Privacy Impact Assessment

PIA# 25-0013

INSTRUCTIONS/INFORMATION:

Why do I need to do a PIA?
Section 69(5.3) of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) requires the head of a public body to conduct a privacy impact assessment (PIA) in accordance with the directions of the minister responsible for FOIPPA.

Do I have to answer all the questions?
Sections marked as "required" must have an answer. Specify *N/A (not applicable)* if appropriate. Other sections not marked mandatory should STILL be answered if the information is known. You will be contacted to answer any questions that are deemed relevant to this assessment so it's best to be complete.

What if my initiative does not include personal information?
You still need to complete some parts of the PIA to ensure compliance with regulation. Under question "4. Elements of Information or Data", specify "*no personal information collected*". Sections that are marked as "*required*" still need to be answered.

What if I have questions?
If you have any questions about FOIPPA generally, you may contact the "*Privacy and Access Officer*" (privacy@tru.ca). For questions specific to this PIA, contact the "*Information Security Director*" (jcuzzola@tru.ca).

Please note: Depending on the dollar amount or length of the agreement you intend to enter into with a third party, you may need to engage the Procurement Services Department. Please see the TRU Purchasing Policy (BRD 02-2) for more information.

Initiative Preamble (Required)

Initiative/ Project/ Program Name:	**RelativeInsight: AI-powered intelligence platform that supports advanced qualitative analysis**		
Name of TRU Department/Branch:	Integrated Planning and Effectiveness		
PIA Drafter (you):	Dana Prymak		
Your Email:	dprymak@tru.ca	Phone:	**250-318-4070**
Service/Vendor:			
Vendor Email:	rachel@relativeinsight.com	Phone:	**447947630132**

Have you consulted IT Department for this Initiative/Project/Program?

_Yes_____ **No**_____X_____ **N/A**_____

(*If no, it is recommended to consult IT Department first to resolve any potential IT-related issues.*)

Part 1 – General

1. Description of the Initiative (required)

Please provide a general description of the initiative and the context in which it functions. This could include the purpose of the initiative, its benefits, the larger process (if any) that it is part of, how it functions, the parties involved, etc. We will be assessing the impacts of this initiative so please include details which help us understand its size/scale and reach.

Relative Insight is a text analysis platform designed to help organizations extract insights from language data. This tool is intended for use in planning engagements, where anonymized transcription notes from sessions can be uploaded to ensure that key themes captured during discussions are accurately reflected in the final plans. Additionally, open-ended survey responses may also be uploaded for analysis, providing deeper insights into participant feedback.

All responses will be pre-screened for identifiable information (such as names or personal details) to maintain privacy and confidentiality. If any responses are identified, such information will be redacted before the upload. No responses will ever be uploaded with any identifiable information.

This tool has the potential to provide significant time savings by automating the analysis and coding of text data—tasks that are currently performed manually. By streamlining these processes, it enables teams to focus more on strategic planning, deriving insights and supporting the decision-making.

2. Scope of this PIA (required)

This section should explain exactly what part or phase of the initiative the PIA covers and, where necessary for clarity, what it does not cover.

We are currently exploring the possibility of securing a two-year contract. The proposed contract includes upload up to six data sources (surveys and transcripts) per month. The full survey module will be available with the current proposal: access to heatmaps, explore, data discovery and accelerator AI modules.

2-1. Is this initiative recurring in a regular interval, e.g., yearly, or biennially? (required)

We are currently exploring the possibility of securing a two-year contract, with the possibility of renewing or reassessing the subscription based on our license use.

3. Related Privacy Impact Assessments

4. Elements of Information or Data (required)

For this initiative, no personal information will be collected, used, and/or disclosed.

Basic information will be collected when TRU employee signs up, see below. This should consist of business contact information which is not personal information.

From Privacy Policy (Privacy Policy - Relative Insight):

Direct interactions:
You may give us your personal data by filling in forms or by corresponding with us by phone, email or otherwise. This includes personal data you provide when you:

- Purchase our Services or use our Site;
- Create an account on our Site or otherwise;
- Contact us to report a problem with the Site or Services, or for any other purpose;
- Request marketing to be sent to you; or
- Give us feedback or contact us.

Automated technologies or interactions:
As you interact with our website, we will automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies and other similar technologies.

Third parties or publicly available sources:
We may receive personal data about you from various third parties and public sources as set out below:

- Technical Data from analytics providers based outside the EU, such as Google Analytics
- Contact, Financial and Transaction Data from providers of technical, payment and delivery services

How data is used:

- To register you as a new customer,
- To process and deliver your order including:
  - Manage payments, fees and charges
  - Collect and recover money owed to us
- To manage our relationship with you which will include:(a) Notifying you about changes to our terms or privacy policy(b) Asking you to leave a review or take a survey

- To administer and protect our business and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)
- To deliver relevant Site content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you
- To use data analytics to improve our Site, Platform, Services marketing, customer relationships and experiences
- To make suggestions and recommendations to you about goods or services that may be of interest to you

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada (required)

The platform is hosted in AWS EU-WEST1. Relative Insight's platform is hosted with cloud infrastructure providers with SOC 2 Type 2 and ISO 27001 certifications, among others. More information available here.

Certificate Number 11663
ISO 27001

5-1. Is a service provider(s) involved? If so, where is the provider located (e.g. Canada, U.S., or other country)? (required)

Relative Insight is located in the UK.

6. Common or Integrated Program or Activity (required)
If you answer yes, please contact the *Privacy and Access Officer*

If you answer "yes" to all 3 of these questions, your initiative qualifies as "a common or integrated program or activity," and you must comply with requirements under FOIPPA.	
1. This initiative involves a program or activity that provides a service (or services);	yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	no
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	no
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	no

7. Data-linking Initiative* (required)
If you answer yes, please contact *Privacy and Access Officer*

If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under FOIPPA.	
1. Personal information from one database is linked or combined with personal information from another database;	no
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	no
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	no

8. Provide a diagram, flowchart, and/or table that shows how your initiative will collect, use, and/or disclose personal information.

N/A – no personal information will be collected, used, and/or disclosed.

Personal Information Flow Table			
	Description/Purpose	**Type**	**FIPPA Authority**
1.	Anonymized transcription notes from sessions can be uploaded. Open-ended survey responses may also be uploaded for analysis. All responses will be pre-screened for identifiable information (such as names or personal details) to maintain privacy and confidentiality. If any responses are identified, such information will be redacted before the upload. No responses will ever be uploaded with any identifiable information.	*N/A*	N/A

9. Risk Mitigation Table (required)

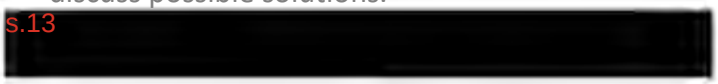
Risk Mitigation Table				
Risk	**Mitigation Strategy**	**Likelihood**	**Impact**	**Exposure**
1	s.13 [redacted]			
2				

3 s.13

4

→ Exposure rating of *high* or *critical* is of concern. Please contact Director, Information Security to discuss possible solutions.

s.13



Risk Exposure Matrix

Risk Exposure Matrix	IMPACT				
	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	Low	Medium	High	Critical	Critical
Likely	Low	Medium	High	Critical	Critical
Possible	Insignificant	Low	Medium	High	High
Unlikely	Insignificant	Low	Low	Medium	Medium
Rare	Insignificant	Insignificant	Insignificant	Low	Low

10. Collection Notice

This notice should advise individuals of the requirement to not include any **personal information**, meaning any information that could identify them – this is not just a name or other identifier, but any personal detail that could connect to them. In determining what information will make someone "identifiable", all information about the person that is publicly available should be considered.

Part 3 – Security of Personal Information

11. Please describe the physical security measures related to the initiative (if applicable).

N/A

12. Please describe the technical security measures related to the initiative (if applicable).

From their website (ISO 27001 & Data Security - Relative Insight):

- Relative Insight Limited is ISO 27001 certified at both its Lancaster and London locations, and is audited annually to ensure its compliance.
- Relative Insight is fully compliant with both GDPR and CCPA data regulations as a Data Processor.
- All of our services are in the cloud, and we only use established providers with the highest security certifications (ISO 27001, SOC, etc.). We do not run our own routers, load balancers, DNS servers, or physical servers when delivering our services to you.
- Relative Insight has a dedicated Security Officer, who oversees certification, compliance and data protection issues. Email address: privacy@relativeinsight.com
  Postal address: Fraser House, White Cross Business Park, Lancaster, UK, LA1 4XQ
  Telephone number: 01524 928190.
- We take pride in our application security, and consider it throughout the development and deployment process.
  - Training and review – Code is reviewed by a senior engineer with security best practice training before being deployed to production systems.
  - Automated testing and build processes – We have an extensive set of automated testing procedures that are run for every code change.
  - Software dependencies – Relative Insight keeps up to date with software dependencies and has automated tools scanning for common security issues
  - Development and QA environments – These environments are separated physically from Relative Insight production environment. No customer data is ever used in development or QA environments.
  - User logins – User passwords are one-way encrypted and salted before being stored in our database.
  - Penetration testing – Relative Insight performs regular penetration test audits with a contracted third party.
- All data transferred in and out of Relative Insight is encrypted using hardened TLS. Relative Insight is also protected by HTTP Strict Transport Security and is pre-loaded in major browsers. Relative Insight uses encryption to protect data in transit and at rest to guard sensitive information against interception. All data transferred in and out of the platform is encrypted using TLS, and HTTP Strict Transport Security.
- Relative Insight will only access your data as part of addressing a support query or if we have been commissioned to provided professional services around it (i.e. an analysis project). In these cases only the relevant and senior staff within Relative Insight will have access to the data.

13. Does your branch/department rely on any security policies? (required)

Yes, Policy No. BRD 16-1: Information Security

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information. (required)
N/A – no personal information will be collected, used, and/or disclosed.

15. Please describe how you track who has access to the personal information. (required)
N/A – no personal information will be collected, used, and/or disclosed.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's personal information updated or corrected? If it is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated.

N/A – no personal information will be collected, used, and/or disclosed.

17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain (required).

No

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate, complete and up-to-date.
For example: check to see that the information was obtained from a reputable source such as another government agency.

N/A – no personal information will be collected, used, and/or disclosed.

19. If you answered "yes" to question 17, do you have a records retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?
If you do not yet have a schedule, please document how these records will be kept until the schedule is in place. Please contact Manager, Information Services.

N/A – no personal information will be collected, used, and/or disclosed.

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

For example: your initiative involves a regular exchange of personal information (both collection and disclosure) with other government(s) and/or other agencies in order to provide services to your clients.

No

Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact Legal Services.	

21. Does the program involve access to personal information for research or statistical purposes? If yes, please explain.

For example: your initiative involves disclosing information to PhD students so that they can conduct research.

No

Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA, please contact *Privacy and Access Officer*.	

22. Will a personal information bank (PIB) result from this initiative? If yes, please list the following information required by section 69 (6) of FIPPA.

A personal information bank means a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol, or other particular assigned to an individual.

Required Information for PIBs:

Name and Description:

Type/Category of Personal Information:

Purpose for Collection:

Authorized Users:

Responsible Authority:

Legal Authority for Collection

No

Part 6 – Canada's Anti-Spam Legislation (CASL) Compliance

23. Please confirm if you plan on emailing, texting, or instant messaging as part of your project. (required)

No. This functionality is not available with the module we are exploring.

24. If you answered yes to question 23, please explain the purpose(s) of the messages you intend to send. Be sure to note any messages involving promotional activities, including links to the TRU public website or other Internet site(s). The purpose(s) you provide will help us identify whether the overall communication is a commercial electronic message (CEM[1])?

N/A

25. If your communication message does fall under CEM rules, you must comply with the unsubscribe mechanism and identification requirements under CASL. Please confirm your method of unsubscribe mechanism that must be processed within 10 business days and how you will meet the identification requirements?

N/A

26. If you do meet the definition of CEM, please confirm that you have a records retention schedule that will ensure that consent communications, both paper and electronic, are stored appropriately and retained for three years after the last communication?

N/A

Part 7 – Common Vulnerabilities and Exposures (CVE) Assessment

(This section to be completed by the **Information Security Office**). If your initiative involves the transmission of personal data between TRU and the vendor, or from the vendor to 3rd parties, then TRU may ask for the name of the software used to determine if there are applicable CVEs.

N/A

[1] If your initiative or program sends commercial electronic messages (CEMs), such as emails promoting a product or service, you must comply with CASL's requirements to: (1) obtain consent, (2) provide identification information, and (3) include an unsubscribe mechanism in each message. Please note that an electronic message that contains a request for express consent is also considered to be a CEM under CASL.

Part 8a – Information Security Director Comments

s.13 [redacted]

John Cuzzola	s.22 [redacted]	2025-05-20
Information Security Director	Signature	Date

Part 8b – Privacy Officer Comments

s.13 [redacted]

Marina Sparks		May 12 2025
Privacy and Access Officer	Signature	Date

Part 9 – Program Area Signatures

Program/Department Manager	Signature	Date
John Cuzzola	s.22 [redacted]	2025-05-20
Information Security Director	Signature	Date
Senior Manager, Program Area/Division	Signature	Date
General Manager	Signature	Date
General Manager	Signature	Date

A Final Copy of this PIA (with all signatures) shall be kept on record by the program area responsible for this project. The signed original record will be retained by the FOI and Privacy Office. ***If you have any questions about FOIPPA generally, you may contact the "Privacy and Access Officer" (privacy@tru.ca). For questions specific to this PIA, contact the "Information Security Director" (jcuzzola@tru.ca).***