissioner of Canada's (OPC) *Principles for responsible, trustworthy and privacy-protective generative AI technologies* states that users of generative AI, as parties, should "know and document their legal authority for collection, use, disclosure and deletion of personal information that occurs as part of the training, development, deployment, operation, or decommissioning of a generative AI system."

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		development, configuration, and support, including the implementation of privacy-related controls and user training. This layered accountability model aligns with Section 4.1 and 4.2 of the ***Directive on Privacy Practices***, which requires Deputy Heads and senior officials to ensure that programs and services using personal information meet privacy requirements, and that mechanisms for training, oversight, and incident response are in place. In the context of EVA Chat, users are made aware of their individual responsibilities through the Terms of Use and privacy training, but ultimate accountability resides with senior program and IT officials as described above.	Training must address potential pitfalls that users may not recognize in generative AI which may result in using personal information in ways which are outside of their program or activity's parameters or legal authority, such as implications for information sharing agreements/arrangements and the transformative implications of generative AI, for example, in the OPC's guidance as referenced above it states: "Be mindful that the inference of information about an identifiable individual (such as outputs about a person from a generative AI system) will be considered a collection of personal information, and as such would require legal authority". Training should also address the ultimate responsibility of executives and senior officials for their program or activity's use and handling of personal information in EVA Chat, including guidance on ensuring legal authority is present, through tailored training to these executives and senior officials. Planned training has not yet been reviewed by the Privacy Management Division. Non-mandatory training will not be endorsed by PMD.
2. Have you documented who has control of the personal information within the system?	Yes	Control over personal information within EVA Chat has been documented. Accessor Control has been implemented in the EVA Chat infrastructure where the information is stored. Please refer to the flow diagram in Section 5: Process Flow Description. This has also been documented in the Audit strategy document. (See Annex F) Role-Based Access controls have been established and documented (See section C.4).	Notwithstanding the personal information collected for the function and security of the solution comprising user data, capture of personal information in the tool comprising input data is incidental to the tool's use by employees for work-related tasks. The tool's capture of personal information in the logs has been documented. No privacy risk or compliance issue identified.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		A SharePoint Site has been designated to track meetings and decisions (See Annex F). As an enterprise solution, document control standards vary depending on the specific programs or projects engaged with EVA Chat. Personal information in input data is utilized to provide context for queries directed toward EVA, such as the translation of a document. Importantly, EVA's guidelines, including the Terms of Use (ToU), inform users not to use the output generated by the solution to make administrative decisions without including human input, review and judgement. (See Annex C: Terms of Use & Privacy Notice Statement). EVA does not use personal information for future text generation or to train the algorithm. The user can access their own previous chat, for continuity, for 30 days.	
3. Have you documented who is ultimately accountable for the personal information within the system?	Yes	Responsibility for EVA, including the collection of personal information collected from employees as user data as part of the tool's operations, lies with the IT Director of the AICoE. Accountability for personal information is controlled by "Authoritative System of Record" which means, any Registered User who logs into the system should only input and use personal information that has been authorized to that user. Registered Users are directed to onboarding guidelines that outline the Responsible Use of Generative AI and provide directions on the appropriate use of EVA Chat. A training course has been created and made available to all employees on SABA (See Annex F).	Please see this risk first identified under section 1, question 1. As stated, accountability for the use of personal information in input data in EVA Chat lies with employees of ESDC as individual users and those senior executives and officials who bear legal authority for the programs and activities those employees work under. Both employees and senior executives and officials require mandatory training to understand their roles and responsibilities when using personal information in EVA Chat. Non-mandatory training will not be endorsed by PMD.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		The course is not mandatory in order to be granted access to EVA Chat, but this supplemental training supports the ToU, detailing the do's and don'ts of using the application. Additional information and resources for users regarding privacy are available on the AICoE portal. It is the responsibility of ESDC employees as users to ensure they use personal information in input data in EVA Chat appropriately. In the case of any incidents affecting personal information, such as a privacy breach, the Chief Information Officer (CIO) will hold ultimate accountability from a departmental perspective.	
4. Will any third parties, including private sector third parties, have access to the system or responsibility for the personal information?	No	No third parties, including those from the private sector, will have access to personal information. An agreement is in place with service provider Microsoft, which details that they have no access to any personal information stored in EVA Chat. Additionally, the EVA application is secured by Secure Cloud Enablement Defense (SCED), which is managed by Shared Services Canada (SSC). SSC also will not have access to any information, including personal information, within EVA Chat.	No privacy risk or compliance issue identified.
5. If third parties will be involved, do you have a written record (arrangement, agreement or contract) of understanding in	N/A	N/A	N/A

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
place that establishes privacy requirements?			
6. Will the institution be provided with the results of regularly scheduled audits and compliance checks on the privacy requirements of all involved parties?	No	Cyber Security has confirmed that EVA Chat will be monitored through the department's Security Information and Event Management (SIEM) system. This includes tracking anomalies in data flows and infrastructure logs and ensuring timely triage and investigation of potential security and compliance issues. These findings are reported to the subscription owner, maintaining accountability and oversight. Azure infrastructure logs (which do not contain personal information) and the PostgreSQL database and volume file storage (which may contain user-entered content and uploads) are also monitored by the Automated Infrastructure Team. These logs can be used to trace when personal information is used. More clarity around the specificity on how the processing of personal information in chat interactions must be flushed out to develop a solution for additional reporting. This creates a **traceability gap** regarding how, by whom, and for what purpose personal information is used within EVA Chat—particularly in generative outputs that may include inferred or sensitive information such as SIN. In line with the **Office of the Privacy Commissioner's 2023 principles for responsible, trustworthy and privacy-protective generative AI technologies**, ESDC acknowledges that **traceability and explainability are essential components of responsible AI deployment**. As such, **IITB should take appropriate steps to ensure that outputs from EVA Chat are either traceable and**	There is limited oversight and auditability of how personal information in input data is used in EVA Chat, including how, by whom and for what purpose, including sensitive personal information such as SIN. There is a general risk that specific risks to privacy may go unidentified due to this gap in information and limited oversight. Without defined activities which audit and monitor the use of personal information in EVA Chat, including identifying cases where personal information has been used to make or assist with an administrative decision, misuse could go undetected. Current auditing and monitoring activities should be expanded to encompass use and handling of personal information in EVA Chat to first, create data on how personal information is being used in EVA Chat, and second, to then use that data to identify any gaps or risks related to use of personal information in the tool, including misuse. As auditing, monitoring and investigative processes of the Automated Infrastructure Team have not yet been finalized, drafts of their processes could be modified to incorporate considerations of auditing, monitoring, and investigating the use and handling of personal information in EVA Chat. Since AI is rapidly evolving, it is imperative that changes or updates to EVA Chat are monitored, and new or renewed privacy assessments conducted when required. In addition to establishing a process for monitoring the use of personal information in EVA Chat, a reporting process to update PMD regularly of any changes to EVA Chat or it's environment should be established for the life of the tool.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		explainable or, where explainability is not technically feasible, explicitly disclose that limitation to users and program authorities. This ensures transparency, aligns with privacy best practices, and upholds the integrity of administrative decision-making processes supported by AI tools. Although EVA Chat does not currently generate outputs that are consistently explainable in the technical sense (due to the nature of large language models), user education, auditability of user interactions, and system-level logs help to support accountability. These safeguards should be further developed as the tool matures.	

2. Limiting collection

Personal information should only be collected as necessary for the purposes that the organization has identified. This includes limiting the amount and type of information. The information should be collected by fair and lawful means.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
1. Will the personal information collected by the system be used in any way? Describe how the personal information will be used.	No	Information, including personal information, inputted into EVA Chat by users (ESDC employees) in the form of prompts and uploads, will be used by EVA Chat's algorithm to generate output (responses to prompts). Information, including personal information, will be stored by the system for 90 days as per departmental practices. Only IT administrators will have access to these logs under prescribed circumstances. Individual users will have access	As accountability for the handling of personal information is controlled by an "Authoritative System of Record" as detailed in section 1, question 1 above, the onus for use of personal information is on the user. The user is expected to only access, input and use information they have a 'need to know' as part of the duties of their position. Users are expected to use information in EVA in ways they are authorized to use it. Any potential new collection, overcollection, or modification of collection is the responsibility of the user and their respective program, and the executives and senior officials responsible for that program.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		to their own chat logs, for 30 days, in order to facilitate continuity of chat with EVA's interface. An ESDC employee's chat history or uploaded information will not be used in any manner to train the model or generate output. An excerpt from the agreement with Microsoft: "Data, privacy, and security for Azure OpenAI Service - Azure AI services | Microsoft Learn Important Your prompts (inputs) and completions (outputs), your embeddings, and your training data: • are NOT available to other customers. • are NOT available to OpenAI. • are NOT used to improve OpenAI models. • are NOT used to train, retrain, or improve Azure OpenAI Service foundation models. • are NOT used to improve any Microsoft or 3rd party products or services without your permission or instruction. • Your fine-tuned Azure OpenAI models are available exclusively for your use. The Azure OpenAI Service is operated by Microsoft as an Azure service; Microsoft hosts the OpenAI models in Microsoft's Azure environment and the Service does NOT interact with any services operated by OpenAI (e.g. ChatGPT, or the OpenAI API)."	However, there is a risk that communications to users and training which address their responsibilities do not adequately address potential impact to the user's program, such as the possibility of violating the terms of an Information Sharing Arrangement/Agreement. Training and communications should be more explicit about the potential consequences of the use of a program's personal information in EVA Chat may have. See this risk first identified in section 1, question 1.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
2. Have you documented the reason(s) for the collection of personal information?	Yes	EVA Chat allows for the entry and upload of Protected B information, including personal information, in order to provide context so the tool can respond to prompts and assist users with their work tasks. Operating within a Protected B environment ensures effective control over access and monitoring of use, safeguarding sensitive information. This structure allows for the efficient use of generative AI tools, enabling quick responses to user inquiries while implementing necessary security measures. By prioritizing security and oversight, a reliable service is delivered that aligns with the growing demand for advanced support solutions, reinforcing the department's commitment to protecting user data and fostering trust. Input data entered into EVA Chat may contain personal information (up to Protected B) as part of user prompts and uploads which are then used by the tool to generate output to assist users with their work. Collection of personal information by the tool through input data is incidental to EVA Chat's use. User data is personal information about ESDC users collected for functional, monitoring and security purposes.	While the Protected B, isolated environment of EVA Chat addresses security risks, the incidental capture and use of personal information in the tool does not conform to best practices for handling personal information with generative AI from a privacy perspective as described in the Office of the Privacy Commissioner (OPC)'s *Principles for responsible, trustworthy and privacy-protective generative AI technologies* which states that use of personal information in a generative AI tool should be "necessary and proportionate" and "the tool should be more than simply potentially useful" (please see section 10, question 7 for further review in the context of the OPC's Principles document). With some exceptions, users should be able to obtain the results they need to facilitate their work tasks from EVA Chat without inputting or uploading personal information, or by replacing personal information with 'dummy'/placeholder information. Due to currently limited oversight and auditability of how personal information is being used entered and handled in EVA Chat, it is not clear if use of personal information in EVA Chat presents a specific risk to privacy. However, it is advised that training and communications should encourage less intrusive practices, such as limiting use and de-identification of personal information in the tool, whenever possible.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
3. Are all the personal information categories listed in the relevant personal information bank (PIB)?	Yes	Information is collected directly from users in accordance with Electronic Network Monitoring Logs (PSU 905) PIB. The following is an excerpt from the Privacy Notice Statement (PNS), which is part of the ToU: "Any personal information will be managed in accordance with the *Privacy Act* and related policies. You have the right to the protection of, access to, and correction of your personal information, which is described in Personal Information Bank Electronic Network Monitoring Logs (PSU 905). Instructions for obtaining this information is outlined in the following government publication entitled Info Source."	User data is personal information collected from users by EVA Chat for the function and security of the tool, which is covered by PIB PSU 905. All other personal information captured by the tool is incidental, not collected purposefully, but as part of prompts, uploads, or output. None of this personal information, present in input data which is then captured in the logs, falls under collection as described in a PIB. No privacy risk or compliance issue identified.
4. Will personal information be collected indirectly, meaning from a source other than the individual that the information is about?	N/A	N/A	N/A
5. If the personal information is collected indirectly, will it be collected with consent from the individual?	N/A	N/A	N/A
6. If the personal information will be collected indirectly without consent, is the collection a result of a disclosure under subsection 8(2) of the Privacy Act?	N/A	N/A	N/A

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
7. If the personal information is collected indirectly without consent, will the information be used to make a decision about the individual?	N/A	N/A	N/A
8. If the personal information will be collected indirectly without consent, could direct notification to the individual result in the collection of inaccurate information?	N/A	N/A	N/A
9. If the personal information will be collected indirectly without consent, could direct notification of the individual defeat the purpose or prejudice the use for which the information is collected?	N/A	N/A	N/A
10. Will consent require a positive action, that is, a written agreement or signature, by an individual rather than being assumed as a default (implied) consent?	N/A	N/A	N/A
11. Have all efforts been made to minimize the collection of data elements?	N/A	N/A	See response to question 2 above.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
12. Are there consequences to the individual as the result of a refusal to consent?	N/A	N/A	N/A
13. Are there mechanisms to permit individuals to withdraw their consent?	N/A	N/A	N/A
14. Will other federal institutions, other jurisdictions or private sector third parties be collecting personal information on behalf of your institution?	N/A	N/A	N/A
a. If yes, will they present the privacy notice at the time of collection?	N/A	N/A	N/A
15. Will the program involve collection of personal information through a common client identifier?	N/A	N/A	N/A
16. Are there mechanisms in place to ensure that the individual has the capacity to give consent?	N/A	N/A	N/A
17. Can personal information be collected from a person authorized to act on behalf of the individual?	N/A	N/A	N/A
18. Are standards and mechanisms in place to ensure the	N/A	N/A	N/A

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
recognition of persons authorized to make decisions on behalf of others (for example, a minor or incapacitated person)?			

3. Limiting use

An organization should identify the purposes for collecting information at or before the time of collection. This will enable the organization to determine which information needs to be collected to meet their needs. An organization should not use personal information for new purposes, unless it has the consent of the individual, or as required by law.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
1. Will personal information entered into the system be used exclusively for the reason(s) it was collected?	Yes	Personal information entered into EVA Chat—whether as part of system logs or user-generated content—is intended to be used exclusively for the purposes for which it was collected. These purposes include enabling user access, supporting accountability, investigating misuse, and enhancing service delivery through employee productivity tools. EVA Chat is not used for profiling, automated decision-making, or secondary use of personal data. To ensure this limitation of purpose is respected, the following measures are in place: • **Access control:** Personal information entered into the system as input data (e.g., chat content, uploads) is accessible only to the employee who generated it or to authorized IT	Personal information as part of input data is collected in logs by EVA. It is the responsibility of users and their respective program authorities to ensure that personal information in chat input and output will be used exclusively for the purposes it was collected, including consideration of whether use of generative AI is appropriate. However, there is no current method, such as auditing or monitoring of collection and use of personal information, which can determine if personal information, captured incidentally as part of employees' use of the tool, is being used for the reason it was collected. Please see the answer to section 1, question 6 regarding this risk. Although not explicitly a risk or issue, **PMD advises IITB to adjust the wording of the notice to users under the chat input box to read "EVA Chat, like all LLMs, can make mistakes. There are risks associated with relying on output from EVA Chat. Verify**

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)

		personnel under specific and auditable circumstances (e.g., incident investigation).
		• **Terms of Use enforcement:** Upon first sign-in and at the start of each session, users must confirm their agreement to the Terms of Use (ToU). These ToU explicitly state that:
		  ○ EVA Chat is approved only for data up to **Protected B**.
		  ○ It must not be used to replace **subject matter expertise**.
		  ○ Users are accountable for verifying the **accuracy and appropriateness** of AI-generated content.
		  ○ EVA must **not be used to make or support administrative decisions** involving individuals.
		• **Minimal and purpose-bound collection:** Only minimal personal information about users (e.g., login ID, timestamp, activity logs) is collected as user data for system function, compliance monitoring, and security. These are not repurposed for unrelated uses.
			important information. Do not use EVA Chat to make or support administrative decisions involving individuals."

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)

		• **User awareness of system limitations:** In alignment with the **OPC's Principles for responsible, trustworthy and privacy-protective generative AI technologies**, IITB is taking steps to inform users of **known risks and limitations**, including:
		  ○ That EVA Chat may generate **incorrect, misleading, or outdated information**.
		  ○ That certain inputs or use contexts (e.g., legal interpretation, critical program decisions) are not appropriate for generative AI tools.
		  ○ That the system does not support **explainability** or traceability of how responses are derived in every case.
		These risks and limitations are documented in training materials, terms of use, and internal communication campaigns, and will be expanded over time as part of IITB's AI awareness strategy.
		In the EVA Chat application under the box for user chat input the notice "LLMs can make mistakes. Verify important information." appears.	

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
2. Do you have processes in place to ensure that personal information will be used only by or disclosed to individuals who have a need to know in the system (including within your institution and any receiving public sector organization or third parties)?	Yes	Users who enter personal information into EVA Chat as input data are presumed to have a right of access to that information under an authoritative System of Record. In the Azure platform and Azure DevOps environment, strict compliance is maintained with AC-6 security controls by applying the principle of least privilege. Users are categorized into three types: Owners, Contributors, and Readers. The Reader role in Azure is designed explicitly to embody the principle of least privilege. Readers have read-only access and are permitted to view all resources but cannot make any changes within a specific scope. This restricted role is crucial in minimizing potential security risks, as it limits each user to the access necessary for their tasks. On the EVA project team, a similar Reader role is enforced, where users can view project information, including the codebase, work items, and other artifacts, but cannot modify them. This application of least privilege bolsters overall system security and integrity. The EVA Chat application has two roles: Users and Admin. Everyone who is part of AD, and has an Entra ID can become a user of EVA Chat. Users will only have access to personal information stored in their own chat history, for the purposes of maintaining chat continuity with	Processes of the Automated Infrastructure Team, including processes to audit, monitor and investigate collection and handling of personal information, as well as potential misuse of personal information in EVA Chat, have not been established. See section 1, question 6, for first identification of this risk.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		the tool, which will remain accessible for 30 days from chat input.	
3. Will personal information be used for a purpose that is not identified in the relevant PIB?	No	User data, personal information about users, is collected for functional, monitoring and security purposes which are identified in Electronic Network Monitoring Logs (PSU 905).	No privacy risk or compliance issue identified.
4. Will the personal information be used for any consistent uses?	No	User data collected by EVA Chat "may be used to substantiate any disciplinary action taken where violation of institutional policies or the Policy on the Use of Electronic Networks is determined, and to support compliance with other relevant Treasury Board policy instruments or policy directions" as described in PIB PSU 905, when identifying misuse of the tool by employees and substantiating disciplinary action such as removal of access to EVA.	No privacy risk or compliance issue identified.
5. Will personal information be used for any secondary uses?	No	User data collected by EVA Chat will not be used for any secondary uses which are not described in PIB PSU 905.	No privacy risk or compliance issue identified.
6. Will there be any new uses of personal information previously collected that are directly connected to the system's original purpose?	No	EVA Chat will not directly create a new use of personal information. New uses of personal information that may result from the input or use of personal information in EVA are the responsibility of the user. as prescribed by their program, project or activity.	There is no specific, described new use of personal information in the use of input data and its entry or upload in EVA Chat. However, users may intentionally or unintentionally create new uses of personal information through their interaction with the tool. As an example, in TBS's *Guide on the use of generative artificial intelligence* it states "…a summary of an application for a service or benefit produced by a generative AI tool could constitute new personal information". New uses of personal information are the responsibility of the employee as a user and the senior executives or officials who bear accountability for the program or activity.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
			Without adequate, mandatory training there are risks that users may not understand limits on the use of personal information in the EVA Chat and may not recognize when they have created a new use of personal information. See section 1, question 1 for first identification of these risks.
a. If yes, could individuals reasonably expect their information to be used for that new purpose?	N/A	N/A	N/A
7. Will the personal information be used in a way that involves technology that either assists or replaces the judgment of human decision makers? An example is a system, tool or statistical model that makes an administrative decision or a related assessment about a client, with or without human review.	Yes	EVA allows a user to hold a 'conversation' with the tool. EVA will answer questions and reach conclusions using uploaded or typed input for context. It can generate different creative formats, format emails, summarize documents etc. It does not automate processes or execute any scripts or programs. EVA does not independently make administrative decisions. EVA supports informed decision-making by providing relevant information, analysing data and trends, outlining the pros and cons of different options, offering scenarios for consideration, and summarizing research findings to help evaluate options effectively. The onus to not use EVA to make or assist with administrative decisions lies with the user. Several initiatives have been implemented to ensure users understand the appropriate use of EVA and the importance of human oversight. Clear Terms of Use outline EVA's intended use	EVA Chat generates responses to user input and uploads which may involve the use of personal information. Although EVA is not intended to assist with or make administrative decisions there is a risk that ESDC employees, as users, could use it for that purpose. Training should ensure that users have a clear understanding that EVA's outputs are not to be used to make administrative decisions but should also integrate privacy training to ensure that users understand: 1) what is personal information and 2) what is an administrative decision, so that they are equipped to identify situations where the judgement of the tool is assisting or replacing their own. Please refer to section 1, question 1 for first identification of this risk.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		and limitations. A non-mandatory course on EVA Chat and Microsoft Copilot which speaks to effective usage and the necessity of human discretion in decision-making, is available. Training on Generative AI, including EVA Chat, is planned to be integrated into the mandatory Essential Training Curriculum for ESDC employees. An optional course on for ESDC employees that is also available. Additionally, users are directed to relevant resources and regular reminders are posted in community forums to reinforce responsible usage and the need for maintaining human involvement in decision-making processes.	
a. If yes, will you comply or have you complied with the Directive on Automated Decision-Making?	N/A	N/A	EVA Chat's Terms of Use advise users not to use EVA Chat to make administrative decisions. ESDC's Responsible Artificial Intelligence and Data Ethics (RAIDE) Team was consulted and stated that they were unable to complete an Algorithmic Impact Assessment on EVA Chat as uses of the tool by ESDC employees, as users, are not precisely defined.
8. Will the personal information be used for planning, monitoring and evaluation purposes or for reporting purposes?	Yes	User data collected by EVA Chat from users will be used to monitor the function and security of the tool.	No privacy risk or compliance issue identified.
9. Are there safeguards in place to ensure that only personal information needed for these purposes is made available to those with a need to know for their work?	Yes	Existing safeguards, individual to respective programs, ensure that ESDC employees only have access to that information which they need to know in order to complete their work tasks. As input is not used to train the model and individual users only have access to their	Processes of the Automated Infrastructure Team, including processes to audit, monitor and investigate collection and handling of personal information, as well as potential misuse of personal information in EVA Chat, have not been established. See section 1, question 6, for first identification of this risk.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		own chat history, a user will have no ability to access any information inputted or uploaded into EVA Chat by another user. Access to personal information collected by EVA, either directly by the tool or incidentally as part of user input, in the logs is only accessible to IT administrators under prescribed circumstances using role-based access to limit availability. EVA's ToU, which must be accepted each day in order to access and use EVA, contains the following wording in the PNS section: " 4. All users are responsible for the content they upload or create using EVA Chat. EVA does not modify uploaded documents. 5. Before uploading **Protected B** information, users must ensure they have the authority to do so and that its use is consistent with the original purposes for which the information was collected or created."	

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
10. Will the personal information be used for the training, testing or refinement of artificial intelligence systems?	No	ESDC employee (user) chat or uploaded information will not be used in any manner to train, test or refine the model. EVA maintains conversation continuity by use of a context window, which allows it to use both the large language model and user context to generate new content. Within a session EVA Chat can use previous responses to generate new text. The chat can be accessed in this way by the user for 30 days. The chat history is not used to train the model or any other system. If user enters a new session they will have to provide context to the tool again to generate content. An agreement with Microsoft outlines that they will not use ESDC data in any shape or form. ESDC data in EVA Chat will only reside in the Canada East Data Centre. Periodic updates to the model will come from Microsoft but will not involve any information taken from ESDC input.	No privacy risk or compliance issue identified.
a. If yes, will you comply or have you complied with the Directive on Automated Decision-Making?	N/A	N/A	N/A
11. Will personal information be used for conducting	Yes	User data gathered by the tool from users, such as time of use, may be used for investigative	Processes of the Automated Infrastructure Team, including processes to audit, monitor and investigate collection and handling of personal information, as well as potential misuse of personal

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
investigations or enforcement activities?		purposes when issues of potential misuse has been identified. Personal information captured incidentally in the logs as part of input data will not be used directly but may be used in investigations into misuse of the tool, subject to ESDC policy and guidelines.	information in EVA Chat, have not been established. See section 1, question 6, for first identification of this risk.
12. Will personal information elements, such as a SIN or any other identifying number or symbol, be used for the purposes of linking across multiple databases?	No	There is no linking of databases implicated in EVA Chat.	No privacy risk or compliance issue identified.
13. When data will be matched for an administrative purpose, will it be consistent with the stated purposes for which the personal information is collected?	N/A	EVA Chat does not match data for an administrative purpose. Users must follow the ToU and are responsible for following guidelines established by their respective programs for data matching activities.	Accountability for the use of EVA Chat to perform data matching activities lies with employees, as users, and the senior executives and officials who bear legal authority for those users' programs or activities.
14. Is there an activity log attached to the personal information record to document uses and disclosures that are not listed in the relevant PIB?	N/A	All uses and disclosures are listed in the relevant PIB.	No privacy risk or compliance issue identified.
15. Will the program result in an increased ability to undertake surveillance or monitoring?	No	Content filtering will allow defined input which falls under violence, hate, sexual, and self-harm categories into EVA Chat to be blocked and monitored by automated alerts. EVA Chat	User usage monitoring is in line with other surveillance and monitoring activities of the department to ensure employee compliance and support IT security measures in the usage of departmental tools.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		will not create an increased ability for surveillance and monitoring outside of the tool.	No privacy risk or compliance issue identified.
16. Will the system, software or program application use any tracking methods, such as cookies, to collect personal information about users and their transactions?	No	No specialized tracking methods are used for EVA Chat.	No privacy risk or compliance issue identified.

4. Limiting disclosure

Personal information shall not be used or disclosed for purposes other than those for which it was collected or for uses consistent with those purposes, except with the consent of the individual or as required by law.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
1. How will the disclosure of personal information be limited to the system?	N/A	EVA is hosted in ESDC's secure Microsoft Azure cloud environment located in Canada approved by CCCS for Protected B information. The system is configured for internal ESDC use only and is accessible to employees through the department's network or VPN. It uses private connections and restricted settings so it cannot be reached directly from the public internet. The Azure OpenAI service also operates in these secure Canadian datacentres but is shared with other Microsoft customers. This setup meets all Government of Canada security requirements and it is managed	No privacy risk or compliance issue identified.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		through IITB security reviews and continuous monitoring. Because user input and file uploads are not used to train the model, and each user can see only their own chat history, personal information cannot be shared between users. Administrators can view logs only when authorized, as described in Annex F on Role-Based Access.	
2. Will personal information be disclosed for a reason or reasons not identified in the relevant PIB?	No	All disclosures of personal information related to user data are identified in the relevant PIB: Electronic Network Monitoring Logs (PSU 905)	No privacy risk or compliance issue identified.
3. Has consent been obtained for personal information that will be used or disclosed for a secondary purpose that has not previously been identified in the relevant PIB?	N/A	N/A	N/A
4. If personal information is disclosed without consent, has the specific authority for the disclosure been identified?	N/A	N/A	N/A
5. Will personal information be disclosed with other federal institutions, other jurisdictions	N/A	N/A	N/A

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
or private sector third parties? If so, identify them.			
6. Do you have an information-sharing agreement (for example, a memorandum of understanding, an accord, an arrangement or a contract) with another federal institution, other jurisdiction, or a private sector or third party?	N/A	N/A	N/A
7. Have formal information-sharing provisions been established on the use, retention, disclosure and safeguarding of personal information?	N/A	N/A	N/A
a. Do these provisions include security incident or privacy breach management?	N/A	N/A	N/A
8. Will any identifying number, symbol or other particular assigned to an individual, such as a SIN, be disclosed?	N/A	N/A	N/A
9. Will personal information be disclosed for data-matching purposes?	N/A	N/A	N/A

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
10. Will personal information be used, disclosed or retained outside Canada?	No	Information is stored at the Canada East Data Centre.	No privacy risk or compliance issue identified.

5. Retention or disposal

Personal information should only be retained as long as is necessary to fulfill the organization's stated purposes. An organization should develop specific guidelines and procedures governing the destruction of personal information.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
1. Is there a retention schedule?	Yes	EVA stores all data for 90 days (with the exception of individual user chat continuity history, which is only accessible by the user who created the input, for 30 days), as it is considered transitory information, with primary storage of personal information remaining in the hands of programs and activities. Currently, disposal processes happen manually through a quarterly meeting, although there is a plan to eventually automate these processes. Data in the logs may be retained longer than 90 days in cases of investigation into suspected misuse of the tool or in response to Access to Information Requests and/or Privacy Requests.	No privacy risk or compliance issue identified.
2. Are there procedures in place for the disposal of personal information?	Yes	Information that is generated and collected by EVA in response to input data is transitory. Data is retained for 90 days for chats, uploads and logs, including information collected about	There is a risk that, in the absence of automated processes for disposal, personal information in the logs due to input data and accompanying output may be kept by EVA Chat longer than is

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		users. Quarterly meetings are held between IT Managers, Senior TA from Infrastructure and the AICoE team to review Audit records and the record retention policy. During this meeting the logs of chat input, output and uploaded files are removed from the fileshare following departmental processes. Eventual automation of this process is planned.	required. It is recommended to establish automated disposal processes.
3. Is there an accurate and up-to-date Records Disposition Authority (RDA) in place?	Yes	Information stored in EVA Chat's logs is transitory, therefore it is disposed of as per the RDA *Disposition authorization for transitory records (2016/001)* which was updated in 2022.	No privacy risk or compliance issue identified.

6. Accuracy

In order to meet the intended purposes, personal information should be accurate, complete and up to date. This principle aims to minimize the possibility that incorrect information is used to make a decision about an individual. This also applies to information disclosed to third parties.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
1. Are there procedures to ensure that personal information is as accurate, complete and up to date as possible?	No	N/A	No privacy risk or compliance issue identified.
2. Will you ensure accuracy through all reasonable steps, including:	No	N/A	No privacy risk or compliance issue identified.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
a. Through direct collection or validation with the individual?			
b. By obtaining information from trusted sources (either public or private) and verifying accuracy against existing personal information before use?	Choose an item.	N/A	N/A
c. With a personal information matching program to verify personal information against a trusted source where authorized or where consent was obtained?	Choose an item.	N/A	N/A
3. Is there a process in place for correcting inaccurate information?	No	N/A	N/A
4. Will third parties to whom personal information has been disclosed, be notified (automatically or not, through procedures in place) of changes to those records?	N/A	N/A	N/A

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
5. Are there processes or protocols in place to monitor changes to records of personal information?	N/A	EVA Chat has no capacity to modify records containing personal information held by programs. Administrators cannot modify logs containing personal information of users.	N/A
a. If yes, does the record indicate the changes made and the date of each change?	N/A	N/A	N/A
6. Is a record kept regarding: a. Requests for a review of errors or omissions?	N/A	N/A	N/A
b. Corrections or decisions to not correct?	N/A	N/A	N/A
7. Do you ensure accuracy by technological means to identify keystroke errors and discrepancies?	N/A	N/A	N/A
8. Are there documented procedures for how to respond to requests to correct personal information?	N/A	N/A	N/A
9. Are systems designed to ensure that an individual has been notified that a correction has been made to their information?	N/A	N/A	N/A

7. Safeguards

An organization should implement appropriate security safeguards to protect the personal information collected. The appropriate safeguard should be determined by the sensitivity, amount, distribution, format and method of storage of the information. Employees in the organization should be aware that confidentiality of personal information should be maintained.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
1. Will privacy training be provided to employees?	Yes	A specialized course has been developed in collaboration with the College at EDSC and is available to employees. Generative AI training is planned to be integrated into the mandatory Essential Training Curriculum for ESDC employees. Additional courses specific to privacy and AI are available through EDSC and CSPS, links are available through the AICoE platform. It is mandatory for a user to accept the ToU once per day when signing in to EVA Chat.	There is a risk that without mandatory training users will not fully understand the requirements and responsibilities on them to safeguard privacy in EVA Chat, see risk related to absence of mandatory training first identified in section 1, question 1. There is also a concern that the current training, which covers both EVA Chat and Microsoft Copilot, may lead to user confusion, as the tools are similar but permit different levels of input (e.g., up to Protected B information is permitted in EVA Chat but not Microsoft Copilot). Such conflagration may lead to an increased risk of breach of personal information for the department. Please also see risk related to inadequacy of training identified first under section 1, question 1.
a. If yes, is there specialized training provided for this specific program?	Yes	Optional training is available on SABA which addresses EVA Chat and Microsoft Copilot and has been designed with the College at EDSC. Generative AI training is planned to be integrated into the mandatory Essential Training Curriculum for ESDC employees. Additionally, AI Education Resources are available on the AICoE portal, providing supplementary information and guidance for employees using EVA Chat. Users must agree to the ToU, which outlines privacy requirements and specify the dos and	See risks described above.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		don'ts of using the EVA application. (See Annex F)	
2. Have security procedures for the collection, transmission, storage and disposal of personal information, and access to it, been documented?	Yes	A full SA&A has been completed. This security assessment was based on a Security Controls Traceability Matrix (SCTM) with 190 controls, of which: • 132 controls were met • 13 controls were partially met • 8 controls were not met • 37 controls were not applicable and were out of scope 1.RA-5 Vulnerability Scanning (ST&E Security Testing) is in progress, currently IT security has not seen, highs, or mediums, only some lows that are false positives, 2.2 Controls related to Audit Trails: Cyber security confirmed that they will monitor alerts from Sentinel SIEM tool for EVA Chat. This will include analysis of audit records, eliminate false positives, etc. (See Annex F) 3. 5 Controls identified relate to Incident Management. An incident management document has been prepared for EVA. (See Annex F)	No privacy risk or compliance issue identified.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		All traffic will be routed through Secure Cloud Enablement Defense (SCED) managed by SSC. It cannot be accessed outside ESDC.	
3. Have all required Authorities to Operate (ATOs) been granted?	Yes	The full ATO for EVA Chat was granted.	No privacy risk or compliance issue identified.
4. If the ATO was granted “with conditions,” is there a mitigation plan in place and a timeline for completion?	Yes	An SA&A Risk Mitigation Plan has been completed and approved by IT Security.	No privacy risk or compliance issue identified.
5. Have all security assessments, authorizations, threat and risk assessments, or their equivalents, been completed in consultation with the departmental information management or information technology security team?	Yes	As detailed under question 2 above, A full SA&A has been completed with ESDC IT Security. 8 Controls were identified as not met in the SA&A, for which a Risk Mitigation Plan was developed. RA-5 Vulnerability Scanning (ST&E Security Testing) is in progress. At this times IT security has only seen lows, which are false positives. Cyber security has confirmed that they will monitor alerts from the Sentinel SIEM tool for EVA Chat. This will include analysis of audit records, elimination of false positives, etc. An incident management document has been prepared for EVA. (See Annex F)	No privacy risk or compliance issue identified.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
6. Will controls be in place for all processes to grant authorization to modify (add, view, change or delete) personal information from records, upon implementation?	Yes	EVA has Role-Based Access Control established, documented and in place (see section C-4, and Annex F). Program-related personal information captured in the logs is incidental and cannot be modified. The logs are retained in their original form. Chat history cannot be altered, only accessed for auditing or investigative purposes. Admin cannot modify logs.	No privacy risk or compliance issue identified.
7. Will security measures be in place to match the sensitivity of the information recorded, upon implementation?	Yes	A Security Assessment Questionnaire was completed and approved by IT Security. (See Annex F). EVA is approved for the input and upload of information which is Protected B or lower, users are advised in the ToU not to enter information above Protected B into EVA.	No privacy risk or compliance issue identified.
8. Will the system use specialized software or new databases?	No		No privacy risk or compliance issue identified.
9. Are there guidelines, policies or training materials for employees who handle personal information that go beyond the requirements of the Directive on Personal Information Requests and Correction of Personal Information?	Yes	Users, as employees of ESDC, have onboarding guidelines in the document “Responsible Use of Generative AI”. Users, as employees, also have access to Information Management training through the department. (See Annex F) Generative AI training is part of the mandatory Essential Training Curriculum for ESDC	Please see risks related to absence of mandatory training and inadequacy of training first identified under section 1, question 1.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		employees. This detailed training course must be completed prior to accessing EVA Chat. (See Annex F)	
10. Can the systems track and record who accesses, changes or discloses personal information, along with the date it happened?	Yes	The Microsoft Azure Log does not capture any personal information. PostgreSQL Database plus volume fileshare tracks the user and time of who uploaded a document. No changes can be made to the logs. There is an access record which traces if a log has been accessed.	No privacy risk or compliance issue identified.
a. If yes, are access, changes and disclosures logged and monitored?	Yes	Azure Logs • This log only shows post, get, and requests and whether they were successful or not. PostgreSQL Database plusvolume fileshare: • Chat History • (Approved List of users) will be switched to azure user group. • Authentication information (Email and OAuth Sub, timestamp) • Uploaded Files	No privacy risk or compliance issue identified.
11. Is there a plan for quality assurance and auditing of programs to assess the system's safeguards to make sure they are working properly?	Yes	Cyber security has confirmed that they will monitor alerts from the Sentinel SIEM tool for EVA Chat. This will include analysis of audit records, elimination of false positives, etc. (See Annex F)	No privacy risk or compliance issue identified.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
12. Are there policies and procedures in place to manage the use of portable storage devices such as flash drives that store personal information?	N/A	N/A	N/A
13. Will user accounts, access rights and security authorizations be controlled by a system or record management process?	Yes	This will be controlled by Role-Based Access to the EVA application. The EVA application operates on an Authoritative System of Record management process. (See Annex F)	No privacy risk or compliance issue identified.
14. Will access rights be provided to users only on a need-to-know basis, consistent with the stated purpose for which the personal information was collected?	Yes	Input data, which includes personal information input into EVA by users, should already be accessible to those users under the need-to-know principle consistent with the policies of their respective programs and duties of work, which is out of scope for EVA. Administrators and others from the Automated Infrastructure Team (AIT) will access logs on a need-to-know basis in order to fulfill work tasks related to the functioning and security of the EVA Chat solution. They will access personal information collected by the tool in accordance with use described in the relevant PIB. Personal information entered or uploaded by users into the tool which may be accessed by the AIT through the logs is incidental and will only be used indirectly by the AIT for work tasks related to EVA, such as investigations into misuse.	No privacy risk or compliance issue identified.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
15. Does your institution have a privacy breach response plan in place? (see the Directive on Privacy Practices)	Yes	ESDC has a departmental privacy breach response plan. In addition, a response management plan for EVA has been developed (see Annex F).	No privacy risk or compliance issue identified.
16. Are there contingency plans and documented procedures in place to identify and respond to privacy breaches?	Yes	ESDC's departmental privacy breach response plan includes contingency plans and documented procedures in place to identify and respond to privacy breaches. In addition, EVA has a contingency and technical recovery plan (see Annex F).	No privacy risk or compliance issue identified.
17. Are there documented procedures in place to communicate privacy breaches to: • the affected individual? • law enforcement authorities? • relevant program managers? • affected third parties, including other federal institutions?	Yes	ESDC's departmental privacy breach response plan includes documented procedures to communicate privacy breaches to all relevant parties including affected individuals, law enforcement, program managers and affected third parties.	No privacy risk or compliance issue identified.
18. Are there procedures in place to remove or modify user access rights when job responsibilities change?	Yes	An Admin Panel manages user access rights, including removals and modifications. Any flagged input or uploads are responded to immediately. Violation of the Terms of Use results in suspension of EVA Chat access. The admin can suspend access as well as remove the account. An investigation and follow-up are	No privacy risk or compliance issue identified.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		conducted according to ESDC guidelines mentioned under Section 3 of the Terms of Use: Policies, Guidelines and Restrictions.	
19. Are there security controls in place for remote access and the use of mobile devices?	N/A	N/A	N/A
20. Identify all instances of connectivity with other systems and the technologies used to establish the connection and communications.	N/A	N/A	N/A
21. Are the connections limited to technical functions and no other residual uses, data matching or other activities?	N/A	N/A	N/A
22. If personal information is transmitted through an electronic system, application/software (including collaborative software), is the transmission of data within a closed system where there is no connection to the Internet, or where there is connectivity to other system(s).	Yes	EVA is hosted in ESDC's secure Microsoft Azure cloud environment located in Canada approved by CCCS for Protected B information. The system is configured for internal ESDC use only and is accessible to employees through the department's network or VPN. It uses private connections and restricted settings so it cannot be reached directly from the public internet. The Azure OpenAI service also operates in these secure Canadian datacentres but is shared with other Microsoft customers. This setup meets all Government of Canada security requirements and it is managed	No privacy risk or compliance issue identified.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		through IITB security reviews and continuous monitoring.	

8. Openness

An organization should be open about its personal information policies and practices. Individuals should be able to access an organization's policies and practices relatively easily. Institutions shall make readily available to individuals, specific information about policies and practices relating to the management of personal information in a transparent manner.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
1. Will a summary of the PIA be published online, using the Summary of the Privacy Impact Assessment template?	Yes	A summary of this Privacy Impact Assessment (refer to *Annex G*) will be posted on ESDC's website in accordance with section C.2.2.15 of Appendix C: Standard on Privacy Impact Assessment under the Directive on Privacy Practices.	No risk or compliance issue identified.
2. Do you have a terms of use to notify users of their responsibilities regarding the handling and use personal information?	Yes	EVA Chat enforces user awareness through a mandatory **Terms of Use (ToU)** acceptance process. Upon initial registration and at the start of each session, users are presented with a ToU screen that outlines their responsibilities regarding the use of personal information in the tool. Users must explicitly agree to the ToU daily; otherwise, access to the tool is blocked. The ToU includes the following privacy notice: "Please note that all content posted when using EVA is subject to the Access to Information Act and the Privacy Act. This means that information may be accessed and disclosed in response to a request under either of these Acts."	No privacy risk or compliance issue identified. **PMD reminds IITB to inform them as the ToU or other communication materials are updated.**

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)

		In addition, the ToU and supporting training materials advise users to:
		
		• Use EVA only with data classified **up to Protected B**
		• Avoid uploading or inputting sensitive personal information unless permitted
		• Validate all AI-generated content before use
		• Avoid using EVA Chat for decisions affecting individuals (e.g., eligibility, entitlements)
		
		IITB is taking the following additional measures:
		
		1. **User Risk Awareness:**
		IITB will ensure that all organizations using EVA Chat are informed of known or likely risks associated with the tool, including:
		  ○ Common failure modes (e.g., hallucinated answers, outdated information, unsupported languages or formats)
		  ○ Contexts where generative AI may be inappropriate (e.g., legal analysis, complex casework)
		  ○ Lack of explainability or replicability in some outputs
		
		These limitations will be included in updated ToU language, internal communications, and	

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		the ongoing AI awareness campaign across ESDC. 2. **Dataset Transparency:** EVA Chat relies on **Microsoft Azure OpenAI's GPT-4 model**, which is commercially hosted and maintained by Microsoft. As such, ESDC does not have direct access to the proprietary training datasets used to develop the base model. However: ○ The tool **does not use or retrain on ESDC data** (chat history is not sent back to Microsoft or used to fine-tune models). ○ ESDC will continue to monitor Microsoft's published documentation regarding the sources, filtering, and licensing of datasets used in the model's development. ○ EVA-specific prompts and instructions are configured locally within the ESDC infrastructure, and any curated prompt tuning or system messages are managed internally and do not involve external data sharing.	

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		Documentation regarding EVA-specific configurations, prompt engineering, and safeguards will be made available to stakeholders through IITB-managed technical documentation and onboarding materials.	
3. Does your privacy notice include all of the following elements: • the purpose and legal authority for the collection • any uses or disclosures that are consistent with the original purpose • the relevant PIB description • any legal or administrative consequences for refusing to provide the personal information • the rights of access to, correction of and protection of personal information under the Privacy Act • the right to file a complaint with the Privacy Commissioner of Canada	Yes	Please refer to Annex C for the PNS.	As EVA Chat logs are meant to be transitory, the right of access will remain with the original data collected by the program, unless the request specifically relates to the EVA Chat logs. No privacy risk or compliance issue identified.
4. Has the privacy notice been adapted for verbal	Yes	Please refer to Annex C for the PNS.	No privacy risk or compliance issue identified.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
communication at the time of collection?			
a. If yes, has a text been developed?	Yes	Please refer to Annex C for the PNS.	No privacy risk or compliance issue identified.
5. Is the privacy notice available and consistent across all media and platforms of collection (that is, phone, paper and online)?	N/A	N/A	N/A
6. Is there a clearly defined and easy process for individuals to communicate with the appropriate individuals regarding the handling of their personal information?	Yes	EVA Chat users are clearly informed of their privacy rights and how to raise questions or concerns regarding the handling of personal information. This information is presented through: • The **Terms of Use** and **Privacy Notice Statement** (Annex C), which are presented upon registration and re-confirmed at the beginning of each session; • The **ESDC website**, which outlines how personal information is managed, references the relevant Personal Information Banks (PIBs) published in Info Source, and provides the contact information for the **Access to Information and Privacy (ATIP) Coordinator**. If an individual wishes to inquire further or file a complaint regarding the handling of personal	As per the OPC's *Principles for responsible, trustworthy and privacy-protective generative AI technologies "*All parties should:…Inform individuals what, how, when, and why personal information is collected, used or disclosed throughout any stage of the generative AI system's lifecycle (including development, training and operation) for which the party is responsible." **As AI, and generative AI in particular, is a newer technology which is being integrated into ESDC services and operations, Canadians may have questions about where, how and for what purpose their personal information is being used, handled and stored with AI, including EVA Chat. PMD advises IITB to work with PASRB on reactive lines to respond to potential queries from Canadians with regards to the handling of personal information in EVA Chat.**

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		information in EVA Chat, they are directed to ESDC's ATIP office through the process defined on the official website. Although **EVA Chat is not currently used to make administrative decisions**, ESDC recognizes the importance of **proactive transparency** when using generative AI. In line with guidance from the **Office of the Privacy Commissioner of Canada**, ESDC and IITB commit to clearly communicating: • Whether and how EVA Chat is used in any program area to **assist** in decision-making processes; • That **outputs must not be used** as the sole basis for a decision affecting individuals; • What **safeguards and human review mechanisms** are required before such outputs are used operationally; • What **recourse mechanisms** are available to individuals affected by any such use; • A **plain-language overview** of how EVA Chat functions (i.e., how it generates responses, the limitations of large language models, and the importance of validating output).	

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		IITB, as the provider of the tool, will ensure that these explanations are accessible to program authorities and end users. Guidance, disclaimers, and system documentation will be updated as the use of EVA Chat evolves.	
7. Is there a communications plan to explain to the public how personal information will be handled and protected?	Yes	ESDC readily makes information available to the public about the departmental policies and practices relating to the management of personal information on its website. This information is made available in a form that is easily understood (such as Privacy Notice Statements, PIBs, etc.). The information made available includes: the means of gaining access to and correcting personal information, a description of the type of personal information held, including an account of its collection, use and disclosure; and online links to other webpages that explain the policies and procedures surrounding the use of personal information. Individuals wishing to access information about the handling and protection of personal information by ESDC, along with the policies and practices, may submit an *Access to Information Act* or *Privacy Act* request. The process for making access requests is outlined on ESDC's access to information and privacy webpage.	See question above. IITB is asked to work with PASRB on any communications with public.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		ESDC currently makes information publicly available on its website regarding the handling and protection of personal information, including: • Departmental privacy policies and management practices • Privacy Notice Statements (PNS) linked to online services • A description of Personal Information Banks (PIBs), including collection authorities, intended uses, and data retention practices • The process for submitting Access to Information Act and Privacy Act requests This content is provided in plain language and includes the necessary links for individuals to understand their rights and seek recourse if needed. ESDC acknowledges the importance of being transparent with citizens about how generative AI tools such as EVA Chat may handle personal information—especially when the tool is internally developed or used in operational contexts. In response: 1. **Public-Facing Clarity (in progress):** IITB, working with PMD and program	

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		areas, is developing messaging and public documentation that will allow ESDC to clearly answer questions such as: “Is my personal information being used in ESDC generative AI tools? If so, how is it being used and stored?” This messaging will explain: o EVA Chat’s intended use for employee productivity (not citizen services) o The fact that **chat inputs and uploaded files may contain personal information**, but this data is stored only within ESDC infrastructure and is not shared with Microsoft or third parties o That **outputs generated by the AI model may include inferred or generated personal information**, which is subject to the **same obligations** under the Privacy Act as directly collected information o How chat history is retained, secured, and accessed only under specific operational	

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		conditions (e.g., audit, investigation) 2. **PIB Alignment and TBS Consultation (required):** ESDC recognizes that there is **currently no PIB that explicitly covers the use of personal information in generative AI tools like EVA Chat**. In keeping with the **TBS Guide on the Use of Generative AI**, which states that even generated personal information must be treated as new personal information, ESDC will: o Assess whether an existing PIB (e.g., for internal communication tools or productivity software) can be **substantially modified** to account for EVA Chat o Or, if needed, initiate the creation of a **new PIB** specific to generative AI use within the department o Begin discussions with TBS and the ATIP Office to determine the appropriate PIB strategy 3. **Internal Oversight and Accountability:** IITB, as the developer and provider of	

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		EVA Chat, commits to ensuring that ESDC's privacy communication to the public reflects: ○ What the tool does and doesn't do ○ How it handles and stores personal information ○ What safeguards and access controls are in place ○ That the system is not used for administrative decisions or automated profiling	

9. Individual access

On request, an individual shall be informed of the existence, use and disclosure of their personal information and shall be given access to that information.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
1. Are systems designed to ensure that an individual can have access to their personal information, including all other programs or applications that have received copies of the information?	Yes	The DESDA and the *Privacy Act* protect the privacy of individuals with respect to their personal information held by ESDC. Both Acts also give individuals the right to access their personal information held by institutions, and to request that corrections be made. ESDC's Info Source Chapter provides individuals with an index of personal information holdings under ESDC's control.	Information held in EVA Chat's logs is transitory and kept for 90 days. It is not meant to replace storage of personal information by programs. A request for access would therefore have to specify that it relates to the EVA Chat logs. Any requests for personal information held in EVA Chat's log which are received within the 90-day period will be led by ESDC ATIP following standard procedures. No risk or compliance issue identified.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		At ESDC, Access to Information and Privacy (ATIP) Operations leads the processing of all requests under the Access to Information Act and provides guidance to the Regional Privacy Offices who lead the processing of requests for personal information pursuant to the *Privacy Act* and DESDA. ATIP Operations also responds to some requests for personal information and liaises with the offices of the Information Commissioner and the Privacy Commissioner. Information on how to initiate a privacy request or requests for the correction of personal information is described on ESDC's website in the official language of choice.	
2. Are all custodians aware of an individual's right of access process (that is, through privacy notices and PIBs)?	Yes	All custodians and users are aware of an individual's right of access process. As part of ESDC's Essential Training Curricula, all employees are required to complete a course on Access to Information and Privacy (ATIP) and Stewardship of Information and Workplace Behaviours (SIWB).	No risk or compliance issue identified.
3. Are there documented procedures developed or planned on how to initiate informal and formal personal information requests?	Yes	There are documented procedures on how to initiate privacy requests or requests for the correction of personal information. ESDC's formal Access to Information and Privacy process has been described in response to question #7 under the Openness section.	No risk or compliance issue identified.
4. If appropriate, are individuals provided with access to their	Yes	Individuals can access their personal information in the official language of their	No risk or compliance issue identified.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
personal information in the official language of their choice?		choice. Instructions for obtaining this information are outlined in the publication Information about programs and information holdings, which is available online in both official languages. Additionally, ESDC is bound by the *Official Languages Act*, the Associated Regulations and relevant Treasury Board policies. Where required, its website information is available in both French and English.	
5. If appropriate, will individuals be provided with access to their personal information in alternative formats?	Yes	Individuals will be offered paper or electronic formats to access their personal information. Furthermore, ESDC's website provides a teletypewriter number on its website for people who are Deaf, deafened or hard of hearing, or have a speech impediment and wish to access their personal information held by the Government of Canada. Individuals may also submit their request in person at a Service Canada Centre.	No risk or compliance issue identified.
6. Has consideration been given to providing individuals "routine" or informal access to their personal information?	No	There is no ability in EVA to provide users with routine access to the personal information collected about them during their use of the tool.	No privacy risk or compliance issue identified.

10. Challenging compliance

An individual shall be able to address a challenge concerning the privacy management practices of an institution to a designated individual in the institution.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
1. Is there a process to receive and respond to privacy-related complaints and questions?	Yes	ESDC has established procedures to receive and respond to privacy-related complaints and challenges, including those concerning the institution's privacy management practices. These procedures are overseen by the **Privacy Management Division (PMD)**. PMD is responsible for ensuring ESDC's compliance with the Privacy Act and for responding to complaints or questions related to how the department manages personal information more broadly—including policies, controls, and institutional safeguards. PMD investigates systemic or program-level privacy concerns, coordinates corrective actions, and works with responsible branches (including IITB and the ATIP Office) to amend policies and procedures if needed. As EVA Chat is an internal, departmental tool PMD will be responsible for privacy complaints and inquiries from internal users related to EVA Chat. • **PMD** will assess whether the complaint relates to how personal information is collected, used, disclosed, or retained within the tool. • If a complaint is deemed justified, PMD will work with IITB and other stakeholders to ensure necessary modifications to practices, safeguards, or documentation are implemented.	No risk or compliance issue identified. Since EVA Chat is an internal tool, PMD will be responsible for privacy complaints from internal users of EVA. ATIP will remain the point of contact for Privacy Act complaints from public, which are not expected to be significant in this instance.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		• Any privacy issues related to transitory data, audit logs, or system design will be reviewed with IITB's Automated Infrastructure Team and Privacy Champions. Note: The **Access to Information and Privacy (ATIP) Office** continues to handle external requests under the ***Privacy Act*****, DESDA** and privacy policies (e.g., access or correction of personal records), but is not the primary body responsible for addressing institutional privacy management challenges—that responsibility rests with PMD.	
2. Are the complaint procedures for the proposed program in line with legislative and policy requirements?	Yes	The complaint procedures for the proposed program and service are consistent with legislated requirements.	No risk or compliance issue identified.
3. Are all those who will have access to and handle personal information aware of an individual's right of access and complaint process?	Yes	All custodians and users are aware of an individual's right of access, correction and to file a complaint with the Office of the Privacy Commissioner of Canada (OPC) under the *Privacy Act.* As part of ESDC's Essential Training Curricula, all employees are required to complete a course on Access to Information and Privacy (ATIP) and Stewardship of Information and Workplace Behaviours (SIWB).	No risk or compliance issue identified.
4. Has a procedure been established to log and periodically review the nature,	Yes	ESDC has established a procedure to log and periodically review the nature, frequency, and	No risk or compliance issue identified.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
frequency and resolution of privacy-related complaints?		resolution of complaints. The ATIP Operations Division has procedures in place to manage and review privacy complaints. EVA has a National Service Desk (NSD) ticketing system to raise any issue related to inappropriate use of EVA. An incident management system document is also in place.	
5. Will there be oversight and review mechanisms to ensure compliance with legislative and policy requirements?	Yes	Accountability for compliance with legislative policy requirements for personal information entered into EVA by users falls under the Authoritative System of Record which places responsibility with individual users and their respective programs. Responsibility for compliance with legislative policy requirements regarding personal information collected directly by the tool falls under oversight and review mechanisms implemented by the department and available to ensure accountability. Some examples include PMD's privacy risk follow-up exercises, conducted bi-annually.	No risk or compliance issue identified.
6. Have you documented who is responsible for receiving and resolving privacy complaints?	Yes	ESDC's ATIP Coordinator is responsible for receiving any questions, comments, concerns or complaints regarding the administration of the *Privacy Act*, the DESDA and privacy policies. PMD is responsible for any internal inquiry which concerns the privacy management practices of ESDC, as EVA Chat is an internal	No risk or compliance issue identified.

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
		tool most complaints are expected to be addressed by PMD. See question #1 for additional information about ESDC's process to receive and respond to privacy complaints.	
7. Have oversight agencies, including the OPC, issued reports or opinions on issues that would be relevant to the program?	Yes	The OPC has released a guidance document concerning generative AI entitled *Principles for responsible, trustworthy and privacy-protective generative AI technologies*.	Under the heading of necessity and proportionality, the OPC's *Principles for responsible, trustworthy and privacy-protective generative AI technologies* document states: "Be open and transparent about the collection, use and disclosure of personal information and the potential risks to individuals' privacy. All parties should: Use anonymized, synthetic, or de-identified data rather than personal information where the latter is not required to fulfill the identified appropriate purpose(s)." and "Organizations using generative AI systems should: Consider whether the use of a generative AI system is necessary and proportionate, particularly where it may have a significant impact on individuals or groups. This means that the tool should be more than simply potentially useful. This consideration should be evidence-based and establish that the tool is both necessary and likely to be effective in achieving the specified purpose. Evaluate the validity and reliability of the generative AI tool for the intended purpose. Tools must be accurate throughout the intended

Question	Answer	Justification (if necessary)	Risk or compliance issue (to be completed by privacy officials on receipt)
			lifecycle of the tool and across the variety of circumstances in which they are used. Consider whether there are other more privacy-protective technologies that can be used to achieve the same purpose." Considerations as detailed in the OPC's guidance on the necessity of including personal information, including considerations of 'least intrusiveness', should be taken into account for EVA Chat.

Section C.2 – Data-Matching Table (if applicable)

No data-matching activities are inherent in the EVA tool. Any data-matching activities undertaken with the assistance of the tool are the responsibility of the individual user and their respective programs. The Terms of Use to which users must agree to each time they open the tool outline this responsibility.

Section C.3 – Information Technology Solutions Table (if applicable)

In the table below, identify IT systems that are in-scope.

Name of information technology (IT) solution	Purpose of IT solution	Business owner	Security assessment reports completed
EVA Chat	The ESDC Virtual Assistant (EVA) aims to provide a state-of-the-art generative AI service tailored for Employment and Social Development Canada (ESDC) employees. EVA will adhere strictly to these standards. EVA is designed to augment and support ESDC employees in their work, enhancing productivity without replacing the essential human elements of the work culture and ethics. The virtual assistant will offer a comprehensive suite of language services, including advanced text analysis, language detection, text translation, speech-to-text and text-to-speech conversion, and computer vision capabilities for image analysis and interpretation. Support for both official languages, English and French, is integral to EVA's functionality.	AICoE Director	1. SA&A Approved and granted Full ATO granted by CIO Accessed against 190 Security Evidence Control. 2. Security Assessment Questionnaire SAQ (Signed by CIO) 3. IT Security Impact Questionnaire (Completed)
EVA Chat Components			
Azure Open AI services	EVA leverages Azure OpenAI services within a Protected B environment, ensuring compliance with ESDC, Canadian Centre for Cyber Security (CCCS)		
Secure Cloud Infrastructure	Secure Cloud Enablement Defense (SCED). All traffic will be going through Secure Cloud Enablement Defense (SCED) managed by SSC	AIS Director	SA&A Approved and granted Full ATO granted by CIO

Privacy analysis:

EVA Chat is hosted in a secure environment, inside ESDC. Relevant assessments including an SA&A have been completed and the ATO granted. There are no privacy risks or compliance issues identified with regards to IT solutions.

Section C.4 – Access Inventory Table

Inventory of individuals or groups who have access to and handle personal information (under your institution's control).

Branch or division	Position or titles	Rationale for access	Number of users	Geographical location (of the individuals or groups and the personal information, if in a different location)
AICoE (Artificial Intelligence Center of Enablement) IITB	AICoE Director	The AICoE Director is the owner of the product and responsible for any personal information.	1	Gatineau, QC/ NCR
AICoE (Artificial Intelligence Center of Enablement) IITB	AICoE IT Manager	AICoE IT Manager is the person responsible for the development and metascience of the project	1-2	Gatineau, QC/ NCR
AIS (Automation Infrastructure Services), IITB	AIS IT Manager	AIS IT Manager is responsible for the infrastructure of the EVA chat. IT Manager manages the access to the infrastructure in consultation with AIS senior Technical Advisor	1-2	Gatineau, QC/ NCR
AIS (Automation Infrastructure Services), IITB	(Team Lead/ Senior Technical Advisor and Technical Advisor) Contributor (AIS Team, Admin)	AIS Senior Technical Advisor is responsible for the overall infrastructure for EVA Chat The Contributor group has full access to manage all resources including accessing the personal information but does not allow you to assign roles in Azure RBAC	3-4	Gatineau, QC/ NCR
AIS/AICoE (Automation Infrastructure Services), IITB	Reader (AICoE team, (Team Lead/ Senior Technical Advisor and Technical Advisor))	Can view all resources including log that include personal information, but there is no ability to make any changes.	4-5	Gatineau, QC/ NCR

Privacy analysis:

A risk related to a lack of some defined processes for AIT roles has previously been noted. There are no other privacy risks or compliance issues identified with regards to access or roles.

Section D: Risk Mitigation and Compliance Issue Action Plan

Risk Mitigation Action Plan

Risk number	Risk description	Affected privacy principle(s)	Risk level	PMD Recommendation	Mitigation measures
1	Users of EVA Chat, and the executives and senior officials who hold legal authority for users' respective programs, are ultimately responsible for the input and use of personal information in the tool. Currently, training on EVA Chat is non-mandatory. Without mandatory training which includes a strong emphasis on privacy considerations there is a risk that users of EVA, as well as executives and senior officials who hold legal authority for ESDC programs and activities, may not be aware of their roles and responsibilities while using the tool or the need to seek approval for use of program personal information in the tool, and therefore may misuse personal information in the tool, including use of the tool to make or assist with administrative decisions.	Accountability, Limiting Use, Safeguards	**Medium** **3X4=12**	Training for EVA Chat should be mandatory for all users, with specialized training for senior executives and officials who have legal authority over programs and related personal information. IITB should only allow user access to EVA Chat after successful completion of training on the tool. Users should have to prove their successful completion of the training through providing a digital certificate, email authenticating completion etc. It is not sufficient to rely on the user checking a checkbox which states they have completed training or other non-authenticated action to grant user access to EVA Chat. Executives and senior officials should also be informed if employees in their charge have taken and successfully completed training related to EVA Chat. Employees, as users, should be directed by training to consult with management on their use of program personal information in the tool. The Terms of Use and any related communication to users should be updated to reflect the mandatory nature of the training.	IITB Change Management and Communications team, with related subject matter experts and the College@ESDC will coordinate the update of existing courses within the Essential Training Curricula. This is mandatory for all ESDC employees. This will ensure that appropriate language addressing the identified risk is included in the material. This will ensure all users are aware of their responsibilities, especially those in positions of authority, and that privacy expectations are clearly communicated and consistently reinforced through onboarding, training, and targeted communications. IITB Change Management and Communications will continue to support the responsible usage of AI by highlighting training resources that promote responsible use themes including privacy elements. User responsibilities are clearly outlined in the terms of service presented at login and PMD provided wording will be applied at the next EVA update (Q3). Feedback mechanisms through the MS Teams channel and monthly Q&A sessions encourage open dialogue, allowing users to share insights and concerns. The awareness campaign engaged over 10,000+ unique users and emphasizes

					ethical usage through best practice guides and other helpful resources. OPI: EIIS Liaison and Coordination Timeline: Q4 FY 25/26
2	Current available training on EVA Chat is inadequate to inform employees, as users, and executives and senior officials who hold legal authority for users' respective programs, of their role and responsibilities from a privacy perspective. Training is also given alongside training for Microsoft Copilot, a tool which the department does not allow the entry of Protected B or personal information, which may lead to user confusion. Training for EVA Chat: - Should include a greater component of privacy, to ensure users understand concepts such as 'what is personal information?', 'what is an administrative decision?', and that they are able to distinguish the purpose of use (admin/non-admin), so they can apply these concepts to their use of the tool. - Training should include a section on governance which guides users about the need for structured internal governance processes where employees seek executive-level and/or program-based approval prior to deciding to use protected information in EVA Chat. - Should be presented in a way which clearly separates web-connected tools which apply user input to the algorithm such as Microsoft Copilot and hold personal information outside the department and isolated tools which do not train the algorithm such as EVA Chat. - Should have specialized training or unit of training for executives and senior officials who	Accountability, Limiting collection, Limiting use, Safeguards	Medium 3X4=12	As training is a departmental responsibility, relevant branches and divisions throughout the department, including, but not limited to, IITB, HRSB, PASRB, CDOB, and PMD should collaborate to prepare and implement training for EVA Chat which includes specific training on user roles and responsibilities, including executives and senior officials, in the use of EVA Chat with regard to privacy and the use of personal information. This training should include clear and extensive examples that help the user identify misuse and meet their responsibilities for the use of personal information in EVA Chat.	IITB Change Management and Communications will work with the College@ESDC and related subject matter experts to update the Essential Training Curricula (ETC), which is mandatory for all ESDC employees, to discuss how employees can appropriately use the results of engagements with AI, and EVA in particular. This will emphasize using AI in a responsible and ethical manner, aligned with organizational policies related to Stewardship of Information and Workplace Behaviours. IITB Change Management and Communications with PMD will review and update the Essential Training Curricula, to include guidance on the limitations of uploading personal information into generative AI tools, and the requirement to respect any program specific limitations on the usage of information. such as EVA Chat. These updates will ensure employees understand the technical limitations of the tool and their accountability in managing sensitive information responsibly. AI CoE will continue to provide AI contextual information to support these efforts This fiscal year, PMD and ETC course owners will introduce a new module

	hold legal authority over a program or activity to ensure they understand their obligations and the obligations of employees in their charge when using personal information in EVA Chat.				focused on responsible AI usage, to be released by College@ESDC. OPI: IITB Change Management and Communications Timeline: Q4 FY 2025/2026
3	There is currently limited oversight and auditability of how personal information is being used and handled within the EVA Chat environment. Without general monitoring and logging of user interactions with the tool involving personal information, there is a risk that individuals may inadvertently or deliberately input or use personal information in ways that they are not authorized by their respective program and the senior executives and officials who have legal authority and bear accountability for their program. This lack of visibility makes it difficult to detect potential misuse—such as entering prohibited data, using data in unauthorized ways such as data matching or relying on the tool to assist in administrative decision-making involving personal information—posing compliance, privacy, and reputational risks for the organization. Additionally, as AI technology is rapidly evolving it is imperative to establish regular reporting of changes and updates to EVA Chat with PMD for the life of the tool, so that PMD can evaluate if new or updated privacy assessment is required.	Accountability, Limiting use	Medium 3X4=12	Auditing and/or monitoring, including accompanying review and analysis processes, should be established by IITB which addresses usage of personal information in EVA Chat. This auditing and/or monitoring should examine, in an aggregate sense, trends of usage across the department and by branch, division, or role, as required, and involve more in-depth investigation when aggregate information shows irregularities or potential patterns of misuse. Monitoring could also flag the use (or repeated use) of sensitive data such as SIN or medical information, particularly for branches or roles which do not typically handle such data or only handle it in the context of administrative decision-making. It is recommended that IITB engage with the RAIDE (Responsible Artificial Intelligence and Data Ethics) Team for advice on statistical approaches to establishing their auditing and monitoring processes. It is also recommended that IITB consult with PMD on any potential privacy concerns in the handling of usage data from auditing and/or monitoring processes. IITB is encouraged to share aggregate, anonymized data from the auditing	AI COE will provide branch level statistics on volumes of suspected usage of sensitive information within EVA. PMD will analyze data provided by IITB through this process to identify trends and potential risks to privacy from the department's use of EVA Chat. OPI: AICOE , Timeline: Q4 FY 2025/2026

				and/or monitoring of the use of personal information in EVA Chat with PMD, the RAIDE Team/CDOB, Information Management and other teams or divisions whose work concerns the handling of personal information at ESDC, in order to facilitate the identification of risks to the department which may be present in EVA Chat and its use, and, in particular, to any direct any data which may indicate problematic usage of personal information directly to PMD. IITB should also establish regular reporting to PMD on any changes or updates to EVA Chat, likely on a quarterly or biannual schedule, in order to keep PMD informed of any changes which may require new or further assessment.	
4	Current processes for disposal of information, including personal information, held in EVA's logs are manual and use quarterly Automated Infrastructure Team/AICoE manager meetings as an anchor point for the disposition process. There is a risk that reliance on these manual processes could lead the transitory information held in EVA's logs to be retained longer than necessary.	Retention and disposal	Medium 3X4=12	PMD recommends automating disposition processes for EVA's logs, in order to ensure information stored in the logs is not kept longer than is needed.	To mitigate this risk with manual processes, an automated log deletion process has been implemented with the deployment of EVA Chat version 1.3 in October 2025. OPI: AICOE (IITB) Timeline: Q3 FY 2025/2026

Compliance Issue Action Plan

No Compliance Issues have been identified for EVA Chat.

Section E: Formal approvals

Sign off by the program area	**Sign-off for the section 10 of the *Privacy Act***
The following signature represents a commitment to comply with the *Privacy Act* and privacy policy requirements as they relate to the administration of this program or activity and addressing the risks as part of the mitigation action plan.	As head of the institution or as delegate, I approve this assessment and am satisfied that privacy risks have been identified and will be mitigated according to the action plan as they relate to the administration of this program or activity.
Signature:	Signature:
Date:	Date:
Mathieu Bergeron Director General	Sally Thorpe Corporate Secretary and Chief Privacy Officer
Enterprise Digital Solutions	Privacy Management Division
Innovation and Information Technology Branch	Corporate Secretariat Branch

Note: *If the program or activity involves more than one institution, the signatures of the official responsible for the program or activity and the signature of the section 10 official for each institution must be provided.*

Annex A: Privacy Risk Assessment Grid

The privacy risk assessment grid in this annex is a non-mandatory tool that can be used to determine the impact of a privacy risk identified during the privacy analysis and the likelihood of the risk occurring. Privacy officials are encouraged to adapt the tools to the needs of their institutions. If you use the grid, follow the steps below.

***Step 1:** Determine the potential impact (to the individual or institution) of the risk should it occur, based on the scale below.*

***Step 2:** Scroll down to the "Impact" column and determine the likelihood of the risk occurring (unlikely, likely, very likely, almost certain).*

***Step 3:** The area in the scale where the level of impact and level of likelihood intersect indicates the level of risk.*

> *Example: A potential asset loss for the institution of $2 million (impact level of 2) that is very likely (likelihood level of 2) to occur under standard circumstances will result in a medium risk (2 + 2 = 4).*

***Step 4:** Repeat for every risk identified in Section C: privacy analysis.*

***Note:** Although it is strongly recommended to use as much evidence as you have at your disposal to objectively complete the assessment, for example, potential days of service disruption (based on previous events), it is important to note than some subjectivity in the assessment and result is expected.*

See the Privacy Risk Assessment Grid on the following page.

Privacy Risk Assessment Grid

Impact scale							
		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 for e.g., harm to individuals or service disruptions.)					Legal Services' risk assessment methodology focusses on the strength of a legal position if challenged in court.

			1	2	3	4	5	**Risk rating**	
Likelihood scale	**Almost Certain** Event is expected; should occur under typical circumstances	5	5	10	15	20	25	Severe (20-25)	
	Likely Event can be anticipated; could occur under standard circumstances	4	4	8	12	16	20	High (15-16)	
	Plausible Event is deemed plausible; could occur under limited circumstances	3	3	6	9	12	15	Medium (6-12)	
	Unlikely Event is deemed improbable; could occur under exceptional circumstances	2	2	4	6	8	10	Low (3-5)	
	Rare Event is deemed highly improbable; could occur under unique circumstances	1	1	2	3	4	5	Insignificant (1-2)	

Annex B: Non-Compliance Grid

The non-compliance grid is a non-mandatory tool that can be used to determine compliance issues and the level of non-compliance. Privacy officials are encouraged to adapt the tools to the needs of their institutions. If you choose to use the grid, follow the steps below.

***Step 1:** Determine the type of non-compliance based on the grid below (that is, legal, Government of Canada policy, internal policy, and so on)*

***Step 2:** Repeat for every compliance issue identified in Section C: privacy analysis.*

Non-Compliance Grid

Law or regulation	Government of Canada policy	Internal policy
Non-compliance with Government of Canada Law or regulation (for example, the *Privacy Act*)	Non-compliance with Government of Canada directive, policy instruments or procedural documents (for example, the *Policy on Privacy Protection*, *Directive on Privacy Practices*)	Non-compliance with the institution's internal directive or policy instruments or procedural documents

Annex C: Terms of Use & Privacy Notice Statement (To be updated as risk mitigation activities are finalized)

EVA Chat Terms of Use

Please review and accept the following terms to proceed.

- Ensure the information being used is not above **Protected B** and that as a steward of government information, you respect its use.
- Do not use EVA to replace subject matter expertise.
- Review generated content for accuracy.
- Do not use EVA for administrative decisions impacting citizens' benefits, rights, or personal data.

View Terms of Use

1. **Acceptance of Terms**
   By accessing or using EVA Chat, you agree to comply with and bound by these Terms of Use.

2. **Intellectual Property**
   All content generated is property of the Crown.

3. **Policies, Guidelines and Restrictions**
   Prior to using EVA Chat, employees must review, understand and agree to adhere to the following policies and ethical guidelines:
   - Generative AI in your Daily Work (Generative AI in your daily work - Canada.ca)
   - Treasury Board Guide on the use of generative artificial intelligence (Guide on the use of generative artificial intelligence - Canada.ca)

4. **Privacy Notice Statement**

   This privacy notice explains how we collect, use, and disclose personal information from its users, helping you make informed decisions about sharing sensitive information in EVA.

   1. EVA collects, processes, and stores personal information to support security, compliance, and to ensure responsible use of GenAI tools. In addition to the information collected by ESDC, EVA collects username, the date and time of visits.
   2. Any personal information will be managed in accordance with the Privacy Act and related policies. You have the right to the protection of, access to, and correction of your personal information, which is described in Personal Information Bank Electronic Network Monitoring Logs (PSU 905). Instructions for obtaining this information are outlined in the following government publication entitled Info Source.
   3. Data collected by EVA will be stored electronically in ESDC's secure environment and will not be shared with external sites nor used for AI model training. It will be used solely by internal Employment and Social Development Canada (ESDC) teams for content filtering, auditing, and evaluation purposes.
   4. All users are responsible for the content they upload or create using EVA Chat. EVA does not modify uploaded documents.
   5. Before uploading **Protected B** information, users must ensure they have the authority to do so and that its use is consistent with the original purposes for which the information was collected or created.
   6. Please note that all content posted when using EVA is subject to the Access to Information Act and the Privacy Act. This means that information may be accessed and disclosed in response to a request under either of these Acts.
   7. You have the right to file a complaint with the Privacy Commissioner of Canada regarding the institution's handling of your personal information.

5. **Training**
   Employees have the option to register in Saba for the ESDC Virtual Assistant (EVA) and Microsoft Copilot Chat course.

While this supplemental training is not mandatory for using EVA Chat, it provides valuable insights into the terms of use, including the do's and don'ts of the application.
Additional information and resources are available on the Artificial Intelligence Centre of Enablement (AI CoE) Portal.

Planned Enhancement:
The **College@ESDC** is currently reviewing the structure of the **Essential Training Curricula (ETC)** and will propose **structural changes to the Policy Management Board (PMB)** in **Fall 2025**. The new structure will **differentiate Treasury Board Secretariat (TBS) mandatory training from ESDC's foundational training**, under which courses like **EVA and Copilot**, and **Responsible and Ethical AI** will be categorized. These courses are intended to become part of the **foundational learning path** for all employees using generative AI tools at ESDC.
The EVA and Copilot training course, available in **Saba (ESDC's learning management system)**, will continue to evolve to reflect current classification levels, appropriate use, and policy obligations. Future updates will include **clear differentiation between EVA Chat, EVA Domain Assistant, and Microsoft Copilot**, new **knowledge check questions**, and updated **risk and responsible use modules** aligned with the **TBS Guide on the Use of Generative AI**.
The **Privacy Management Division (PMD)** is actively participating in the review of this revised training approach. Their feedback will inform future iterations to ensure privacy risks and obligations are clearly addressed. The College is also leading the creation of a **Digital Learning Framework** and **EX Steering Committee on Digital Competencies** with partners from **CDOB and IITB** to strengthen the department's overall digital and AI readiness.

- Please note that EVA is currently not supported on mobile devices.

6. **Termination of Access**
   Non-compliance may result in suspension or termination of access.

7. **Modifications to Terms**
   The IITB/AICoE may modify these terms at any time. Continued use implies acceptance.

8. **Contact Information**
   For questions, contact edsc.dgiit.cdeia-aicoe.iitb.esdc@hrsdc-rhdcc.gc.ca

Acknowledgments

(checkboxes)

Please confirm the following before proceeding:

- ☑ I have read and understood the Do's and Don'ts of using generative AI tools responsibly as well as the TBS policy and guide mentioned under Section 3 of the Terms of Use: **Policies, Guidelines and Restrictions**.
- ☑ I understand that EVA Chat collects, uses and stores personal information for security monitoring and compliance. EVA Chat may also generate outputs based on personal information.
- ☑ I agree to the EVA Chat Terms of Use, including all ethical guidelines and restrictions, and that I will respect the Protected B limitations of the information uploaded or provided to EVA.
- ☑ I understand the importance of registering for the ESDC Virtual Assistant (EVA) and Microsoft Copilot Chat.

ACCEPT

Annex D: Personal Information Bank

Electronic Network Monitoring Logs

Description: The records containing the information described in this bank relate to the use by individuals of government institutions electronic networks. Logs containing details of network use by individuals are compiled and are reviewed by appropriate officials of the institution when there is suspected misuse, policy non-compliance, or potential compromise of a government institution's electronic network, as defined by the government institution's policies or the Policy on the Use of Electronic Networks, or other relevant Treasury Board policy instruments or policy directions. Examples of information that may be in the records include network logs that may link an employee's workstation to an Internet Protocol address, listings of sites visited and information on any transactions conducted, including date, time, duration and nature of the visit or transaction. The records may also include information on the use of authorization codes assigned to particular individuals, including successful or unsuccessful use of the codes, date, time and frequency.

Class of Individuals: Employees of the government institution and other individuals using institutional electronic networks, including: student employees; contract staff and agency personnel; members of the public; Ministerial staff; or Members of Parliament that send e-mail to the government institution or specific individuals within the government institution.

Purpose: The information contained in the records may be compiled to support the investigation of suspected or alleged misuse, policy non-compliance, or deliberate or inadvertent impairment or compromise of government electronic networks by persons employed by the institution or by other individuals from outside the institution.

Consistent Uses: The information may be used to substantiate any disciplinary action taken where violation of institutional policies or the Policy on the Use of Electronic Networks is determined, and to support compliance with other relevant Treasury Board policy instruments or policy directions. This information may be shared for disciplinary purposes (refer to PSE 901 Employee Personnel Record and PSE 911 Discipline). If an internal investigation determines that criminal actions may have taken place, the information may be shared with appropriate police authorities. This information may be used to provide reports to management. The information may also be used for research, planning, audit and evaluation purposes.

Retention and Disposal Standards: For information about the length of time that specific types of common administrative records are maintained by a government institution, including the final disposition of those records, please contact the institution's Access to Information and Privacy Coordinator.

RDA Number: 98/001

Related Record Number: PRN 932

Bank Number: PSU 905

Annex E: List of Acronyms

Acronym	Definition
AI	Artificial Intelligence
AICoE	Artificial Intelligence Center of Enablement
CAB	Change Advisory Board
CCOE	Cloud Centre of Excellence
CI/CD	*Continuous Integration and Continuous Deployment*
ConOps	*Concept of Operation*
DevOps	*Development and Operations*
ESDC	*Employment and Social Development Canada*
EVA	ESDC Virtual Assistant
EVA DA	EVA Domain Assistant
GD Mailbox	General Delivery Mailbox
GoC	*Government of Canada*
IaaS	*Infrastructure as a Service*
IT	Information Technology
NSD	*National Service Desk*
OCMC	Operations and Change Management Committee
PaaS	*Platform as a Service*
PBMM	Protected B Medium Medium
POB	Program Operations Branch
SCCM	System Center Configuration Manager
SQL	Structured Query Language
SROC	Supplementary Record of Claim
SSC	*Shared Service Canada*
UTC	Coordinated Universal Time
VM	Virtual Machine

Annex F: List of References

List relevant references used in the preparation of the PIA (Legislation, Agreements, SA&A, operations manuals, program policies or procedures) that involve the handling of personal information.

From EVA Foundational project high level requirements
EVA Foundational Project - LITE HL Bus Req.docx (sharepoint.com)

Saba - EDSC | ESDC: Course and Class Details

EVA - IT Security Role Based Access Control (RBAC) -V1.0.docx

APPROVED - SoSAR for ESDC Virtual Assistant (EVA) Chat Full Deployment.pdf

Saba - EDSC | ESDC: Information Management at a Glance

RE_ AU-6(3) -_ Audit Review_ Analysis_ and Reporting _ Correlate Audit Repositories - Sentinel SIEM - Process description (RACI).msg

AICoE EVA Cloud Solution Audit Strategy v1.docx

AICoE EVA Cloud Incident Management process V1.docx

Audit records Quarterly review and record retention policy review.ics

References for Microsoft standards and practices

Data, privacy, and security for Azure OpenAI Service - Azure AI services | Microsoft Learn

Overview of Responsible AI practices for Azure OpenAI models - Azure AI services | Microsoft Learn

Code of Conduct for Microsoft AI Services | Microsoft Learn

Using your data with Azure OpenAI in Azure AI Foundry Models - Azure OpenAI | Microsoft Learn

Annex G: Azure Content Filtering

See the matrix monitor below for an example of incident tracking. If the system detects any prompt that complies with content filtering configuration, it will block the tool from generating a response to the content, presenting the user with an error message, flag it by type of violation and send a notification via email to the admin. AI Centre of Expertise (AICoE) management will then take necessary action as per ESDC policy and guidelines. This tool will track incidents. Also, an incident can be reported via National Service Desk (NSD) ticket directed to AIcoE GD mailbox.

In the first response, EVA recognizes the prompt and does not provide any response. It blocks the content by generating Error 400. Client Error model error. Please refer to Annex F, Figure 2. Secondly an alert is generated to the admin of EVA infrastructure. Please refer to Annex F., Figure 3 saying Azure Monitor Alert EVA Chat Blocked Calls. The overall progression of EVA chat and blocked and flagged prompts can be seen in Annex F, figure 1.

Please refer to this document related to content filter. We are monitoring all the ones mentioned below.

Azure OpenAI Service content filtering - Azure OpenAI | Microsoft Learn

The content filtering system integrated in the Azure OpenAI Service contains:

- Neural multi-class classification models aimed at detecting and filtering harmful content; the models cover four categories (hate, sexual, violence, and self-harm) across four severity levels (safe, low, medium, and high). Content detected at the 'safe' severity level is labeled in annotations but isn't subject to filtering and isn't configurable.
- Other optional classification models aimed at detecting jailbreak risk and known content for text and code; these models are binary classifiers that flag whether user or model behavior qualifies as a jailbreak attack or match to known text or source code. The use of these models is optional, but use of protected material code model may be required for Customer Copyright Commitment coverage.

Content Filtering

Figure 1

The content will be flagged into the EVA Chat matrix It is monitored and alerted ***(EsPAICoE-OpenAI-Prd is the subscription where EVA chat resiseds)***

Total Calls (Sum), EsPAICoE-OpenAI-Prd

Harmful Volume Detected (Sum), EsPAICoE-OpenAI-Prd

Total Errors (Sum), EsPAICoE-OpenAI-Prd

Sample of blocked content response by EVA

Figure 2

Alert generated based on the blocked prompt:

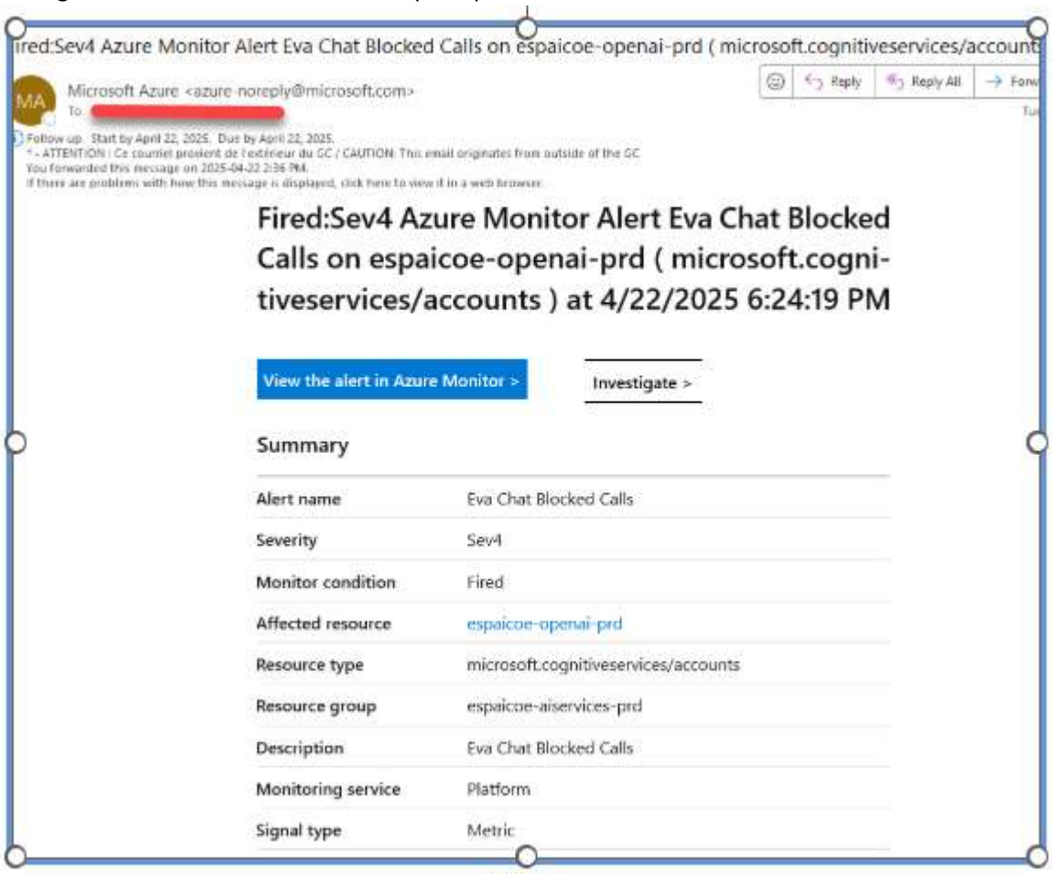


Figure 3

Annex H: Summary of the Privacy Impact Assessment (Web Summary)

Title

Privacy Impact Assessment Report for ESDC Virtual Assistant Chat (EVA)

Description

The ESDC Virtual Assistant (EVA) Chat is a generative AI service for Employment and Social Development Canada (ESDC) employees to help them with their work tasks such as drafting emails and summarizing meetings.

EVA Chat is a tool internal to ESDC and not connected to the internet. It uses a secure environment.

Why a privacy impact assessment was completed

A privacy impact assessment was completed to look at how EVA Chat handles personal information, to see if the information was secure, and to make sure employees were told not to make decisions, especially ones impacting people, using only advice from EVA Chat.

Additional information

The PIA has identified four (4) medium risks related to Accountability, Limiting use, Safeguards and Retention and disposal. A risk mitigation action plan has been developed, and mitigation measures are underway, with completion estimated for Q4 of fiscal year 25/26.

Related personal information banks

Electronic Network Monitoring Logs Bank Number: PSU 905

For more information about this privacy impact assessment

Program: Director General, Innovation, Information, and Technology Branch, Employment and Social Development Canada

Privacy Management Division: Executive Director, Privacy Management Division, Corporate Secretariat, Employment and Social Development Canada