Horizons Global Consulting

— your privacy and security management partner —

A Short Privacy Self Assessment Questionnaire

	Question	YES	NO
1.	Have you delegated responsibility for privacy and compliance with the privacy legislation to a specific individual (privacy officer) or group (privacy team)?		
2.	Have you developed and implemented specific privacy policies and procedures to protect personal information?		
3.	Do you identify and document the legitimate business purposes for collecting personal information either at or before the time the information is collected?		
4.	Do you define what personal information is needed to fulfill the purposes identified, taking into account both primary and secondary purposes (e.g. order processing, audit, marketing, etc.)		
5.	Do you require express (rather than implied) consent whenever possible, and in all cases where the information is sensitive or the individual would reasonably expect it?		
6.	Is the consent statement clearly worded, so that an individual can reasonably understand: • the personally identifiable information to be collected and its source? • the purpose for which the information will be used? • the date of the consent and means of authorization? • the organization to which the consent is given? • any future uses of the information? • other organizations to whom the information may be disclosed?		
7.	If you collect personal information from a third party, do you ensure the third party has gained consent from the customer for the disclosure? E.g. sharing of mailing lists between non-profit organizations, purchase of mailing lists.		
8.	Do you have procedures to ensure that, where personal information is to be used for any purpose other than the purpose for which it was collected or compiled, the use is consistent with the original purpose and consented to by the individual?		
9.	Do you have procedures to ensure that you do not disclose information except with the consent of the individual or as required by law?		
10.	If personal information is collected, used or disclosed to third parties in carrying out programs or services or managed by them on your behalf, are provisions in place to ensure that the third party meets the privacy protection requirements of the legislation?		
11.	Do you dispose of or destroy personal information in a way that prevents unauthorized parties from gaining access to it?		

	Question	YES	NO
12.	Do you conduct periodic assessments to check the accuracy of personal information records and to correct them, as necessary, to minimize the use of inappropriate data for decision making?		
13.	Do you have security safeguards (physical, organizational and technological) to protect personal information in your control against loss or theft, and unauthorized access, disclosure, copying, use, or modification?		
14.	Are security measures appropriate to: the sensitivity of the information; the amount of information; the extent of distribution; the format of the information (for example, electronic or paper); and the method of storage?		
15.	Do you transmit personal information over secure channels and/or encrypt any transmissions over open channels?		
16.	Do you regularly conduct third party monitoring and audit of security systems?		
17.	Do you prepare privacy documents (such as application forms, questionnaires, survey forms, pamphlets and brochures) that clearly explain personal information policies and procedures to clients and customers?		
18.	Do you have procedures and systems in place to: • verify the identity of individuals requesting access to their information? • facilitate a response to requests for personal information including those in alternate formats, such as Braille or audio tapes? • correct personal information if the individual requests, or annotate the information if a correction is not made? • enable third parties that have received personal information for which a correction is requested to be notified?		
19.	Do you have procedures to receive and respond to complaints or inquiries about your handling of personal information?		
20.	Have you trained your staff on your privacy policies and procedures for managing personal information including: • who is responsible for dealing with privacy questions? • why you are collecting, using and disclosing personal information? • when and how consent may be withdrawn and the consequences, if any? • the steps and procedures for requesting personal information and filing complaints?		

Scoring – 5 points for each Yes answer, 0 points for each No or Don't Know answer.