

Specimen — illustrative example

Beacon Talent Partners is a fictional organisation. This document comes from the scenario described on riskwoven.com/examples, and is not an assessment of any real entity. It is advisory output to support your own decisions: not legal advice, not a certification, and not an audit.

Written and reviewed by RiskWoven.com. Written by RiskWoven.com's AI drafting agent and checked by RiskWoven.com's independent review stage before release. The review is automated. It is not a human, legal or audit review.

Privacy and Personal Information Policy

Beacon Talent Partners

Document type	policy	Version	1.0 Draft
Owner	Head of Delivery	Customer decision role	Managing Director
Effective date	Upon customer release	Review cycle	Annual
Framework basis	RiskWoven AI practical best practices		
Jurisdiction	Ontario, Canada		
Prepared for	Beacon Talent Partners	Industry	Recruitment and staffing
Organization size	26-100	Locations	Not specified

Advisory draft for accountable-owner and professional review. Validate legal, regulatory, contractual, technical and operational requirements before customer release. This is not legal advice, a certification, or a compliance determination.

1. Purpose

Beacon Talent Partners processes personal information about job candidates, client contacts, and its own employees as a core part of its recruitment and staffing work. This policy states

Beacon's commitment to handling that information lawfully, fairly, and transparently throughout its lifecycle — from collection through to deletion or disposal.

This policy sets the mandate. It tells everyone at Beacon what must be true about how personal information is handled, and who is accountable for making it so. Detailed requirements, step-by-step procedures, and technical controls sit in the supporting instruments listed in Section 12.

2. Scope

This policy applies to:

- all Beacon Talent Partners employees, contractors, and anyone acting on Beacon's behalf;
- all personal information Beacon collects, uses, stores, shares, or disposes of in connection with its recruitment and staffing activities;
- all systems and services used to process that information, including the applicant tracking system and the candidate ranking service.

The three categories of data subject covered by this policy are:

1. Job candidates — individuals who apply to Beacon or whom Beacon sources for client roles.
2. Client contacts — individuals at client organisations with whom Beacon works.
3. Beacon employees — individuals employed by or contracted to Beacon.

Candidate information is the most sensitive category Beacon holds and receives the highest level of protection under this policy.

3. Definitions

Personal information means any information about an identifiable individual. In Beacon's context this includes, but is not limited to, candidate CVs, interview notes, employment history, education records, recruiter assessments, client contact details, and employee records.

Processing means any operation performed on personal information, including collection, recording, storage, use, disclosure, transfer, and deletion.

Consent means a freely given, specific, informed, and unambiguous indication by a data subject that they agree to the processing of their personal information for a stated purpose.

Consent must be capable of being withdrawn.

Data subject means the individual to whom personal information relates — a candidate, client contact, or Beacon employee.

Privacy incident means any event, whether confirmed or suspected, that results in unauthorised access to, disclosure of, loss of, or destruction of personal information, or that prevents Beacon from meeting its obligations to data subjects.

4. Accountability

The **Managing Director** holds ultimate accountability for Beacon's compliance with this policy and for decisions that require executive authority, including the onboarding of critical suppliers who process personal information.

The **Head of Delivery** owns this policy day to day. The Head of Delivery is responsible for:

- maintaining the record of processing activities;
- receiving and coordinating responses to privacy requests and complaints;
- ensuring staff who handle personal information are aware of their obligations;
- escalating material privacy incidents and unresolved complaints to the Managing Director;
- keeping this policy current and presenting it for annual review.

Every Beacon employee who handles personal information is responsible for following this policy and for raising concerns or suspected incidents to the Head of Delivery without delay.

5. Lawful Authority, Purpose, and Transparency

Beacon must identify a lawful basis for processing before it begins. The two bases Beacon relies on are:

1. **Consent** — obtained from candidates at the point of application. Consent must be recorded, must be specific to the stated purpose, and must be capable of withdrawal.
2. **Legitimate recruitment purpose** — relied on for candidates who are sourced rather than self-referred, where direct consent is not obtained at the point of first contact. The Head of Delivery must document the legitimate purpose assessment before sourcing activity begins for a new role type or channel.

Beacon must tell data subjects, at or before the point of collection:

- what personal information is being collected;
- why it is being collected and what it will be used for;
- who it may be shared with, including third-party processors;
- how long it will be kept;
- what rights the data subject has and how to exercise them.

This information must be provided in plain language. The Head of Delivery is responsible for ensuring Beacon's candidate-facing privacy notice is accurate, current, and accessible.

No new category of processing may begin without the Head of Delivery first confirming that a lawful basis exists and that the transparency obligation has been met. The Managing Director must be informed of any material change to Beacon's processing activities.

6. Data Minimisation and Purpose Limitation

Beacon collects and uses only the personal information that is reasonably necessary for the stated recruitment purpose. The categories Beacon currently processes are:

- **Candidate information:** identity details, CVs, employment history, education records, and recruiter notes and interview assessments.
- **Client contact information:** names, job titles, contact details, and role specifications.
- **Employee information:** identity, employment, payroll, and performance records.

Personal information collected for one purpose must not be used for a materially different purpose without a fresh lawful basis and, where required, fresh consent.

Recruiters must not retain local copies of candidate information on laptops or personal devices. All candidate information must be held in the applicant tracking system or, where the ranking service is involved, processed through that service in accordance with the contract terms described in Section 9.

The Head of Delivery must review the categories of information Beacon collects on a cycle set by Beacon and recorded in the review record. Annual review is offered as a starting point; this is an organisational parameter, not a requirement derived from any cited control.

7. Accuracy

Beacon takes reasonable steps to keep personal information accurate and, where necessary, up to date.

Recruiters are responsible for updating candidate records when they receive new information from the candidate or identify an inaccuracy.

Data subjects have the right to request correction of inaccurate information. The process for handling correction requests is set out in Section 10.

8. Information Security and Safeguards

Beacon must protect personal information using safeguards proportionate to the sensitivity of the information and the harm that could result from a breach.

Candidate information is the most sensitive category Beacon holds. It must receive the highest level of protection Beacon applies.

The specific technical and organisational controls that implement this mandate — including access controls, encryption requirements, and system integrity measures — are set out in the **Information Security Policy**, the **Access Control Policy**, the **Data Classification and Handling Standard**, and the **Password and Authentication Standard**. This policy does not duplicate those requirements.

Key safeguard commitments that flow from this policy are:

- Access to candidate personal information is restricted to those who need it to perform their role. Access rights are reviewed by the named system owner on a cycle set by Beacon and recorded in the access register. Quarterly review is offered as a starting point; this is an organisational parameter.
- The applicant tracking system is hosted in Canada. Personal information must not be transferred outside Canada without the Head of Delivery first confirming that adequate protections are in place. The requirements for cross-border transfers are set out in Section 9.
- No candidate personal information may be used to train a third-party AI model. This is a contractual requirement for all processors and is addressed in Section 9.

- Privacy incidents must be reported and managed in accordance with the **Privacy Breach Response Procedure**.

9. Processors, Third Parties, and Cross-Border Transfers

Processor assessment

Beacon uses third-party processors to support its recruitment work. The two critical processors are the applicant tracking system vendor and the candidate ranking model provider. Both are classified as critical because of the volume and sensitivity of candidate data they handle.

No critical processor may be onboarded without:

- Managing Director review and a recorded review decision;
- evidence of bias testing on the ranking model, reviewed before onboarding and on a cycle set by Beacon thereafter;
- a written contract containing the terms set out below.

The **Third-Party Risk Management Policy** governs the broader supplier risk framework. This policy states the specific requirements that apply when a processor handles personal information.

Required contract terms

Every contract with a processor that handles Beacon's personal information must include:

- a prohibition on using candidate data to train the processor's own models;
- an obligation to delete candidate data on Beacon's instruction, propagated to any subprocessor the vendor uses;
- a requirement to notify Beacon of a suspected or confirmed privacy breach within a deadline set by Beacon and recorded in the contract. Beacon has specified 24 hours as its required notification window; this is Beacon's contractual requirement and is not derived from any cited control. Beacon's legal reviewers should confirm this is consistent with applicable Ontario privacy law before the contract is finalised;
- a requirement to obtain Beacon's written agreement before engaging a subprocessor;
- an obligation to provide evidence of fairness testing on request.

The Head of Delivery maintains a register of processors and the contract terms in place for each.

Cross-border transfers

The applicant tracking system is hosted in Canada. The candidate ranking service uses AWS infrastructure. Before any personal information is transferred to or processed in a jurisdiction outside Canada, the Head of Delivery must confirm in writing that adequate protections are in place. The Managing Director must be informed of any new cross-border transfer arrangement. Beacon's legal reviewers must confirm what protections applicable Ontario privacy law requires for such transfers.

10. Data Subject Rights

Beacon recognises the following rights for data subjects whose personal information it holds:

- **Access** — the right to know what personal information Beacon holds about them.
- **Correction** — the right to have inaccurate information corrected.
- **Deletion** — the right to request deletion of their personal information. Candidates may exercise this right at any time.
- **Complaint** — the right to raise a concern about how Beacon has handled their information.

How to submit a request

Data subjects submit requests to the Head of Delivery through Beacon's published privacy contact address.

How Beacon responds

Beacon acknowledges every request within 5 business days of receipt. The Head of Delivery records the request, the acknowledgement date, and the outcome in the privacy request register.

Beacon completes requests within the period required by applicable Ontario privacy law. The Head of Delivery must confirm the applicable deadline with Beacon's legal reviewers and record it in the privacy request register template. This policy does not state a specific number of days because the applicable statutory deadline must be confirmed by legal review rather than assumed.

Where a deletion request is received, the Head of Delivery must instruct the relevant processors — including the applicant tracking vendor and the ranking service provider — to delete the candidate's data in accordance with the contract terms in Section 9.

Where a request is refused, the Head of Delivery must record the reason and inform the data subject of their right to escalate the complaint.

Complaints

Complaints are received and managed by the Head of Delivery. Where a complaint cannot be resolved at that level, it is escalated to the Managing Director. The Head of Delivery records all complaints and their outcomes in the privacy request register.

11. Retention and Disposal

Personal information must not be kept longer than is necessary for the purpose for which it was collected, or longer than applicable Ontario privacy law requires.

Retention periods for each category of personal information are set by Beacon and recorded in the **Records Retention and Disposal Policy**. This policy does not duplicate those periods. Where a conflict arises between this policy and the Records Retention and Disposal Policy, the Head of Delivery must escalate to the Managing Director for resolution.

When personal information reaches the end of its retention period, it must be disposed of securely. The method of disposal must be proportionate to the sensitivity of the information. Candidate information must be disposed of in a way that prevents reconstruction.

Deletion requests from candidates, as described in Section 10, take effect regardless of whether the standard retention period has expired, subject to any overriding legal obligation to retain the information. The Head of Delivery must confirm with Beacon's legal reviewers whether any such obligation applies before refusing a deletion request.

12. Privacy Incidents

A privacy incident is any event — confirmed or suspected — that results in unauthorised access to, disclosure of, loss of, or destruction of personal information, or that prevents Beacon from meeting its obligations to data subjects.

Anyone at Beacon who suspects a privacy incident must report it to the Head of Delivery immediately.

The Head of Delivery is responsible for:

- assessing the incident and determining whether it meets the threshold for notification to affected data subjects or to a regulatory authority under applicable Ontario privacy law;
- engaging the Managing Director where the incident is material;
- following the **Privacy Breach Response Procedure** for all confirmed incidents;
- recording the incident, the assessment, the actions taken, and the outcome in the incident register.

Where a privacy incident involves a processor, the Head of Delivery must invoke the notification and cooperation obligations in the relevant contract.

Beacon's legal reviewers must confirm the notification thresholds and timelines required by applicable Ontario privacy law. This policy does not state specific thresholds or timelines because those are statutory requirements that must be confirmed by legal review.

13. AI and Automated Processing

Beacon uses a candidate ranking service that applies automated processing to candidate personal information. This processing carries specific risks — including the risk of bias — that require additional controls.

The following requirements apply to any automated processing of candidate personal information:

- The ranking service provider must not use candidate data to train its models. This is a contractual requirement.
- Evidence of bias testing must be obtained from the provider before onboarding and on a cycle set by Beacon and recorded in the review record.
- Candidates must be informed that automated processing is used in Beacon's recruitment process, as part of the transparency obligations in Section 5.
- Recruiters must not treat an automated ranking as a final decision without human review. The recruiter responsible for the role retains accountability for placement decisions.

The **AI Risk Management Standard**, the **AI Governance and Accountability Policy**, and the **AI Acceptable Use Policy** set out the broader controls that apply to Beacon's use of AI. This policy states the privacy-specific requirements that apply when AI processes personal information.

14. Training and Awareness

Every Beacon employee who handles personal information must understand their obligations under this policy before they begin handling such information, and must refresh that understanding on a cycle set by Beacon and recorded in the training register. Annual refresher training is offered as a starting point; this is an organisational parameter.

The Head of Delivery is responsible for ensuring training is delivered, recorded, and kept current. Training records must identify who completed training, when, and in what form.

15. Exceptions

Any departure from this policy requires the prior written agreement of the Managing Director. The Head of Delivery records every exception, the reason for it, the conditions attached to it, and its expiry date in the exception register.

Exceptions are time-limited. An exception that has passed its expiry date without renewal is no longer in effect. The Head of Delivery reviews the exception register on a cycle set by Beacon to identify expired exceptions and escalate unresolved ones to the Managing Director. Quarterly review is offered as a starting point; this is an organisational parameter.

The number of exceptions past their expiry date is a metric reported to the Managing Director as part of the annual policy review.

16. Metrics and Monitoring

The Head of Delivery tracks and reports the following metrics to the Managing Director at least annually, and more frequently where a metric indicates a control failure:

- Privacy requests completed within the target response period, expressed as a percentage of all requests received.
- Processing activities with a documented lawful basis and purpose, expressed as a percentage of all processing activities in the register.
- Percentage of required reviews — including processor reviews, bias testing reviews, and access reviews — completed on time.
- Number of exceptions past their expiry date.
- Number of material control failures and overdue corrective actions arising from privacy incidents or audits.

Where a metric falls below a threshold set by Beacon, the Head of Delivery must produce a corrective action plan and present it to the Managing Director within a timeframe set by Beacon. The Head of Delivery must set these thresholds and timeframes and record them in the review record before the first reporting cycle.

17. Review and Maintenance

The Head of Delivery presents this policy to the Managing Director for review annually. The review must be recorded, including the date, the reviewer, and any changes made or deferred.

The policy must also be reviewed promptly following:

- a material privacy incident;
- a significant change to Beacon's processing activities, systems, or supplier arrangements;
- a change in applicable Ontario privacy law that affects Beacon's obligations.

The Managing Director holds review authority for this policy. A reviewed and current version of this policy must be accessible to all Beacon employees.

18. Related Documents

This policy is supported by and must be read alongside the following instruments:

- Privacy Breach Response Procedure
- Records Retention and Disposal Policy
- Information Security Policy
- Access Control Policy
- Data Classification and Handling Standard
- Password and Authentication Standard
- Third-Party Risk Management Policy
- Third-Party AI Review Procedure
- AI Risk Management Standard
- AI Governance and Accountability Policy
- AI Acceptable Use Policy
- Security Incident Response Procedure
- AI Incident Response Procedure

Where this policy and a sibling instrument address the same topic, the Head of Delivery must confirm that the requirements are consistent. This policy does not reproduce the text of any sibling instrument and does not assert what those instruments say.

Owner review items

The drafting process identified the following in the supplied answers. Resolve each before customer release.

Type	Detail	Where
gap	The organisation's jurisdiction is stated as Ontario, Canada, but the specific applicable privacy legislation has not been confirmed. Candidate instruments for legal review include PIPEDA, Ontario's private-sector privacy legislation, and any sector-specific regulation that applies to recruitment and staffing. Beacon's legal reviewers must confirm which instruments apply, what notification thresholds and timelines they impose, and what retention obligations they create. This policy deliberately avoids stating statutory deadlines or thresholds that have not been confirmed.	Sections 10, 11, 12
gap	The 24-hour breach notification window in Section 9 is Beacon's stated contractual requirement, drawn from the customer answers. It is not derived from any cited control or confirmed statutory obligation. Beacon's legal reviewers should confirm whether applicable Ontario privacy law imposes a different or additional notification obligation on Beacon itself, separate from the contractual obligation it places on processors.	Section 9
gap	The AWS infrastructure used by the ranking service may involve processing in jurisdictions outside Canada. The customer answers do not confirm the AWS region or regions in use. The Head of Delivery must confirm where the ranking service processes data and whether a cross-border transfer assessment is required before this policy takes effect.	Section 9
gap	The customer answers state that candidates may request deletion at any time, but do not address whether any legal obligation to retain candidate information overrides that right (for example, for tax, employment, or anti-discrimination purposes). Beacon's legal reviewers must confirm the circumstances, if any, in which Beacon may lawfully decline a deletion request.	Sections 10, 11
gap	The existing Records Retention and Disposal Policy is listed as a sibling document. This policy defers retention periods to that instrument. Beacon must confirm that the Records Retention and Disposal Policy contains specific, confirmed retention periods for each category of personal information covered here — candidate, client contact, and employee — and that those periods are consistent with applicable Ontario privacy law. This policy cannot assert what the sibling says.	Section 11
vague	The customer answers do not specify the published privacy contact address through which data subjects submit requests. The policy refers to a published address; Beacon must confirm this address exists, is current, and is accessible to candidates before this policy is issued.	Section 10
gap	The customer answers do not address whether client contacts are informed of Beacon's processing of their information, or what lawful basis Beacon relies on for that processing. The transparency and lawful basis obligations in Section 5 apply to client contacts as well as candidates. Beacon must confirm its position.	Section 5
gap	The customer answers do not address whether candidates are currently informed that automated ranking is used in Beacon's recruitment process. Section 13 requires this disclosure. Beacon must confirm whether its existing candidate-facing privacy notice covers this and update it if not.	Section 13

Information the organization must supply

These values were not available from the intake and are required before this document can operate:

- Confirmation from legal reviewers of which Ontario privacy legislation applies to Beacon Talent Partners, including any sector-specific regulation for recruitment and staffing.
- The statutory response deadline for privacy requests under applicable Ontario privacy law, so that the Head of Delivery can record it in the privacy request register template.
- The statutory notification thresholds and timelines for privacy incidents under applicable Ontario privacy law, so that Section 12 can be operationalised.
- Confirmation of the AWS region or regions used by the ranking service provider, and a cross-border transfer assessment if processing occurs outside Canada.
- Legal confirmation of the circumstances, if any, in which Beacon may lawfully decline a candidate deletion request.
- Confirmation that the Records Retention and Disposal Policy contains specific, confirmed retention periods for candidate, client contact, and employee personal information consistent with applicable Ontario privacy law.
- The published privacy contact address for data subject requests, confirmed as current and accessible to candidates.
- Confirmation of Beacon's lawful basis for processing client contact information and whether client contacts are currently informed of that processing.
- Confirmation of whether Beacon's existing candidate-facing privacy notice discloses the use of automated ranking, and an update to that notice if it does not.
- Organisational decisions on the following parameters, which this policy identifies as Beacon's to set: (a) the cycle for reviewing categories of information collected; (b) the cycle for reviewing access rights to candidate information; (c) the cycle for refresher privacy training; (d) the cycle for reviewing the exception register; (e) the metric thresholds and corrective action timeframes for Sec
- Legal review of the 24-hour processor breach notification requirement in Section 9 to confirm it is consistent with Beacon's own statutory obligations under applicable Ontario privacy law.

Written and reviewed by RiskWoven.com. Written by RiskWoven.com's AI drafting agent and checked by RiskWoven.com's independent review stage before release. The review is automated. It is not a human, legal or audit review.