

Internal Audit Questions

In order to develop your privacy policy, you will need to communicate with all of your organization's divisions to determine what nonpublic personal information is being collected, for what purpose, and with whom it is being shared. These questions are intended to guide you in reviewing your information handling practices and in developing a privacy policy that is consistent with your obligations under the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act.

General Business Questions

1. Which employees have access to nonpublic personal information?
2. Do these employees understand the privacy issues outlined in the attached memoranda?
3. Are procedures in place to educate employees on any privacy issues that they do not understand?
4. Is privacy a subject covered in employee training?
5. Are procedures in place to deal with privacy issues, events and concerns as they develop?

General Information Handling Questions

6. What categories or kinds of information do you collect?
7. What are the mechanisms you use for collecting this data?
8. What person or entity collects it?
9. For what purpose(s) is it collected?
10. Is data that is collected for one purpose is ever used for another purpose?

Questions Relating to Information Security and Integrity

11. What mechanisms do you use to protect the safety, confidentiality and integrity of the information you collect?

12. What mechanisms do you use to prevent unauthorized access or use of the information?
13. Do you have a list of every employee or type of employee who will have access to personal data?
14. Which of these employees actually need access to such information in order to carry out their assignments?
15. Do your employees that have access to such information understand the importance of reporting security glitches or other problems relating to preserving the confidentiality and integrity of the information you collect?

Disclosure of Information to Third Parties¹

16. Do you disclose nonpublic personal information to affiliates or nonaffiliated entities? If so, you must answer the following questions (questions 17-22).
17. What are the categories or kinds of information that you disclose to third parties?
18. What are the categories of persons or entities to whom you disclose nonpublic information (including both affiliates and nonaffiliated third parties)?
19. What are the purposes for which the data is disclosed?
20. Is the information collected about former customers treated the same way?
21. If not, how is its treatment different?
22. Who are your employees that deal with third parties? (You should inform all of your employees who deal with third parties of the importance of reporting any suspected misuses of shared information as soon as possible).

¹ You will use the information gathered here to assist you in selecting appropriate clauses to satisfy paragraph 2 of the sample privacy form in Appendix 1. For example, the clauses from which you may choose to satisfy paragraph 2 (See Appendix 2) ask you to list the kinds of information you may disclose to third parties (See Clause 2(b) in Appendix 2). Your answers here will assist you in listing such categories of information.

Information Disclosure to Non-Affiliated Third Parties²

23. Do you disclose nonpublic personal information to nonaffiliated third parties? If so, you must answer the following questions (questions 24-30)
24. Is the third party's use of the information limited solely to providing services on your behalf?
25. If so, what kind of services?
26. Does the third party's usage fit within a category specifically exempted by the GLBA?
27. If so, what category or categories (see attached cover memorandum for a list of specific exemptions, such as servicing and processing transactions)?
28. Do you share information with nonaffiliated parties for purposes of jointly marketing financial products, or with service providers (such as envelope stuffers) to market your own products?
29. Do you have contracts in place with the persons or entities to whom you disclose nonpublic information for marketing purposes?
30. Are there specific limitations in those contracts on how the information can be used?

Questions Relating to the GLBA Opt-Out Right³

31. Do you share GLBA information with unaffiliated third parties for purposes other than those specifically permitted by the GLBA? If so, you will need to provide an opt-out notification, and you should answer the following questions (questions 32-33).
32. Do you have mechanisms in place that will allow data to be separated if the opt out right is exercised?
33. Do you have mechanisms in place that will allow to you confirm whether the opt-out right has been exercised?

² You will use the information gathered here to assist you in selecting clauses to satisfy both paragraphs 2 and 3 of the sample privacy form in Appendix 1. For example, you must determine whether the disclosures you are making are covered by a GLBA exception in order to select a number of the clauses listed for paragraphs 2 and 3 (such as the clauses numbered 2(e) or 3A(2) in Appendix 2).

³ Your answers here will assist you in determining whether you have to make the GLBA opt-out disclosure in paragraph 3B of the sample privacy form in Appendix 1.

Questions Relating to the FCRA Opt-Out Right⁴

34. Do you have affiliates with whom you share nontransactional information? If so, you must answer the following questions (questions 35-39).
35. What type of nontransactional information do you share with your affiliates?
36. For what purposes is it shared?
37. Does the information you share with your affiliates bear upon consumer credit worthiness, credit standing, credit capacity, character, general reputation or mode of living?
38. Is the information that you share used to as a factor in establishing a consumer's eligibility for credit, insurance or employment purposes?
39. If your answers to questions 37 and 38 are yes, you are required to provide your consumers with an opportunity to opt-out of your sharing such information with affiliates.

Handling Complaints and Inquiries

40. How are your policies regarding the collection, use and distribution of information explained to your customers?
41. Who is in charge of handling consumer complaints and inquiries?
42. How are consumer complaints and inquiries handled?
43. Are complaints and inquiries logged?
44. Is there a commitment to correcting errors?
45. Are there mechanisms in place to resolve consumer disputes if they arise?

Transfer of Personal Data from Members of the European Union

46. Do you transfer personal data from European Union member states?
47. If so, then you should refer to the memorandum attached as Appendix 9 and comply with the requirements listed therein.

⁴ Your answers here will assist you in determining whether you have to make the FCRA disclosures in paragraph 4 of the sample privacy form in Appendix 1.

Reviewing Vendor Contracts

48. Do you transfer nonpublic personal information to third parties pursuant to service provider or vendor contracts or pursuant to joint marketing agreements?
49. If so, you should obtain copies of all contracts or agreements and review them for compliance with the GLBA service provider/joint marketing exception. (To ensure compliance with the exception, you will need to make sure that the contracts have certain language prohibiting the third party from reusing or redisclosing such information other than as permitted by law. You should refer to the memorandum attached as Appendix 4 for more information about the service provider/joint marketing exception and sample contract language).