

**(English Version)**

**October 29, 2004**

**SUBMISSION OF THE PRIVACY TASK FORCE AND THE FINANCIAL SERVICES COMMITTEE OF THE AMERICAN CHAMBER OF COMMERCE IN JAPAN (THE "ACCJ") IN RESPONSE TO THE REQUEST FOR PUBLIC COMMENTS BY THE FINANCIAL SERVICES AGENCY ON ITS DRAFT GUIDELINES ON THE PROTECTION OF PERSONAL INFORMATION IN THE FINANCIAL SECTOR**

The ACCJ appreciates the opportunity to comment on the draft guidelines targeting the financial sector with regard to the Law Concerning the Protection of Personal Information (the "Guidelines"). We would like to take this opportunity to commend the Financial Services Agency (the "FSA") on its promotion of transparency in the process of drafting the Guidelines. The ACCJ believes that the Basic Law is a necessary and sound measure to protect legitimate individual privacy expectations, while also taking into account the need for companies handling personal data to have flexibility in structuring their operations in line with commercial realities. The Guidelines to be promulgated by each ministry will be essential to interpreting the general provisions of the Basic Law, and should follow the proper balance struck in the Basic Law encompassing both the principle of personal information protection as well as the value of the proper and efficient use of information. With those thoughts in mind, the ACCJ would like to offer the following comments on the draft Guidelines.

Inter-Agency Coordination

Under the scheme of the Basic Law, different ministries are responsible for sector-specific guidelines. Therefore, strong inter-ministry coordination during the development of these guidelines is essential to avoid conflicting regulations and guidelines. In particular, it will be important that the guidelines developed by all of the ministries be consistent with each other. For example, as currently drafted, both the FSA Guidelines and the MHLW Guidelines are applicable to employees of organizations over which the FSA has jurisdiction. The definitions and terms used, and the obligations imposed, by all of the ministries in their respective guidelines should be consistent throughout all of the guidelines. It will also be important to have strong inter-ministry coordination in the enforcement process. In cases where there is joint jurisdiction, ministries should develop consolidated views and issue joint rulings or findings. Businesses should not be left responsible

for working out differences between the ministries. To the extent possible, those rulings or findings should be published and made public so that Businesses can understand the ministries' interpretation and can rely on such interpretations in structuring their business processes going forward. The FSA should work with other ministries to actively use a coordinated "no action letter" procedure, through which a Business can consult with the ministries, and then rely on the ministries' decision to take no administrative action against such business. Such a procedure is essential to promoting a transparent and predictable system for enforcing the Basic Law and its relevant guidelines.

### Substantive Provisions of the Draft Guidelines

#### **Definition of Personal Information (Article 2)**

For the reasons set forth below, we request that the FSA exclude (a) business and professional information, (b) publicly available information and (c) anonymous and encrypted data from the definition of "personal information" under Article 2 of the Guidelines.

##### **(a) Business and Professional Information**

We recommend that the FSA exclude from its definition of personal information "information that identifies an individual in a business, professional or official capacity, including the carrying on of a business; or describes the professional or official responsibilities of the individual and the activities and related transactions and is used for intended business purposes," such as the information contained on a business card. Alternatively, the FSA could extend to such information the exemptions that apply to the handling of telephone books and navigation systems (Article II.1(4) of the METI Guidelines; Article 2(4) of the Basic Law). In the case of the latter, they are not considered to be personal data, and, therefore, the obligations imposed on Business are not applicable.

When business contact information is being exchanged between business professionals for intended business purposes it is generally impractical or unnecessary to obtain consent, because individuals expect that their information will be used in this way. Moreover, imposing notice and consent obligations on the collection, use and transfer of business contact or professional information for intended business purposes can be extremely time-consuming, expensive, and burdensome without providing corresponding privacy protection. It would not be an exaggeration to say that this requirement would conflict with the very nature of Japanese sales methods and business introductions. For example, foreign financial services

companies typically use global customer relationship management (CRM) databases, which require the sharing of information about customer relations, sales prospects, etc., with affiliates inside and outside of Japan, and such companies frequently receive business information from persons representing other organizations, such as pension funds or institutional investors. Such information should be excluded from coverage under the Guidelines.

While the Guidelines do exempt business and professional information in certain circumstances, the exemption is too narrow and would not permit, for example, sending information or marketing materials to those individuals. If it is not possible to completely exempt the information contained on business cards, it should be possible to remove certain information to exempt it from the definition of personal information; for example, the name (but not the title) of the holder.

### **(b) Publicly Available Information**

Information that is publicly available should be excluded from the definition of personal information. Publicly available information means personal information about an individual that the individual knowingly makes or permits to be made available to the public, or is legally obtained and accessed from government records that are available to the public, journalistic reports, or information required by law to be made available to the public. Once information has become public, there should be no limitations on the truthful use of such information.

### **(c) Anonymous or Encrypted Data**

Data that has been anonymized or encrypted should be excluded from the definition of personal data. Information that has had all personally identifiable information removed or made inaccessible is essential for research and other statistical purposes. Thus, information that has been anonymized or encrypted (and the recipient does not have the de-encryption key), should be excluded from the definition of personal information because it no longer contains any information that can be used to identify an individual.

## **Notice (Articles 3 and 13)**

The purpose of use specification requirement (Article 3) and the restrictions on providing information to third parties (Article 13) in the Guidelines appear to place unnecessary and overly burdensome notice obligations on Businesses. As drafted, each purpose and all third parties, joint partners, and members of credit bureaus must be identified individually

(as opposed to providing a description of the categories or types of purposes and/or third parties).<sup>1</sup> This is problematic because:

1. In the event that the financial institution opts to work with a different entity or share data with a different third party even if it is for a previously identified purpose and the entity is similar to (or belongs to the same category as) the previous entity, a new notice (and consent) would be required.
2. This requirement imposes a standard on Businesses that is higher than that used in the OECD Guidelines and the EU Directive, and is inconsistent with business realities.
3. It contradicts the standards and practices developed in the financial services industry during the past several years, often at considerable costs to companies, that have served the goal of protecting personal information very well
4. As drafted, such a requirement would result in overly detailed and lengthy notices, making them less accessible and less likely to be read by individuals, and would result in a proliferation of notices that would impose an unnecessary and unreasonable burden on Businesses and their employees.

When an organization provides information to a third party or engages in a joint use of the information, the organization must have the flexibility to change service providers without having to provide a new notice to consumers. As an example, if a third party service provider were to cease business for whatever reason and, therefore, an alternative service provider were to be contracted to provide the same service, there should not be a notice requirement. A financial services organization should be required to disclose that it provides information to a third party for the purpose of providing back office services, but it should not be required to disclose the specific name of the third party that it chooses to use to provide those back office services.

We urge the FSA to clarify that the descriptions of the types or categories of uses, such as those cited as examples in Article 3.1, are sufficient and that Businesses do not need to provide a detailed, itemized list of individual uses (rather than the categories of uses). Such a requirement would necessitate detailed customization of applications and terms and conditions, and would be extremely burdensome. We also suggest that the FSA clarify that such descriptions of purposes of use may be provided

---

<sup>1</sup> Both the names of the member companies that will be accessing credit information from the credit bureau must be listed somewhere, as well as the membership criteria, and must be kept up-to-date. A more workable approach might be to encourage credit bureaus to establish a central home page that keeps an up-to-date list of member companies and membership criteria, to which Businesses Handling Personal Information could refer.

through the application form that the customer signs when applying for credit or another financial product or service and that separate notices are not required.

With respect to the timing of notices in general, we agree that, whenever possible, notice should be provided in advance; however, there are situations where it will not be technically possible or practical to provide notice in advance or at the time of collection. Therefore, the Guidelines should clearly recognize that after-the-fact notice is acceptable in appropriate situations. In the case of cookies, for example, it is not technically possible to give notice until after the cookie is activated because otherwise you will not know to whom to give notice. Similarly, if a consumer uses an ATM, he or she must insert a card, which entails the collection of information by the financial institution, in order to commence the transaction, or to determine in what language the notice should be given. Thus, the financial institution can not provide notice regarding the manner in which information will be used until after some information is collected.

We also suggest that Article 8.2 be revised to clarify that the purpose of use does not need to be disclosed in advance of acquiring personal information in a contract, application or other document, but rather at the time of acquiring such information.

### **Consent (Articles 3, 4, 5 and 13)**

The Basic Law provides that, in most situations, opt-out consent is appropriate.<sup>2</sup> The Guidelines appear to be inconsistent with the Basic Law in requiring opt-in consent in many instances where the Basic Law envisions opt-out consent as acceptable. In particular:

- Article 4 seems to indicate that whenever consent is required, it must be written opt-in consent (including a “confirmation touch” in the case of a touch-screen panel). This will be an extremely onerous obligation for financial institutions, raising costs for consumers without providing meaningful additional privacy protections. Article 4 should be amended to include examples of opt-out consent, for example, by providing bold disclosure that information may be used for additional purposes or shared with third parties, but that the principal may opt-

---

<sup>2</sup> For example, Article 18(3) of the Basic Law provides that, if the purpose of use of previously collected information changes, an organization need only provide notice to the individual or make a public announcement of the new use. That is the equivalent of opt-out consent, and no affirmative action by the individual is required. Similarly, Article 23 provides that as a general matter Personal Information should not be provided to third parties without consent of the principal. Article 23(2), however, provides that if the individual has been given notice, the personal information may be disclosed to a third party so long as the individual has the right to request that it not be provided (i.e., opt-out).

out of such sharing or change of use by so notifying the company. For the avoidance of doubt, it should also be clarified that even an opt-out method of consent is not required for use of information for a purpose already set forth in an initial contract.

- Article 5.1 (Limitations on Purpose of Use) suggests that opt-in consent is required whenever there is a change in purpose. Articles 3.3, 13.1 and 13.3 should be amended in a manner that clarifies that opt-in consent is not required when the information is to be used for the specified purpose of use (for example, those purposes specified in a notice or public announcement).
- Article 3.3 seems to suggest that separate opt-in consents are required for collection, use of data for credit accommodation purposes, and for marketing purposes. The Guidelines also suggest that there are types of contractual language that impose unacceptable conditions on individuals by using their “dominant bargaining position”. The types of contractual language that raise such concerns are not clear. Businesses should be permitted to state in their application forms that individuals must agree to the collection and use of their personal information for credit accommodation purposes. Otherwise it will be impossible to provide the desired financing to customers.
- Under Article 13, opt-in consent is required to share data with third parties, including credit bureaus. This strikes us as particularly problematic for financial institutions because it would seem to allow those individuals with bad credit to prohibit the sharing of such information with the credit bureaus. Moreover, the METI Credit Guidelines, in contrast, permit such sharing, which creates an unfair advantage for those entities subject to METI’s jurisdiction. Moreover, sharing information with credit bureaus and their member companies for account analysis purposes should not require any consent (whether opt-out or opt-in), but only clear disclosure to the consumer. Particularly in light of national policies against excessive lending (e.g., Article 13 of the Money Lending Business Law), credit bureaus should be recognized as a joint-user of the customer’s financial information.

Particularly in cases where the entity collecting and using the information is the same, there does not appear to be any additional personal information protection interest served by requiring opt-in consent. In order to preserve the proper balance set forth in the Basic Law, we suggest that the sections mentioned above be revised to allow for opt-out consent.

## **Provision of Information to Third Parties (Article 13)**

In contrast to the Basic Law, the Guidelines do not exclude from its definition of a third party controlling shareholders, or those entities that are acting as an agent, engaging in joint marketing activities, or replacing existing Businesses in a merger situation. We urge the FSA to clarify in the Guidelines that the definition of third parties for purposes of the Guidelines does include these exceptions and that opt-in consent would not be required to transfer information to these entities.

The Guidelines should also clearly indicate, either by exemption from its definition of a third party or its third party consent requirements, that data may be shared with affiliates for cross marketing purposes through the use of opt-out consent. Sharing data with affiliates for cross marketing purposes is akin to joint marketing initiatives between unrelated corporate entities. In addition, a Business should be able to expand or amend the names of its affiliates with whom information may be shared through a general disclosure (such as on the website of a Business) rather than by consent.

The Guidelines should exempt from any consent requirements certain types of third party data sharing such as sharing with credit bureaus (mentioned above), with other banks or entities when it is necessary to accomplish a transaction requested by the customer, with third parties responsible for collecting payment or settlement of delinquent accounts,<sup>3</sup> in the merger context (mentioned below), or with regard to reinsurance companies. Database providers used for fraud and other background check purposes should also be deemed not to be third parties because these types of checks are made for purposes other than just paying capacity. For example, information is collected about customers and shared with database companies in order to reduce fraud, to understand the customer's habits in terms of regular payment patterns, misuse of accounts and frequent over drafts or to contact the customer if there are problems with an account

In the insurance business, opt-in consent should not be required to share personal information with reinsurance companies for proper business purposes. The purpose of sharing information is to fulfill the obligations previously assumed by the primary insurance company and, therefore, it should not be necessary to obtain additional consent from the principal. We believe that, in this circumstance, reinsurance parties are serving as outsourcing partners rather than third parties. If, however, the FSA regards reinsurance parties as "third parties," then it should make clear, where an organization has provided notice to the individual or has made a public

---

<sup>3</sup> The duty to cooperate with third parties for the resolution of debts is already recognized by the FSA's own guidelines (e.g., MBL Article 21 Guidelines, Section 3-2-7), and the Guidelines should be in harmony with these existing guidelines under other applicable laws.

announcement of the purpose of use, that the personal information may be disclosed for such purposes with the use of opt-out consent.

Article 13.3 provides that a Business shall not use any information concerning the paying capacity of financial consumers obtained from a credit bureau for any purpose other than examining the paying capacity of that person. We believe that the flat prohibition on such use of credit bureau information is inconsistent with the policy of the Basic Law that notice and individual consent should govern the appropriate use of information. Accordingly, we request that the FSA clarify that this limitation of use shall not apply when the credit bureau has provided notice to financial consumers or has made a public announcement -- whereby financial consumers will have been given appropriate notice -- of a purpose of use beyond the examination of the paying capacity of such financial consumers and further that such information may be disclosed for such other purpose of use with the use of opt-out consent. We also request that the FSA clarify that a Business may use information other than information concerning the paying capacity of financial consumers that it receives from a credit bureau subject to the credit bureau providing notice to financial consumers or making a public announcement of the purpose of use and further that such information may be disclosed for such purpose of use with the use of opt-out consent.

With regard to Articles 13.4 and 13.6, we suggest that the FSA clarify whether, in order to place a "principal in circumstances whereby matters can be easily learned," it would be sufficient to disclose a third party's or joint user's business name or homepage address. Would it be necessary to list third parties and joint users separately?

Finally, the ACCJ urges the FSA to clarify the meaning of Article 13.5 because the logic of the introduction to the paragraph seems to lead to the opposite conclusion from the one that is currently written.

### **Mergers and Acquisitions (Article 5)**

In mergers between financial services companies, it is standard practice for the purchaser to review the target company's customer information as part of the evaluation process. Prospective investors or purchasers of company assets need to review such information for due diligence purposes related to the contemplated transaction. The same applies to financial partners providing financing solutions for the purchase of goods and services. If the sharing and use of customer personal information subject to Non-Disclosure Agreements is prohibited, as it appears to be under Article 5.2, it would seriously impede M&A activity between financial services companies. Furthermore, if a company were required to notify

customers and obtain their consent, such disclosure would raise the risk of “insider trading”.

We urge the FSA, therefore, to clarify in the Guidelines that notice and consent are not required for Businesses to share Personal Information with (i) prospective investors or purchasers of their assets who need to review such information for due diligence purposes related to the contemplated transaction, or (ii) with entities providing financing solutions for the purchase of goods sold by Businesses.

### **Access/Disclosure to Principal (Article 15)**

Article 15 of the draft Guidelines states that, once the purpose of use has been achieved, a Business should destroy the applicable personal information. We request that the FSA clarify that a Business may hold information beyond the purpose of use (for example, beyond the expiration of the term of an insurance contract) in order to be able to either reply to customer inquiries received after such purpose of use has been achieved or respond to legal challenges regarding performance under a contract between the Business and its customers.

With respect to access to information, we suggest the FSA clarify that a Business is not required to maintain such information, once the purpose of use (such as the expiration of the term of an insurance contract) has been achieved, solely for the purpose of providing access to that information. We also suggest that the FSA clarify that access to personal information by the individual is limited to the period in which the information is being used to accomplish the purpose of use.<sup>4</sup>

In addition, the Guidelines should explain more fully the circumstances under which access need not be given if the business operations would be “markedly impaired.” The meaning of this phrase is unclear. The only example given mentions situations in which the volume of information requested does not correspond to the reason for the disclosure. Another example could be when requests are made to access transaction data 1-3 years after the transactions were completed. In this case, the cost of

---

<sup>4</sup> Financial organizations keep transaction data for extended periods of time for record keeping purposes. However, the cost of permitting access to all of that stored transaction data would be prohibitive. Thus, access requests for transaction data should be limited to a reasonable period of time after the transaction has been completed (e.g., 1-3 years) and all information requests should be accommodated only if such requests do not place an undue burden on the financial organization. In addition, there is a countervailing obligation under the Basic Law to retain information no longer than the period for which it will be used for the purposes for which it was collected. Thus, the Basic Law encourages organizations to delete information that is no longer needed, which means that access will not be possible once this information has been deleted or anonymized.

permitting access to all of that stored data would be prohibitive and place an undue burden on the financial organization.

It would also be helpful if the FSA clarified the meaning of the word “promptly” [“遅滞なく”] with respect to its statement that a Business Handling Personal Information must “promptly” [“遅滞なく”] disclose Held Personal Data if so requested by a Principal. It is crucial that the FSA not create guidelines that are vague and subject to subjective interpretation by individual inspectors. By drafting such vague provisions in the Guidelines, the FSA is creating a serious risk of clashes between inspectors and financial institutions during regulatory inspections.

### **Collection of Sensitive Information (Article 6)**

The Guidelines prohibit the collection of sensitive information (defined as “information relating to political views, religion (religious beliefs, thoughts, and articles of faith), membership in a labor union, ethnic group and race, lineage and domicile, healthcare and sex life, and crime records”). Given that these Guidelines would apply to the personnel (i.e., employees and other workers) of financial institutions, this prohibition may be in direct conflict with the MHLW guidelines on employees. In addition to creating a conflict with the MHLW guidelines, the prohibition on the collection of sensitive information would raise significant problems (such as inhibit the ability of institutions to run background checks, possibly provide or administer life insurance or health insurance plans, accommodate someone who is disabled, collect applicant flow data, collect and pay labor union dues, provide domestic partnership benefits, limit the ability to extend loans through a medical provider or union, reference and cause contributions to a particular charitable organization). Sensitive information may also need to be gathered to better serve customers with disabilities).

These restrictions could be especially troublesome in light of requirements that financial businesses ensure that employees in charge of money lending operations are suitable for their responsibilities (e.g., Money Lending Business Law, Secs. 24-7, 13-3). The Guidelines, therefore, should:

- (1) explicitly permit the collection and selective use of such information in the employment context;
- (2) make clear that such uses would come under the exception for collections “pursuant to law or ordinance”;
- (3) not be applicable to personal information of employees and workers of financial institutions; or

(4) allow for the collection of sensitive data for customers based on opt-out consent.

The exception for collections “pursuant to law or ordinance” should include foreign laws or regulations. U.S. life insurance companies, for example, are often required to collect information regarding the citizenship of their policyholders in order to comply with U.S. tax laws and regulations.

In addition, collection of information by video camera near an ATM or in a bank for security purposes should be specifically permitted despite the fact that sensitive personal information, such as an individual’s race or ethnic origin, might be collected as a result of such video taping.

Finally, while Article 6.1(7) permits financial companies, including insurance companies, to use or share with third parties a customer’s sensitive information with his or her consent, to the extent necessary to conduct their business, we urge the FSA to clarify that such consent should be opt-out consent, particularly where an organization has provided notice to the individual or made a public announcement of the new use and the fact that personal information may be disclosed to third parties. For example, domicile information is regularly collected by financial services companies for anti-fraud screening purposes, by making a copy of a driver’s license. The FSA should clarify that such information may be collected pursuant to Article 6.1(7) with the use of opt-out consent.

### **Securing Accuracy of Data Content (Article 9)**

The Guidelines state that information must be destroyed once the purpose of use has been achieved. This requirement is not technically feasible since it is virtually impossible to completely destroy or delete data. For example, data is almost always stored on back-up media that frequently may be stored off-site. Shadow copies of data may also exist within the computer systems. Instead, the Guidelines should confirm that a Business may suppress data or remove data from active use or delete data wherever possible.

The Guidelines should also clarify that Personal Data should not be destroyed or deleted where doing so would cause a Business to violate applicable law (e.g., instances where the law provides that a Business must retain copies of certain information material to the operation of its business for a prescribed period of time).

Regarding the proposed duty of a Business Handling Personal Information to maintain accurate personal information under Article 9, the Guidelines should clarify the proper response of a Business when it receives personal information from a Principal pursuant to law, and such information

is at odds with information received from the Principal in an application. Should the entity change the information provided by the Principal to match that provided pursuant to law, or should it keep the information as provided by the Principal?

Article 9 also states that Businesses Handling Personal Information must set forth a storage period according to the purpose of use, but, the Guidelines also stress in Article 3.1 that the purpose of use must be specific. Because a business could have many different purposes of use, we envision a situation in which different storage periods would have to be established for different purposes of use, thus requiring the same information for the same Principal to be stored repetitively for different periods of time in order to comply with Article 9. The Guidelines should clarify that this is not necessary and that a Business can make determinations regarding the retention of information based on the type of information rather than on the purpose of use.

### **Security Control Measure (Article 10)**

The security control measures covered by the Guidelines should be at a high level and not include specific and detailed security obligations. Attachment No. 5 should be presented as a "best practices" standard and the Guidelines should clearly state that a Business has no legal or regulatory obligation to follow these suggestions.

In Article 10.6, the Guidelines state that a Business must take specific "Organizational Safety Control Measures", such as the "Establishment of means enabling the confirmation of the handling status of Personal Data." The meaning of the "means enabling confirmation" is not clear. For example, does this refer to an information system, or an electronic software or hardware system? Or does it refer to a check sheet, or a confirmation means involving live persons, such as putting a compliance officer in place?

Also, under Article 10.6(1), do the Guidelines contemplate the appointment of a person responsible for managing personal data for each division of a financial services company that uses personal information, or does this mean one individual responsible for managing personal data used across an entire company?

### **Employment Contracts (Article 11)**

We suggest that the FSA clarify whether Article 11.3(1) is meant to apply only to existing employees who change jobs within the company and therefore have no reason to use and share personal information in their new

capacity, or if it also suggests that contracts must cover current and retired employees (the confusion relates to the meaning of the term “職を退いた者”).

The Guidelines require individual employment contracts with employees that would preclude them during their employment with the institution from sharing personal information with a third party for any reason other than the purpose of use. This mandatory use of contracts is not realistic. For existing employees, what happens if the employee refuses to sign an employment contract? Could their employment be terminated for refusal to sign? Would such a refusal be considered a termination for legitimate purposes? We suggest that the Guidelines permit a Business to comply with these provisions by including such obligations in the Business' work rules.

With respect to former employees, either those who have retired or resigned from the institution, Businesses have little control over their behavior once they have left their employment. Contractual provisions regulating post-employment behavior are similarly unrealistic. The Guidelines should make it clear that they do not cover employees who have already retired or resigned.

In addition, like the security control measures covered by the Guidelines, the employee supervision measures covered by the Guidelines should be at a high level and not include specific and detailed security obligations. Attachment No. 5 to the Guidelines should be presented as a “best practices” standard. In addition, any further guidelines adopted by the FSA in relation to employee supervision should be “best practices”. Any provisions regarding employees should also be consistent with the MHLW Guidelines.

### **Procedures for Responding to Request for Disclosure (Article 19)**

Instead of setting up the means to respond to a disclosure request in every branch or sales office, the Guidelines should permit the establishment of one location, or a very limited number of locations, where customers can make such requests.

### **Handling of Leakage (Article 22)**

Article 22 should make clear that the measures that apply to leakages apply to only those situations in which data are leaked as opposed to lost or destroyed. The response required after data are inadvertently leaked as opposed to inadvertently destroyed is quite different.

We suggest the following modifications to the text:

22.1 In the event a material leakage of personal information occurs, a Business Handling Personal Information in the Financial Sector shall promptly report this to the competent authorities.

22.2 In the event a material leakage of personal information occurs in the business, a Business Handling Personal Information in the Financial Sector shall use its best efforts to publicly announce the relevant facts and steps taken to prevent reoccurrence and the like to the extent necessary to prevent secondary damage and the avoidance of the occurrence of similar cases, and the like.

22.3 In the event a material leakage of personal information occurs in the business, a Business Handling Personal Information in the Financial Sector shall promptly notify the Principal or publicly announce, subject to such leakage regarding the relevant facts of such leakage.

## **Issues Not Addressed in the Guidelines**

### **Data Collected Outside of Japan**

The FSA should clarify whether the Guidelines would apply to personal information that is not collected in Japan, but transferred to Japan for processing and use or whether it would only apply to information collected and used in Japan. For example, if personal information is transferred from Europe for processing and use, would the European privacy rules or the Japanese privacy rules (e.g., notice and consent) apply or would both regimes apply? Extending the obligations of the Basic Law to such data would be overly burdensome and discourage investment in Japan. The FSA should also clarify whether the Guidelines apply to situations where the Business is located outside of Japan and the data is processed in Japan merely for the supply of a service (e.g., database storage, IT support services, and call center services).

### **Mandatory or Voluntary Provisions**

While the Guidelines lay out many mandatory provisions, some are voluntary. These voluntary provisions often represent best practices by large businesses. We believe that the Guidelines should be limited to those provisions that the government wants to make mandatory on all businesses. Businesses should be free to decide for themselves the measures appropriate for their unique operations, if any, which go beyond legally mandated requirements.

We recommend, therefore, that the FSA include in the Guidelines only those provisions that are intended to be mandatory on all companies subject to its jurisdiction. If, however, the FSA believes that voluntary Guidelines are necessary, it should make explicit that the voluntary provisions represent examples of ways that Businesses may comply with the Basic Law, or represent examples of best practices, but do not represent the only ways to comply with the Basic Law.

The Guidelines should also make clear that the failure to adopt a particular suggestion does not mean that an organization is failing to provide adequate security or to meet industry best practice standards. In addition, having recommended provisions gives inspectors too much discretion during the audit/inspection process and can undermine the inspection process. What the inspectors are required to examine should be clear (e.g., mandatory provisions); not discretionary. When Guidelines are drafted as “voluntary,” there is a likelihood that in administrative and private civil enforcement these voluntary standards will become, in the eyes of the administrative authorities and courts interpreting the law, evidence working against companies who do not comply with the voluntary provisions.

### **Compliance with Foreign Laws or Ordinances**

The Guidelines should make clear that a foreign law or ordinance qualifies for the exceptions “pursuant to a law or ordinance” contained in the Basic Law (such as Articles 16(3)(i), 18(4)(iii), 23(1)(i), and 25(1)(iii)). The Guidelines should clarify that when a global organization is required to disclose information pursuant to the law or regulations of a non-Japanese country, such a disclosure is considered a disclosure “pursuant to a law or ordinance” as that term is used in the Basic Law. In other words, compliance with the laws or ordinances of countries other than Japan should be considered a disclosure pursuant to a law or ordinance.

### **Retroactive Applicability**

The Guidelines are not clear as to whether they would apply to personal information that has already been collected by financial services companies. If so, this would be extremely burdensome and costly; it would require financial services companies to expurgate personal information from many millions of pages of documents and from CRM databases. We recommend that the FSA make clear that these Guidelines have no retroactive effect.

## **Articles Requiring Further Clarification**

### **Coverage Under the Guidelines**

The FSA should confirm that information obtained by entities that are sales agents of insurance companies, and whose information has not been shared with insurance companies, does not fall under the Guidelines.

### **Notification, etc. of the Purpose of Use in Acquisition (Article 8)**

In Article 8.3, we request that the FSA list the case where a Business acquires image data of an individual through an automated loan contracting machine as an additional example of the expression "if the Purpose of Use is clear from the circumstances of acquisition".