University of Lethbridge

QUESTIONNAIRE FOR PRIVACY SCAN

General

1. Is there a new collection of personal information? Yes ☐ No ☐
   If yes, why?

   If no, what is the source of the information (e.g. registration/enrollment information)?

2. Is there disclosure of personal information? Yes ☐ No ☐

   If yes, list the personal information to be disclosed:

   If yes, why is the personal information being disclosed?

Accountability (Contract Clauses)

3. Does the contract address all aspects of privacy compliance?

   Collection: No
   Use: No
   Disclosure: No
   Access: No

4. Who controls the information?

   How is it used?

   How is it accessed?

   How long will it be retained?

5. Is the contractor subcontracting services? Yes ☐ No ☐

Access or transfer of information to another

6. Has the contractor claimed limited liability in the event of a breach?

7. Are there termination procedures that will allow recovery (return) of personal information?

8. Are there termination procedures that require the contractor to securely delete personal information with in reasonable and specified time frames?

Security

9. Where will the date be stored? Local (Alberta), within Canada, or outside of Canada?

For cloud based storage, will data be segregated or stored with data from other organizations?

10. Will the information be encrypted at rest and in transit? Yes ☐ No ☐

If yes:

At Rest – Who owns the encryption keys? Is additional protection needed?

In Transit – Does the data transfer occur over an encrypted (https) connection?

If no, why not?

11. What are the procedures for authentication? (password, token, complexity requirements) Are passwords adequately protected from disclosure and plain text recovery?

Are these adequate relative to the sensitivity of the information?

12. Are there policies and procedures that restrict access to data? Will the contractor provide evidence of these policies/procedures?

    Internal access to data (University of Lethbridge)

    Contractor access to data

13. What are the notification procedures if there is a security breach?

14. Can evidence of effective controls for both internal business practices as well as certification of the data centers being identified?
    i.e. ISO 27000, PCI-DSS compliances, SOX, Sarbanes-Oxley?
    Copies of Policies/Standards
    Any evidence of third party audit's for compliances?

15. What is the disaster recovery/business continuity plan?

    Internal recovery plan (University of Lethbridge)

    Contractor Recovery Plan

16. Is there an exit strategy, meaning if we terminate our agreement with this organization how do we get our data back, and how do we ensure they don't retain copies?

Secondary Uses

17. What will the contractor do with the information that is shared/disclosed to it?

18. Will the contractor analyze the data for its own purposes?

19. Can the contractor sell the information?

20. Will the contractor use or allow access to the information for target advertising?

21. Will any of these secondary uses result in the University's non-compliance with applicable privacy laws?

Knowledge, Consent and Transparency

22. Are the students/Alumni aware that the University will share their information with a third party?

Where applicable, has the University met the notice requirements?

23. Will the contractor process the information for the same purpose for which is was collected? Is there consent from students [Refer to Q#21]

24. Will the data be portable? Will you be able to transfer the personal information back in-house or to another contractor?

25. Does the contractor have a designated privacy person that is accessible?

26. Does the University have the ability to:
Access data at any time? Yes ☐ No ☐
Make corrections? Yes ☐ No ☐
Investigate any allegations of non-compliance with privacy obligations? Yes ☐ No ☐

27. If there are subcontractors involved, will the University lose control of personal information to the subcontractors?

Jurisdiction and Access

28. Where will data be stored [Refer to Q#9]

29. What are the risks in outsourcing to that jurisdiction (if outside of Alberta)?

30. Could foreign entities potentially have access to the data?

31. What are the contractor's policies with respect to access to information requests?

32. Will a warrant or subpoena be required prior to granting access to foreign courts, governments agencies, and law enforcement?

33. Will the contractor inform the University if data is requested prior to granting access to foreign courts, government agencies and law enforcement?

34. Will the contractor inform the University if data is requested or disclosed pursuant to a legal requirement?

35. Will the contractor seek direction from the University prior to sharing information with others, including law enforcement?