

**(English Version)**

**July 14, 2004**

**SUBMISSION  
OF THE PRIVACY TASK FORCE  
AND THE FINANCIAL SERVICES COMMITTEE  
OF THE AMERICAN CHAMBER OF COMMERCE IN JAPAN  
IN RESPONSE TO THE REQUEST FOR PUBLIC COMMENT  
BY THE MINISTRY OF ECONOMY, TRADE AND INDUSTRY  
ON ITS DRAFT GUIDELINES TARGETING ECONOMIC AND  
INDUSTRIAL SECTORS WITH REGARD TO THE LAW CONCERNING  
THE PROTECTION OF PERSONAL INFORMATION**

**I. SUMMARY**

We appreciate the opportunity to comment on the draft guidelines targeting economic and industrial sectors with regard to the Law Concerning the Protection of Personal Information (the "Guidelines"). As we have stated in a previously issued ACCJ Viewpoint to the Japanese government during the development of the Law Concerning the Protection of Personal Information (the "Basic Law"), entitled "Adopt the Revised Personal Information Bill", we believe 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.

Moreover, since under the scheme of the Basic Law different ministries will be responsible for sector-specific guidelines, 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 are consistent with each other. For example, the definitions and terms used and 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. Similarly, the relevant ministries should use a “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.

We believe that a number of modifications need to be made to the Guidelines before they are finalized by METI. The Guidelines lay out detailed mandatory and voluntary provisions. While many of the provisions are voluntary, often representing best practices by large businesses, the level of specificity contained in the Guidelines makes them overly prescriptive. Consistent with the Japanese government’s stated approach of promoting self-regulation, each Business needs to decide for itself the measures appropriate for its operations.

Compliance should be encouraged as a matter of policy in Japan for all companies, to promote greater transparency through even and fair enforcement of the law. By laying out explicit “voluntary” procedures and provisions, companies that really do care about compliance will interpret such provisions strictly, as an indication of where future enforcement is likely to go, and failure of a company to comply with even voluntary Guidelines may cause reputational damage. This could have the undesirable result that companies striving to comply faithfully with the law may be put on an uneven playing field as compared to competitors who view the same provisions as “merely voluntary.” Furthermore, when Guidelines are drafted as “voluntary,” there is 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.

We recommend, therefore, that METI include in the Guidelines only those provisions that are intended to be mandatory on all companies subject to its jurisdiction. If, however, METI believes that voluntary Guidelines are necessary, METI 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.

The purpose of use specification requirement (Article II.2(1) of the Guidelines) also imposes a standard on Businesses that is higher than that used in the OECD Guidelines and the EU Directive. Further, such a standard runs counter to the Japanese government's policy and the Basic Law's intent of encouraging industry self-regulation to promote standards well-tailored to each industry's particular practices. 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 employees.

In addition, the Guidelines suggest that contracts between Businesses and outsourcers are necessary and recommend the scope of measures that should be contained in those contracts. Depending on the industry sector and the relationship between the Business and the outsourcer, contracts may or may not be needed. We believe that the Guidelines should acknowledge that Businesses will need to decide for themselves whether a contract is necessary and that it will depend on the context of the business relationship between the Business and the delegate.

With respect to security control measures, we believe that the Guidelines should be high level and should be limited to a discussion of those provisions that are deemed mandatory. The Guidelines should also acknowledge that the security measures adopted will vary from Business to Business, industry sector to industry sector and will depend on the nature and sensitivity of the data in question.

We further urge METI to clarify in the Guidelines that consent is 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. If Businesses are precluded from engaging in legitimate and standard due diligence when contemplating a merger or acquisition, investment in Japanese companies may be severely hampered, and the goal of the Japanese government to encourage foreign direct investment in Japan may be thwarted.

## **II. DETAILED COMMENTS**

### **A. Definition of Personal Information (Article II.1(1) of the Guidelines; Article 2(1) of the Basic Law)**

#### **1. Business and Professional Information**

Article II.1(1) of the Guidelines includes in the definition of personal information an individual's occupation and title and information "publicized in publications". The examples of personal information provided include "information related to one's post or affiliation in a company, with an individual's name" and "information published in official gazettes, telephone books, employee lists".

We believe that 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 should be excluded from the definition of personal information or at least not subject to the same privacy requirements when such data are used for the intended business purposes. As we have seen from our experiences with EU data protection law, imposing notice and consent obligations on the collection, use and transfer of business or professional information for intended business purposes can be extremely time-consuming, expensive, and burdensome without providing corresponding privacy protection. The information one expects to find on a business card, with a few additions such as professional license information, description of professional duties, and general work schedule (e.g., the hours and days of the week the individual can be reached at work), is generally supplied by the individual with the intention and expectation that these details will be used – and disclosed – in the context of the business relationship. This is particularly relevant in Japan, where business cards are regularly exchanged in the ordinary course of business. A business contact who gives out his or her business card expects the recipient to put the information on the card into a database, to use the information to contact him or her, and to transfer the information for business purposes to others in the recipient's organization, including affiliated companies in that organization.

We recommend, therefore, that METI excludes 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". Alternatively, METI could extend to such information the exemptions that apply to the handling of telephone books and navigation systems (Article II.1(4) of the 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. While the Guidelines do exempt this information in certain circumstances, the exemption is too narrow and would not permit sending information or marketing materials to those individuals, for example.

## **2. Encrypted or Anonymized Information**

In addition to including a broad list of information that falls within the definition of Personal Information, the Guidelines indicate that such information falls within the definition “regardless of whether or not this information has been encrypted.” Encryption can be used to transmit data securely to its intended recipient and it can also be used as a means to anonymize data. In some cases, a Business may receive data, the personally identifiable elements of which have been encrypted and it is precluded from de-encrypting the data either by law and/or by virtue of the fact that it does not possess the key or that it would be difficult and unlikely to be able to obtain the key because it would involve a disproportionate amount of time, effort and expense. In such cases, the data is akin to statistical data which is cited by the Guidelines as an example of data not corresponding to Personal Information. We urge, therefore, that the Guidelines make clear that data that has been anonymized via encryption or other means and for which the Business has no legal or technical means of de-anonymizing or de-encrypting, should not be considered to be personal information.

It would also be helpful to clarify the examples of personal information cited to make them more precise and understandable to businesses (such as in the case of Example No. 5 – “information that would be capable of identifying a specific individual through an added recognition of surrounding information”), as well as to include specific examples of “information that can be easily compared with other information to identify a specific individual”. In particular, it would be useful to include examples of where “a comparison would be difficult” and “a comparison would be easy”. For the same reason, it would be useful to add a fourth example under the examples of “information not corresponding to personal information”, along the following lines: “Example 4) Anonymized information, that is, where the Business cannot identify the Principal by using reasonable and lawful means available to the Business. For instance, when a potential acquirer of a target business obtains a list of job titles and corresponding salaries, that information would be excluded from the definition of personal information

because the potential acquirer would have to make unreasonable efforts to re-identify the Principals.”

### **3. Publicly Available Information**

We also recommend that publicly available data be excluded from the definition of personal information or businesses that handle such data be exempted from the duties imposed on businesses that handle personal information. Publicly available data encompasses a wide range of data sources including public records, news reports, research made available to the public, public directories and indices, and other open sources of information. For example, if an individual posted contact information on the web on his or her home page where he or she was advertising a product for sale, any organization that wanted to use that information to contact the individual or to send that individual some marketing materials would be required to comply with all of the obligations in the Guidelines including notice and perhaps gain consent. This seems counterintuitive and unnecessary given that the individual put his or her name on the web for the very purpose of making it available to other people and organizations. Once truthful information about an individual becomes publicly available (e.g., a news story about a specific news worthy event involving a specific individual or information about an individual disclosed during a legislative or court hearing), it is unreasonable for the individual or the government to control the subsequent use of the same truthful information.

We recommend, therefore, that METI exclude publicly available data from the definition of personal information, or that at least METI limit the scope of data protection obligations applicable to publicly available data, for instance, by setting aside the obligations of notice and consent. We suggest that METI consider for its definition of publicly available data the definition used in the draft Asia Pacific Economic Cooperation (APEC) Privacy Framework (see <http://www.export.gov/apececommerce>): “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.”

### **4. Data Collected Outside of Japan**

In addition, METI 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. METI 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).

## **B. Notice/Purpose Specification (Article II.2(1) of the Guidelines; Articles 15 and 16 of the Basic Law)**

### **1. Notice Content**

Under the Article II.1(7) (“Notify the Principal”), the word “directly” should be deleted. Indeed, the notification could be made indirectly by a person other than the Business. The Guidelines appear to require that a Business describe in detail and individually all of the purposes for which it plans to use the Personal Information. According to the Guidelines, both individual and ultimate purposes must be specified. General statements such as “improving customer service” are insufficient. This requirement imposes a standard that is considerably higher than that found in the OECD Guidelines or the EU Directive. While we believe that purposes of use should be described wherever possible in concrete, easy-to-understand terms and with a reasonable degree of specificity, we believe that imposing a requirement to list every possible use would result in overly detailed and lengthy notices, making them less accessible and less likely to be read by individuals. In addition, if a notice must be provided for each purpose of use, this requirement would result in a proliferation of notices having to be issued which would impose an unnecessary and unreasonable burden on Businesses. Thus, not only would such a notice place an undue burden on Business, but it would also be meaningless to Principals and would not increase privacy protection. It should be sufficient to describe categories of purposes and related purposes without having to specify each individual purpose of use.

Indeed, even under the EU Directive, where information must be collected for “specified, explicit . . . purposes,” the requirement to give notice to the Principal is simply to give notice of the purposes of the processing. In practice, examples of purposes, as opposed to every single purpose, are routinely given. For example, it should be sufficient to list that an organization may collect information in order to: fulfill requested product orders, provide customer service and support for existing or future products purchased by the customer, provide customers with convenient access to its products and services, provide product announcements, product updates, special offers, and other information it thinks customers would like to hear

about. However, it would seem to go beyond that which is necessary to have to list also the following: “in order to manage our product stock, deliver our products to you, issue an invoice, ensure due payment, provide you with warranty services either by phone or on-site, send you product upgrades, handle any litigation between us, manage the accounting and current finances of the company, comply with our current tax and export control obligations, etc.”

## **2. Timing of Notice**

We urge METI to clarify that, under Article 18, Paragraph 2 of the Basic Law, while notice should be provided in advance whenever possible, there are situations where it will not be technically or practically feasible to provide notice in advance or at the time of collection. In the case of cookies, for example, it is not technically possible to give notice until after the cookie is set and activated. The manner in which cookies function requires that the cookie be activated, and, thus begin collecting information, before any notice can be given.

## **3. Notice Location**

The examples provided concerning the placement and form of the notices to be given suggest that the actual notice must be placed on the front page of the agreement, the Business’ homepage, or on the terminal device of the Principal. The Guidelines should make clear that a reference to the location of the notice (e.g., that the notice can be found at the back of the written agreement) or a click-through link to the notice on a homepage, or other website linked to the homepage, is equally acceptable.

## **4. Notice Regarding Videosurveillance**

Furthermore, because under Article II.1(1) of the Guidelines “information recorded by security cameras and other image information capable of identifying an individual” is cited as an example corresponding to Personal Information, it is unclear under the Guidelines whether a video image alone is personally identifiable or whether additional information about the individual is needed to make the video image personal information. If the video image alone constitutes Personal Information, then it is also unclear, if the building owner hires a third party to provide building security, whether the building owner or the security company is the entity responsible for posting notice of its purpose of use. If the security company were responsible, then, under Article 23, Paragraph 2 of the Basic Law, the security company also would need to provide the principal with the ability to opt out of the sharing of the image with the building owner, unless Article 23, Paragraph 1(ii or iv) of the Basic Law applies in this instance. We recommend, therefore, that the Guidelines make clear that the video image

alone does not constitute Personal Information or, at a minimum, make clear that opt out consent obligations do not apply to the use of video images for security purposes.

## **5. Miscellaneous**

Finally, it would be helpful to provide more examples of when it is “difficult” and “not difficult” for the Principal to foresee purposes of use. The example provided in the Guidelines under Article 15, Paragraph 2 is very narrow. A Business’ data processing needs will grow with the size of its business and Businesses should not have to ask for consent for any new type of purpose of use. For example, a medium-sized Business may process employee data for mere human resources and payroll purposes. If it grows, it may launch a stock option plan or other employee benefits plan. This should not be considered as a different purpose of use requiring employee consent, and it should be deemed within the scope of what is reasonably foreseeable by the employee. In addition, the Guidelines should state expressly that “law or ordinance” in Article 16, Paragraph 3, Item (i) of the Basic Law includes foreign laws or ordinances as well as Japanese laws and that a “national agency or the like” in Article 16, Paragraph 3, Item (iv) of the Basic Law includes foreign governmental agencies as well as Japanese governmental agencies.

### **C. Security (Article II.2(3)2)-4) of the Guidelines; Article 20 of the Basic Law)**

#### **1. Mandatory or Voluntary**

The sections of the Guidelines relating to security are quite extensive. Although for most of these provisions, METI appears to indicate that they are “desirable” and, therefore, presumably voluntary, the likely effect will be that they will become the de facto standard and regarded as mandatory. These security provisions would require that virtually every organization in Japan establish a formal information security department for the handling of personal information and that each set up a new internal organization to deal with access, audits, classification schemes, physical and electronic security, training, supervision, contract negotiation and ledgers.

An information security program should be tailored to the particular organization and should take into consideration the type of information being handled by the organization. A small manufacturer of handbags should not be held to the same standard as a major multinational corporation. Likewise, a steel manufacturing concern will have different data security needs than would a travel agency or an internet access provider.

## **2. Encryption**

We urge METI to ensure that the Guidelines should have sufficient flexibility to enable these different types of businesses to each shape an effective information security program appropriate for the size and complexity of the Business, as well as the reasonable likelihood that the Business will be dealing with substantial amounts of sensitive personal information. For example, in Article II.2(3)-2 of the Guidelines, the organizational security control measures section (“Matters Desired for Inclusion in Rules, Etc, Concerning the Handling of Personal Data”) appears to recommend that there be “encryption of personal data upon the transfer and transmission thereof (for example, when transmitting personal data using public lines), and confirmation of the destination and confirmation of receipt upon transfer for example the use of mail that documents delivery, or the like).” Encryption may be appropriate when very sensitive information is being transmitted if the circumstances of the transfer put such information at risk. There are other methods for protecting transmitted personal data that do not involve encrypting such data such as using a privately leased line or other secure path for unencrypted data. As written, however, the Guidelines recommend the encryption of virtually every e-mail (most e-mails contain the name and e-mail address of the individual sending the message) regardless of whether the e-mail contains sensitive or confidential information. In addition, if an organization is transmitting business contact information (name, work email, and work phone number) of their vendors from whom they purchase office supplies, it seems extreme to require that such a transmission be encrypted.

Not only would the cost of encryption be prohibitive, but encryption only works if the recipient has the ability to un-encrypt the message. Thus, in order for an organization to send information, it would first be required to ensure that the recipient had a compatible ability to un-encrypt the message. Similarly, if an organization is sending a package by postal mail that contains non-sensitive personal information the use of mail that confirms delivery will drastically increase the cost of sending such a package.

Further, a blanket encryption requirement might impede a Business’ ability to comply with different, potentially incompatible, government regulations. For example, the U.S. Securities and Exchange Commission requires companies to produce e-mail messages within a certain time period. If a significant number of those messages were encrypted, it would severely impair a Business’ ability to comply with that regulation.

## **3. Flexibility**

We believe that the Guidelines should not propose a “one-size-fits-all” solution that requires that all information should be encrypted or that every

transaction should create an audit trail that is entered into an audit ledger. Rather, we believe that the Guidelines with respect to security measures should be very high-level in nature and simply state that an enterprise handling personal information must adopt the organizational, personnel, physical and technological security measures to prevent unauthorized disclosure, loss or use. The adequacy of the security measures should be assessed in light of the state of the art in the concerned industry, which would give enough flexibility to take into consideration technological changes. If METI believes some examples are necessary, it should limit the number of examples and clearly state that they are illustrative, and not necessarily applicable or appropriate for every Business. METI also should state that the security measures adopted will vary from Business to Business and industry sector to industry sector and will depend on the nature and sensitivity of the data in question.

In addition, many organizations already have systems in place to ensure the protection of confidential information, such as trade secrets, and thus those organizations should be enabled to extend their existing processes to cover personal information rather than be required to set up an entirely new infrastructure. If organizations are encouraged to extend existing security programs to protect personal information in the particular context of each organization, the result will be in greater protection of personal information. Companies will be able to utilize their existing infrastructure to much more quickly increase the protection of personal information. Also, as these existing systems will often have been time-tested, the resulting security will likely be more robust than security associated with a newly adopted program according to a regulatory mandated scheme that may or may not be appropriate for the particular business.

#### **4. Employee Non-Disclosure Agreements**

Similarly, in the section on Personnel Security Control Measures, it is suggested that organizations have non-disclosure agreements with employees. As written, this obligation would apply to every employee of the organization without respect to whether the employee had access to trade secrets or to personal information. Moreover, the level of detail required in the non-disclosure agreement including the list of individuals who have access to a building and the terms and conditions under which non-employees can enter a building will mean not only that the contracts will be extremely lengthy, but that the average employee will not be able to understand to what he or she is agreeing. Thus, it appears that the obligation will be a significant burden on organizations and will do little to enhance security of personal information.

**D. Supervision of Delegates -- Outsourcing (Article II.2(3)4) of the Guidelines; Article 22 of the Basic Law)**

**1. Verification**

The Basic Law requires that a Business, in the event that it delegates any or all of its handling of personal data, engage in the “necessary and appropriate supervision” of the delegates. The Guidelines suggest that such supervision may include incorporating the security control measures to be followed in a contract and “causing compliance with the content of the corresponding agreement, or regular verification at predetermined intervals”. Regular verification at predetermined intervals is prohibitively expensive. Often contractual guarantees are used instead of physical inspections or audits. If a vendor were required to provide regular verification reports to its clients, the vendor would spend all of its time responding to verification requests as opposed to carrying out the processing duties for which it was hired.

**2. Contracts**

The Guidelines need to recognize that, depending on the industry sector or the Business concerned, outsourcing agreements or contracts may or may not be necessary. For example, a Business could have a long established business relationship with another Business that routinely provides services to it. In this case, the contract may not be necessary. The same would be true if the Business outsources to one of its affiliates. Moreover, in Japan, since both businesses would be subject to the Basic Law, a contract might be unnecessary. By way of comparison, the EU Directive does not require a contract – it merely requires that such processing “be governed by a contract or legal act binding the [delegate] to the [Business] and stipulating that the [delegate] shall act only on instructions from the [Business] and shall comply with the data protection laws.” For this reason, we believe that the Guidelines should acknowledge that businesses must decide for themselves about whether a contract is necessary and that it will depend on the context of the business relationship between the Business and the delegate.

**3. Exception for Lawyers, Public Accountants, Etc.**

The Guidelines also suggest that delegates should be precluded from divulging the information they process. Since many outsourcing relationships do require disclosures, blanket prohibitions on divulging information may not be appropriate. For example, if an organization retains

a public relations firm, it is appropriate for the public relations firm to provide information to the public. That is the purpose of the relationship. Similarly, delegates, such as lawyers and public accountants, are legally and ethically bound to maintain the confidentiality of information they receive. Consequently, the Business should be the one to determine the conditions or requirements to be imposed on the delegate; the Guidelines should not suggest or imply that the failure to include such provisions is an indication of improper supervision of delegates.

#### **4. Data Retention**

The Guidelines also appear to suggest that contracts should specify that Personal Data should be destroyed or deleted. First, the Guidelines should acknowledge 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). In addition, 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 indicate that a Business may suppress data or remove data from active use or delete data wherever possible. Indeed, even in the EU Directive does not require deletion or destruction of information, the general principle is that information must be kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the information was collected or processed. Moreover, organizations often have legitimate reasons for retaining information relating to the services it provided to a customer. For example, if an outsourcing relationship ended in the middle of a long-term contract (e.g., 7-10 years), the third party might be required to retain the information until after the contract has been closed out and audited by the customer. In addition, if a litigation or other dispute has arisen and the personal information is relevant, a third party may be legally precluded from destroying or deleting the personal information. In practice, the information might be required to be retained until all statutes of limitation applicable to possible claims among the parties had lapsed. Instead, the Guidelines should indicate that a Business may suppress data or remove data from active use or delete data wherever possible.

#### **5. Copying**

The Guidelines also appear to suggest that contracts should prohibit processing and use by delegates outside the scope of the outsourcing agreement. In addition, the Guidelines appear to suggest that contracts

should prohibit delegates from copying or reproducing personal information. There are many legitimate reasons why a delegate may be required to reproduce personal information as part of its duties. For example, a delegate may be required to translate the information into a different language or the delegate may be obligated to convert the information into machine code for the purposes of processing the information. Both actions could be considered a form of reproducing or copying the information and thus prohibited under the Guidelines.

**E. Provision to Third Parties (Article II.2(4) of the Guidelines; Article 23 of the Basic Law)**

Article II.2(4) of the Guidelines makes explicit that affiliates are considered to be third parties. We believe the Guidelines should make explicit in this Article or elsewhere in the Guidelines that affiliates are exempt from some or all of the obligations placed on third-party sharing of data. Indeed, in the framework of a corporate group, it is usual that several affiliates are involved in data processing to carry out the same purpose. In an example of customer contract management, one affiliate may be in charge of customer management and take orders, while another affiliate ensures the manufacturing of some equipment parts, while another affiliate takes care of maintenance, while even another affiliate runs the servers and the database used to store the customer's information. As far as the customer is concerned, this organization of tasks has no impact on his/her privacy interests and his/her data would be handled the same way as if only one legal entity were handling it. Requiring customer consent for the sharing of information in such a case would adversely affect large organizations, which would have to restructure their legal entities, and in most instances they would not be able to perform a customer contract if a customer refused to give consent to the transfer of information to other affiliates of the corporate group.

At a minimum, METI could distinguish between those Businesses with whom the Business has an ongoing relationship (as would be the case with affiliates) and those with whom it does not. For those organizations with which it has an ongoing relationship, the Business and the third party or the Business and its affiliate, should have the ability to determine which of the two entities will assume responsibility for the proper handling of the personal information. This may be accomplished either through contract or some other means such as codes of conduct or internal corporate rules (with respect to affiliates). For those organizations with whom the Business has no ongoing relationship and for whom it is not able to remain accountable, notification at the time of collection or consent to transfer personal information may be appropriate.

**F. Consent of the Principal (Article II.1(10) of the Guidelines; Articles 16(1), 16 (2), 16(3), 23(1) of the Basic Law)**

**1. Opt-In/Opt-Out**

Article II.1(10) of the Guidelines appears to recommend the use of opt-in consent as the preferred form of consent. No examples of opt-out consent are provided, thereby suggesting that an opt-out approach is not acceptable. This is inconsistent with Article 23 of the Basic Law which makes plain that, if the appropriate prior notice is provided, opt-out consent is acceptable. Interpreting consent in the Basic Law to require opt-in imposes a very high and unreasonable burden on Businesses. The conduct of the Principal should also be interpreted as providing consent in some instances; provided that clear notice has been given to the Principal, and that, under such circumstances, it is therefore clear that the individual by his/her acts consents to the data processing. Such could be the case when notice is provided by a pre-recorded message on the telephone, and the Principal, after having heard the notice message, continues with the call, or when notice is clearly provided on a website and the individual continues surfing on the site after having seen the notice. Failure to clarify the availability of opt-out procedures could have a negative effect on a wide range of economic activity, including marketing aimed at bringing offers to consumers, dampen economic growth, and be inconsistent with the approach of the Basic Law.

**2. Mergers and Acquisitions**

In addition, the Guidelines should clarify that consent is not required to share Personal Information with prospective investors or purchasers of company assets who need to review such information for due diligence purposes related to the contemplated transaction or to financial partners providing financing solutions for the purchase of goods and services. It is often the case that discussions regarding a potential merger or acquisition are highly confidential until after some degree of due diligence has been completed. Also, disclosing the proposed transaction to individuals raises the risk of "insider trading". Thus, it would be unworkable to provide sufficient information regarding the potential transaction to individual employees such that they can provide informed consent. Even under the EU Directive, which arguably has the most burdensome requirements, disclosures without consent would be allowed in such circumstances. Additionally, authorities in the EU are actually questioning the use of consent in the employment context because of the imbalance of power between

employers and employees. Wherever possible, a Business would anonymize the data but there may be instances where such anonymization is not possible. For example, a prospective investor or purchaser of a Business might request information on the compensation packages offered to senior executives to determine if it can replicate their compensation or to determine whether after a merger the new company would be required to hire additional employees. In such cases, consent should not be required and the Business should be able to share the information with the potential investor or buyer without obtaining the consent of the individual employees. If consent were required under such circumstances, it would be very difficult to conduct merger and acquisition transactions and foreign direct investment into Japan could be severely hindered.

### **3. Sale of Equipment**

In the context of a sale of equipment, Businesses provide their customers with several ways of payment, some of them involve a financing solution provided by a third party. It would be detrimental to commerce if Businesses had to wait and obtain the consent of customers to build their offer, including the various financing solutions available to them. It would also impair commerce if, once a sale is concluded, a company, which could lawfully assign its account receivables to a financial organization, had to obtain, in addition, the consent of its customers to transfer the data relating to the assigned account receivable.

#### **G. Acquisition of Personal Information (Article II.2(2); Articles 17 and 18 of the Basic Law)**

The Guidelines should clarify that Article 17 of the Basic Law (“An Enterprise Handling Personal Information must not acquire Personal Information by fraud or other unjust means.”) includes only willful conduct and does not include negligence. Additional examples would be helpful. In addition, it may be better to use examples other than the one pertaining to the acquisition of Personal Information from a child. Collection of information from children raises a number of very complicated issues. For example, a Business may need to obtain from the child Personal Information of his or her parents in order to confirm with the parents that the child may participate in a game or contest sponsored by the Business.

It should be made clear that all cases where data is not collected directly from an individual should not be systematically considered as “acquisition by fraud or other unjust means”. Acquiring information from public sources (such as newspaper articles) is not an unjust means of

acquisition. Nor is asking questions to an employee or a distributor about his/her next of kin (e.g., to find out if a spouse works for a government agency) in order to prevent conflicts of interests and other risks.

#### **H. Disclosure of Held Personal Data (Article II.2(5)2))**

The examples provided in the Guidelines when a disclosure could markedly hinder the implementation of business operations are rather narrow. In a litigation context, for example, Businesses often must assess the cost of litigation, including the amount of damages, for budgeting purposes. It would be very detrimental to a Business if it had to provide this assessment to an employee, customer, or other business partner with whom it is in litigation. It may also be extremely disruptive for a Business to have to provide its employees with prospective data. For instance, managers often suggest the amount of employee raises, but these are not definite amounts, as they have to obtain the approval of other managers and to ensure that the budget is available and to ensure that employees are treated fairly. Having to disclose interim data would seriously disrupt the activities of a Business.

#### **I. Revision of Held Personal Data (Article II.2(5)3) of the Guidelines; Article 26 of the Basic Law)**

With respect to Article 26, Paragraph 2 of the Basic Law, it would be helpful if the Guidelines also clarify that a business may undertake the correction in the way that the Business considers as reasonable and that the correction does not need to be made in the exact way requested by the Principal.

#### **J. Record Retention and Disclosure of Held Personal Data (Article 11.2(5)2) of the Guidelines; Article 25 of the Basic Law)**

The Guidelines are silent on the issue of how long personal information records must be retained by Businesses and may be accessed by Principals. It would be helpful if the Guidelines were to indicate what would constitute an appropriate period of time, taking into account that which would be a reasonable and appropriate period often may vary from Business to Business and industry sector to industry sector. Without setting forth some guidance in this regard, the Guidelines may be interpreted as requiring that such records be retained indefinitely and further as permitting a Principal to request disclosure of such records perpetually, which is neither reasonable, nor commercially practicable nor consistent with good privacy practices. We recommend that the same rules that currently apply to document retention

and document disclosure requirements for each industry should apply to personal information records retention and document disclosure requirements for each such industry.

### **III. REQUESTS FOR FURTHER CLARIFICATION**

The intended meaning of the following sections of the Guidelines is unclear and we request greater clarification from METI in each such instance:

A. *Purpose and Scope of Application (Article I of the Guidelines).* The last paragraph of this Article states that “business groups and the like, based on their corresponding actual business conditions, may establish their own autonomous rules which cover the affiliate companies of the group, and may establish group guidelines.” It is unclear exactly what these autonomous rules may be. Are the Guidelines suggesting that some type of corporate codes of conduct or rules can be used and, if so, what would be the relationship between these rules and the Guidelines? Are they in addition to or in lieu of the obligations in the Guidelines? Would ministerial review and/or approval of these rules be required? The Guidelines should clarify that such rules may be voluntary. Industry guidelines should be deemed purely internal to members of that industry, and only provisions stated as being binding in the Guidelines should be deemed binding on Businesses.

B. *Examples Not Included in Calculations of the Number of Specific Individuals under the Definition of Enterprise Handling Personal Information (Article II.1(3) of the Guidelines; Article 2(3) of the Basic Law).* In the 4th Example, what does “have no interest in the context thereof mean”? For example, does this mean that a warehouse should not have any knowledge whatsoever of the contents of any deposits made in such warehouse?

D. *Example Where Consent Required (Article II.2(1) of the Guidelines; Articles 16(1), 23(1) of the Basic Law).* Please provide further examples of where prior consent of the Principal is required.

E. *Examples Under Article 16(3), Item ii of the Basic Law (Article II.1(1) of the Guidelines).* The Guidelines in describing the Basic Law include two examples of instances where it is not necessary to obtain the prior consent of the Principal because disclosure is necessary for the protection of life, person or property and it is difficult to obtain the Principal’s prior consent. For greater clarity, we recommend including another example whereby a financial institution searching for a missing debtor may ask

neighbors of the debtor for the debtor's current address. In addition, under the first example given, it states: "the results of careful examinations or information concerning the medical examination or the like are provided to researchers or the like without names." Is it correct to understand that the information provided is no longer personal information because it is no longer personally identifying when the name is removed? Or is it correct to understand that the information remains personal information for purposes of the Basic Law, but that by removing the name the provider is only excepted from the prior consent requirement? If the information remains personal information, does the initial provider remain liable for the acts of third parties regarding such information?

F. *Examples Where Notice to the Principal or Public Announcement Required (Article II.2(2) of the Guidelines; Article 18(1) of the Basic Law).* Please clarify what would occur when the personal information of a Principal is also the personal information of another individual. For example, the address of several family members is often the same. In such a case, is a Business required to notify the individual(s) who did not provide such information to the Business of the purpose of use?

G. *Examples Under Article 18(4), Item ii of the Basic Law (Article II.2(2) of the Guidelines).* The Guidelines should include more examples of "other matters related to corporate secrets" such as credit standards.

H. *Examples Under Article 18(4) Item iv of the Basic Law (Article II.2(2) of the Guidelines).* The Guidelines should also clarify that the provisions of Paragraphs 1 through 3 of Article 18 of the Basic Law shall not apply when a financial institution requests a customer to submit an application containing certain personal information in such case where the clear purpose of use is for the identification of the customer and the collection of his or her claim.

I. *Role of a "Chief Privacy Officer (Article II.2.(3)-2) of the Guidelines; Article 20 of the Basic Law).* The Guidelines should clarify whether the position held by a "person who protects and controls personal information (a so-called 'Chief Privacy Officer')" needs to be a full-time position, or whether a "Chief Privacy Officer" can hold concurrent posts within a Business.

J. *Examples Regarding Protection from Divulgence, Damage or Loss of Collected Records (Article II.2.(3)-2) of the Guidelines; Article 20 of the Basic Law).* The Guidelines should give some examples of what is considered "appropriate protection from the divulgence, damage or loss of collected records."

K. *"Necessary and Appropriate Supervision" of Delegates (Article II.2(4) of the Guidelines; Article 22 of the Basic Law)*. Because what constitutes "necessary and appropriate supervision" can vary Business to Business and industry sector to industry sector, the Guidelines should clarify that what constitutes "necessary and appropriate supervision" may vary according to the amount of the delegated personal data, the period of delegation and other factors.

L. *Matters Desired for Inclusion in Agreements When Delegating the Handling of Personal Data (Article II.2(3)-4) of the Guidelines; Article 22 of the Basic Law)*. According to the fourth bullet point set forth under this article of the Guidelines, it is desirable to include in a delegation agreement provisions regarding the content and frequency of reports to the delegating party concerning the "status of the handling of personal data". Please clarify what such status is intended to mean and include.

K. *Article 23, Paragraph 4, Item ii of the Basic Law (Article II.2(4) of the Guidelines)*. Given the need for companies to engage in legitimate and standard due diligence when contemplating a merger, acquisition or other financial investment, the Guidelines should clearly provide that consent is not required to share personal information with prospective investors or purchasers and any provisions to the contrary should be deleted. According, we recommend deleting the sentence that reads "It is important to be careful since an internal examination, and provision of one's own personal data to the other company prior to the succession of the business operations does constitute a provision to a third party."

M. *Examples of Delegation of Personal Data (Article 23, Paragraph 4, Item i of the Basic Law)*. The Article provides that providers of personal information to delegates remain responsible for supervising how personal data is handled by its delegates. While we agree in principle that providers of personal information should supervise their delegates, the second example given provides a situation where supervision may not be possible. In this example, a department store hires an express courier to deliver goods to a customer. In order to deliver the goods, the store must provide the courier with personal information of its customer (e.g., name, address and telephone number). Although the courier is performing a service on behalf of the Business, the Business does not usually have a contractual right to supervise or control how the personal information given to the courier is handled or used. The courier, in this instance, however, would be subject to the Basic Law and should, therefore, be responsible for providing notice directly to the individual concerned and obtaining consent of that individual before it uses the information for any other purposes.

N. *Examples of Jointly Used Items of Personal Data (Article II.2(4) of the Guidelines; Article 23(4), Item iii of the Basic Law)*. Clause (b) of this Item provides that the respective joint users would not need to be identified as long as the framework (*gaien*) of the scope of the joint use is made clear from the perspective of the Principal. The Guidelines should provide some descriptions of appropriate frameworks (*gaien*) as examples. Clause (c) of this Item provides that the purpose of use by joint users “may not be for separate purposes of use”. The Guidelines should clarify what is meant by “separate” purposes of use by providing examples of the same purpose of use and separate purposes of use.

O. *Further Examples Under Provisions for Joint Use (Article II.2(4) of the Guidelines; Article 23(4), Item iii of the Basic Law)*. The Guidelines show examples of items of personal data allowed under Joint Use and state that certain examples (specifically (a) and (b)) “may not be modified”. Does this mean that Joint Use is only allowed for items in this example? We believe that items of personal data allowed under Joint Use should not be restricted in this manner, but rather the Guidelines should be flexible and allow for items of Joint Use that are appropriate to the particular Business and industry sector.

P. *Revision of Held Personal Data (Article II.2(5)-3) of the Guidelines; Article 26(2) of the Basic Law)*. The Guidelines should clarify that a Business may implement a correction requested by a Principal in the way that such Business considers reasonable. That is, a Business should not be required to implement a correction in the exact way requested by the Principal so long as such Business adopts a reasonable means of making the requested correction.

Q. *Procedures for Complying with Requests for Disclosures, Etc. (Article II.2(5)-6) of the Guidelines; Article 29 of the Basic Law)*. In Example 4) under Item iii of this portion of the Guidelines, clarification should be made that, when confirming that the person making a request for disclosure is the Principal or an agent thereof, a Business may examine a copy of such person’s driver’s license or resident’s card (not both as presently contemplated by the draft Guidelines). Under the Law Concerning Identification, etc. of Customer, etc. by Financial Institutions, etc. (*Honnin Kakunin Hou*) and its enforcement regulations, the submission of either a driver’s license or a resident’s card is a sufficient form of identification (*honnin kakunin shorui*).

R. *References to the Term “Homepage”*. The Guidelines frequently refer to the term “homepage”. The term “homepage” implies that it is limited to the single gateway page of a website. It would be more accurate

to replace the term “homepage” with either the word “website” or the phrase “website linked from a homepage” to avoid an unintended limitation that is inconsistent with business or technical practices.

*S. Request for Further Clarification Regarding Retroactive Application of the Basic Law.* METI should make clear in the Guidelines that the Basic Law only applies to personal information gathered after the effective date of the Basic Law and will not be applied retroactively. Applying the requirements of the Basic Law to personal information collected prior to the effective date of the Basic Law would impose an unreasonable burden and expense on businesses.

#### **IV. CONCLUSION**

To be effective, privacy rules must reflect both the legitimate need of consumers and employees to protect privacy and the legitimate needs of businesses to preserve the free flow of information in a global context. The free flow of information often serves the interests of consumers and employees. We believe that, by adopting a balanced approach to privacy, Japan can reap huge benefits from increased productivity and competitiveness for its economy – serving job seekers, employees, employers, investors, and tax payers alike. Proceeding without such a balance, however, by over-regulating and restricting data flows in a global information economy, will make it extremely difficult for global businesses to deliver cost-effective and customized services to their customers in Japan and around the world and will only discourage and diminish business investment and activity in Japan.

We believe that Japan can play a leadership role in developing a flexible and tailored privacy approach that is responsive both to the global needs of business, reflecting the way in which data processing is now conducted, and the need to appropriately protect data and individuals. We urge the METI to address the issues we raise in these comments before it finalizes these Guidelines. Establishing privacy guidelines without taking these issues into account would result in a privacy regime that will become ever more unworkable and will thwart the further development of electronic commerce without providing a high level of privacy protection to individuals living and working in Japan.