



Personal information protection law

Japan



Contents

Introduction	1
Purpose	2
Legislative framework	3
Scope	4
Obligations on businesses	5
Potential implications and the future	14
Conclusion	17

For further information
please contact

Akihito Katayama
Ark Mori Building 18F
1-12-32 Akasaka
Minato-ku
Tokyo 107-6018

T+ 81 3 3584 8331

F+ 81 3 3584 8501

E akihito.katayama@freshfields.com

W freshfields.com

The information and opinions contained in this document are not intended to be a comprehensive study, nor to provide legal advice, and should not be relied on or treated as a substitute for specific advice concerning individual situations.

©Freshfields Bruckhaus Deringer 2005

Introduction

Privacy and data protection issues are of fundamental importance in all industrialised democratic countries. The 1970s, '80s and '90s saw legislative developments around the world, and Japan passed an act protecting computer-processed personal data held by administrative bodies (*gyousei kikan no hoyuu suru denshi keisanki shori ni kakaru koj-in jouhou no hogo ni kansuru houritsu*) in 1988. This followed an international comparative study of privacy laws and consequent legislative recommendations by a government research committee.

Although the Japanese government had preferred to encourage industry self-regulation rather than national legislation, it had to respond to consumers' heightened awareness of the need to protect personal information at the national level because of the passage of several local ordinances throughout the 1990s and the ever more vocal media reports on privacy violations by both businesses and the government.

Following the publication of a report by a government working group in November 1999 and outline legislative proposals in October 2000, and prolonged debates in the diet and the public arena, Japan implemented the personal information protection law (*kojin jouhou no hogo ni kansuru houritsu*) (the Act) and other relevant acts in May 2003. The parts of the Act related to information held in the private sector are currently a hot topic in the Japanese business community as they came into force on 1 April 2005.

Purpose

Developments in new technologies to transact business efficiently, and the wider use of such technologies, have resulted in changing relationships between businesses and consumers, with increased privacy risks. The Act protects the rights and interests of individuals by establishing legal requirements to be observed at national government, local government and private sector business levels. This client guide provides a broad and introductory overview of the Act's provisions and related guidelines applying to businesses operating in Japan.

In summary:

- the Act protects individuals by regulating the handling of information by private sector businesses;
- the Act only protects living individuals, affording no protection to corporations, partnerships or other forms of association;
- subject to limited exceptions, it requires businesses, among other things, to:
 - use personal information for a clearly defined purpose, which must be notified to the individual concerned;
 - use lawful and proper means to acquire personal information;
 - maintain the accuracy and currency of personal information;
 - implement appropriate measures to maintain the security of information;
 - allow individuals to access their personal information; and
- through setting new privacy protection standards and implementing penalties for failure to meet the required standards, the Act imposes the risk of losing customers on companies that do not uphold their privacy policy or the Act's minimum standards. Conversely it incentivises businesses to boost consumer confidence by ensuring that their privacy policies are met.

Legislative framework

One of the new legislative framework's features is the split between the rules implemented at the national level by the Act, and the detailed guidelines produced by the various government ministries for the business sectors for which they are responsible. Companies seeking to ascertain their obligations under the Act will also have to refer to these guidelines and interpret the Act according to their activity. This legislative system strikes a balance between the US arrangement of sector-specific laws enforced by independent regulatory agencies and state-attorneys general, and the EU model of overarching legislation enforced by independent data protection agencies.

A full analysis of the various guidelines is beyond the scope of this guide, but we do refer to some matters in the guidelines that are of particular interest to businesses in Japan.

Scope

The Act makes different provisions for the following three classes of information.

Personal information

The Act broadly defines ‘personal information’ (*kojin jouhou*) as information about a living individual that distinguishes him from other individuals. This would include, among other things, his name, date of birth, postal and email addresses, job title, photograph, employment information, information in the phone book, public journals and personnel lists.

It also comprises information that does not, on its own, distinguish a specific individual but which supplements public information, and thereby distinguishes a specific individual. It even includes information that, with the addition of subsequent information, becomes sufficient to distinguish a particular individual (at which point it becomes personal information).

According to guidelines established by the Ministry of the Economy, Trade and Industry (the METI Guidelines), email addresses such as ‘keizai_ichiro@meti.go.jp’ can be personal information, as the email address distinguishes the individual Ichiro Keizai, who is employed at the ministry. Conversely, email addresses such as ‘abc012345@ispisp.jp’ are not classified as personal information because they do not differentiate a specific individual.

Personal data

‘Personal data’ (*kojin deta*) is defined as personal information stored on a database. A ‘database’ is broadly defined as a collection of information arranged so that it can be retrieved by computer, or information structurally constituted to facilitate easy retrieval.

Held personal data

‘Held personal data’ (*hoyuu kojim deta*) is personal data that a business handling personal information (see below) has authority to disclose, correct, add to, delete, stop using or stop providing to third parties. Excluded from this definition is personal data specified by government decree as a matter that, if disclosed, will harm the public interest, and personal data that will be deleted within six months.

Obligations on businesses

This section outlines the main obligations on businesses under the Act.

The Act defines businesses handling personal information (*kojin jouhou toriatsukai jigyousha*) (BHPIs) as persons/entities that use a personal information database for business. This can include using personal information on employees for internal human resources purposes or personal information on customers for sales or promotional activities. BHPIs have different obligations under the Act for each of the three types of information defined above, but a government decree excludes businesses that have had 5,000 persons or less on their database on any day within the last six months from the BHPI definition. The following summary outlines the scope of the obligations under the Act and how some of the relevant guidelines supplement it.

Personal information provisions

Article 15 (specification of the purpose of use) provides that a BHPI must specify how it will use the personal information it holds. It is difficult to assess the extent of this requirement, but it would seem sensible to conclude that it will be determined in proportion to the nature of the information held and the type of business holding it. For example, the METI Guidelines confirm that, in practical terms, this obligation will be discharged by ensuring that the individual concerned can make a rational judgement as to the precise purpose of use to which his personal information will be put. But merely expressing the purpose of use in abstract terms, such as stating that it will be used for 'business purposes' or for 'improving customer service standards' will be insufficient.

If the purpose of use changes, the subsequent purpose must be 'reasonably related' to the original. Similarly, guidelines published by the Ministry of Health, Labour and Welfare, which set out measures to be taken by BHPIs to ensure the proper use of personal information on past, present and future employees, as well as job candidates who are unsuccessful in an application to the company concerned (the Employment Guidelines), require the purpose of use to be specified in concrete terms so that the employee concerned can understand how his personal information might be used.

Article 16 (limitations on the purpose of use) restricts how BHPIs can use personal information to achieve the purpose of use pursuant to article 15. This restriction does not apply if:

- the prior consent of the relevant individual is obtained;
- use is authorised or required under Japanese law;

- the restriction should be ignored to protect life, safety or property where it is difficult to obtain the consent of the individual concerned;
- the restriction should be ignored in the interest of the improvement of public health or the sound upbringing of children, where it is difficult to obtain the consent of the individual concerned; or
- obtaining the consent of the individual concerned might impede the execution of government business.

The Employment Guidelines state that, where the consent of the individual concerned is required, it is desirable for the business to publicise or inform him of the purpose of use and give him the opportunity to show his consent to the proposed arrangement, either orally or in writing (this also applies to article 23 below). Also, the Ministry of Justice issued guidelines on the management and collection of receivables by companies authorised by article 3 of the special measures law¹ regarding servicer business (the Servicer Guidelines), which provide that the preparation and sale of information lists acquired to collect the receivables are beyond the purpose of use in article 16.

Article 17 (appropriate acquisition) prohibits a BHPI from acquiring personal information by fraud or other unfair means.

Article 18 (notification of the purpose of use on acquisition) provides that on acquiring personal information, a BHPI must promptly notify the individual concerned of the purpose of use, or publicly announce it (unless this has already been done). In addition, if a BHPI acquires the personal information in a contract or other document from the individual concerned, the BHPI must disclose the purpose of use to him in advance. However, the latter obligation does not apply where notification might cause harm to the life, safety or property of the individual concerned or a third party. The guidelines for the finance sector issued by the Financial Services Agency (the FSA Guidelines) and the Servicer Guidelines provide that notification must be in written form and that public announcement of the purpose of use must be made in an 'appropriate manner' to the business concerned.

If the purpose of use changes, the BHPI must notify the individual concerned or publicly announce the change. However, this does not apply where:

¹ The special measures law requires companies engaged in the collection of debts to obtain a licence from the Minister of Justice.

- there is a risk of endangering the life, safety, property, rights or welfare of the individual concerned, or the rights or profits of the BHPI;
- co-operation is required with the execution of a government operation and informing the individual concerned might impede the execution of this business; or
- the purpose of use is clear from the circumstances of the acquisition of the personal data.

Personal data provisions

Article 19 (securing accuracy of content) requires BHPIs to endeavour to maintain accurate personal data in a current format to the extent necessary to achieve the purpose of use. The FSA and Servicer Guidelines, and the guidelines produced by the Ministry of Internal Affairs and Communications for telecoms companies (the Telecommunications Guidelines), require BHPIs to set time limits for the retention of such data and to return or dispose of it once the time limit has passed.

Article 20 (security control measures) requires BHPIs to adopt measures necessary and appropriate for preventing the unauthorised disclosure, loss or destruction of personal data. The FSA, Servicer, Telecommunications, Employment and METI Guidelines, and the guidelines published by the Ministry of Finance (the Finance Guidelines), list requirements for the improvement of internal security systems.

Article 21 (supervision of employees) obliges BHPIs to provide the requisite level of supervision to any employee handling personal data to ensure the security of the information handled.

To protect data held for employment purposes (under both articles 20 and 21) the Employment Guidelines provide that BHPIs must take steps to:

- clarify which employee handles personal data and make clear the authority of that employee;
- ensure that the personal data is used only by the authorised employee and only to the extent necessary for the execution of his duties;
- ensure that personal data obtained in the course of the authorised employee's duties is not leaked to third parties or used for improper purposes (this also applies after the employee has completed his duties);
- appoint a person with appropriate knowledge and experience to manage the personal data; and

- make this person and any other employees engaged in handling personal data aware of the importance of their responsibilities, and implement training programmes to make such employees fully conversant with the requisite procedures involved.

Article 22 (supervision of parties entrusted with information) obliges BHPIs that have entrusted personal data, in whole or in part, to a third party, to monitor that third party appropriately and to the extent necessary to ensure the safe administration of the information. The FSA, Servicer, Telecommunications, Employment and Finance Guidelines provide that BHPIs must enter into specified contractual arrangements to ensure supervision is correctly carried out. The METI Guidelines in particular make detailed provisions, recommending that parties engaged in entrusting information to other parties should make contractual arrangements covering the following:

- the responsibilities of the entrusting and entrusted parties;
- the safe maintenance of personal data;
- the return of personal data following completion of the purpose for which it was obtained;
- the content and frequency of reports on the state of use of personal data;
- confirmation that contractual obligations are being observed (such as the right to check the security of the data entrusted);
- sanctions in the event the contract is breached; and
- communication arrangements in the event that data security is breached.

Article 23 (restrictions on the provision of information to third parties) provides that, as a general rule, BHPIs cannot release personal data to a third party without the consent of the individual concerned. This is a key rule within the Act. The general prohibition does not apply where disclosure is:

- required or permitted by Japanese law;
- necessary to preserve life, safety or wealth, and it is difficult to obtain the individual's consent;
- necessary to improve public health or the sound upbringing of children and it is difficult to obtain the individual's consent; or
- required of a business by a government body where obtaining consent of the individual concerned might impede the execution of government business.

As an exception to this general prohibition, article 23 provides that BHPIs can release personal data to a third party if they cease such provision upon the request of the individual concerned. This also applies if the following information is given in advance to the individual concerned, or he is placed in a position where he could readily find out about it (the Opt-out System):

- the fact that the purpose of use shall be the provision of personal data to a third party;
- the content of the personal data;
- the means by which the personal data will be provided to the third party; and
- the fact that the provision of personal data to a third party will cease at the request of the individual concerned.

A BHPI which intends to change the content of the personal data provided, or the means by which it will be provided to a third party, must give advance notice to the individual concerned or place him in a position where he could readily find out about the change.

The general restriction on the provision of personal data to third parties does not apply where information is provided to a person/entity who is not considered a third party because the personal data is:

- entrusted to another person/entity to the extent necessary to achieve the purpose of use of that personal data;
- provided to another company in accordance with succession to business operations for reasons such as a merger; or
- used jointly with a specified person/entity and the individual concerned is notified in advance or placed in a position where he can readily learn of this fact and of the items of personal data to be used jointly, the range of joint users, the purpose for which the personal data will be used and the name or title of the person responsible for the management of that personal data.

The Employment Guidelines provide that where employment information is provided to third parties, BHPIs should:

- ensure it is not leaked or used for improper purposes;
- ensure that third parties obtain advance written approval from the BHPI for personal data to be provided to another third party. This does not apply to the matters excepted under article 23;
- clarify the length of time that the personal data will be held by the party receiving it;

- clarify that the personal data will be returned, destroyed or deleted by the party receiving it when the purpose of use has been achieved; and
- prohibit the copying or duplication of personal data by the party receiving it (unless necessary to create a back-up copy).

Finally, if a BHPI changes the purpose of use of information used jointly with a specified person/entity, or if the name or title of the person responsible for the management of personal data changes, the BHPI must notify the individual concerned in advance or place him in a position where he can readily learn of the change.

Held personal data provisions

Article 24 (public announcement of held personal data) obliges BHPIs to place the individual concerned in a position where he can readily learn of:

- the name or title of the relevant BHPI;
- the purpose of use of all held personal data, with limited exceptions where there is a fear of endangering the life, safety, property, rights or welfare of the individual concerned or the rights or profits of the BHPI, or co-operation is required with the execution of a government operation;
- procedures for responding to certain requests made by the individual concerned; and
- matters specified by government decree to secure the correct handling of held personal data, such as the complaints procedure.

Article 24 also provides that if the individual concerned asks a BHPI to provide notification of the purpose of use of held personal data identifying him, it must provide it without delay. This obligation does not apply where:

- the purpose of use of the held personal data has already been made clear; or
- there is a fear of endangering the life, safety, property, rights or welfare of the individual concerned or the rights or profits of the BHPI, or co-operation is required with the execution of a government operation.

Finally, article 24 provides that where a BHPI decides not to respond to a request to provide notification of the purpose of use of held personal data to the individual concerned on the basis of either of these two exceptions, it must inform the individual without delay.

Article 25 (disclosure) provides that a BHPI must disclose held personal data in writing, or give notice that no such information is

held if that is the case, to the individual concerned upon that individual's request. However, such disclosure can be withheld where there is a fear that it might cause damage to the life, safety, property or other rights of the individual concerned or a third party, the execution of business operations of the BHPI or the violation of another law or ordinance. If disclosure is withheld on this basis, the BHPI must notify the individual concerned without delay.

In general, the Employment Guidelines recommend that BHPIs should pay attention to the following to ensure the appropriate handling of employment related held personal data. When:

- they are going to make a decision regarding the handling of the data, they should give advance notice to the labour union and carry out a consultation process; and
- they have made a decision regarding the handling of the data, they must inform workers.

Article 26 (corrections etc) provides that if an individual concerned asks a BHPI to correct, supplement or delete the content of held personal data on the basis that it is incorrect, the BHPI must give due consideration to the request and perform the correction if justified. The BHPI must notify the individual concerned of its decision without delay.

Article 27 (cessation of use etc) provides that if an individual concerned asks a BHPI to stop using or delete held personal data on the basis that it was handled in breach of the purpose of use of such information (article 16), or acquired by fraud or other unfair means (article 17), and the BHPI finds that there are grounds for this request, it must stop using or delete the data without delay to the extent necessary to correct the violation. This obligation does not apply where cessation of use or deletion would cause excessive expense or extreme difficulty and other substitute measures to protect the rights and welfare of the individual concerned are taken.

If a BHPI is asked to stop providing information to a third party on the basis that the provision is in violation of article 23 outlined above, and the BHPI finds that there are grounds for this request, it shall cease without delay. This does not apply if it would cause excessive expense or extreme difficulty and other substitute measures are taken to protect the rights and welfare of the individual concerned.

Article 28 (explanation of reasons) provides that a BHPI must use its best efforts to explain to the individual concerned the reason for its decision regarding the withholding of notification of the purpose of

use, disclosure, correction, cessation of use or deletion of held personal data.

Procedural requirements

Article 29 (procedures for responding to requests for disclosure etc) provides that BHPIs may set up procedures by which individuals concerned can request notification of the purpose of use, disclosure, correction, cessation of use or deletion of held personal data. The FSA Guidelines provide that disclosure should be made, among other things, through the company's homepage or the information desk at the company's office. The Servicer Guidelines provide that procedures should be set up internally to ensure that disclosure can be made in a timely manner, and the Employment Guidelines recommend that BHPIs should set up a reading area so that requests for disclosure can be met quickly and conveniently.

Article 30 (processing fees) gives BHPIs the right to charge a reasonable processing fee for a request for notification of the purpose of use (article 24) or disclosure (article 25).

Article 31 (processing of complaints) provides that BHPIs must process complaints on the handling of personal information appropriately and promptly on a best efforts basis, and establish a system for this purpose. The Employment, METI, Telecommunications, Servicer and FSA Guidelines recommend that BHPIs set up processes to facilitate the timely and appropriate handling of complaints.

Sanctions and enforcement

Article 34 provides that a competent minister can, to protect individual rights or welfare, and where there has been a breach of articles 16-18, 20-27 or 30, recommend to the BHPI in question that it take appropriate steps to correct the breach. If the recommendation is not followed and there is a threat of impeding an individual's material interests, the competent minister can order the BHPI to comply with the recommendation. Further, if there has been a breach of articles 16, 17, 20-22 or 23 paragraph 1, and if the measures are urgently required, a competent minister may order the BHPI to cease the violative conduct or to take other necessary measures to correct the violation. Under article 56, a person in breach of such an order shall be liable to imprisonment for up to six months or a fine of not more than 300,000 yen. Under article 58, a company shall also be liable for a fine of not more than 300,000 yen when its representative, agent, employee or any other person engaged has breached such order in the course of its business.

It should be noted that even if an action such as the provision of personal data to a third party is lawful under the Act, it still might be

challenged as defamatory or as an infringement of the privacy of the individual concerned.

Article 37 provides that the competent government minister may appoint certain entities to ensure that BHPIs handle personal information appropriately by, for example, resolving complaints regarding its handling or by providing information that contributes to its appropriate handling. These entities are known as approved personal information protection organisations (APIPOs). Under article 41, BHPIs can consent to becoming a subject business of an APIPO, and the APIPO must publicly announce the names of its subject BHPIs so that individuals concerned can easily find out which APIPO they should complain to. Under article 42, on receiving a complaint from an individual who is the subject of personal information held by a BHPI, APIPOs can request an explanation from the BHPI in question so they can investigate and pursue the prompt resolution of the matter.

Reporting

Article 32 provides that a competent minister may require a BHPI to report on the handling of personal information to the extent necessary for enforcement. Under article 57, failure to provide such a report, or the filing of a false report, shall attract a fine of not more than 300,000 yen. Under article 58, a company shall also be liable for a fine of not more than 300,000 yen when its representative, agent, employee or any other person engaged has failed to provide such report or filed a false report in the course of its business.

Announcement of a privacy policy

The FSA and the Telecommunications Guidelines require BHPIs to publish a privacy policy to announce matters referred to under several of the provisions mentioned above. It is envisaged that consumers sensitive to the preservation of their privacy will judge BHPIs, in part, on whether they keep the promises made in their policy statement.

Potential implications and the future

International experience suggests that a number of areas covered by the Act might be developed further in the future.

Enforcement under the Act falls to the ‘competent ministers’ of the relevant government authorities. This system might provide added flexibility, with the competent ministers overseeing their own specialist industry, but the Japanese government might be challenged to ensure properly co-ordinated regulation, with each competent authority being limited to its own industry. Also, other than the limited information seeking powers afforded to APIPOs under article 42, the Act does not provide individuals with a mechanism to personally seek redress. The Act merely gives the minister discretion to admonish BHPIs in breach of the Act, with a subsequent power to order such BHPIs to cease the prohibited conduct.

The Act itself makes no distinction, as is common in some countries, between ordinary and sensitive information. However, the various guidelines make provisions for sensitive information in their own areas. The FSA, Servicer and Telecommunications Guidelines provide that, subject to limited public interest exceptions, BHPIs should take particular care to ensure that sensitive information, such as information relevant to ethnicity, nationality or religion, is not acquired, used or provided to third parties. Given the importance of confidentiality regarding sensitive information, it will be interesting to see if this piecemeal approach to regulation is effective in practice.

Implications for M&A

The restriction on the provision of personal data to third parties (article 23) might be problematic in the context of M&A, where the buyer performs detailed due diligence on its target company to establish any underlying liabilities in the valuation process. As set out above, article 23 establishes a general prohibition on the provision of personal data to third parties without the consent of the individual concerned. In practice, in the majority of cases it seems highly unlikely that a target company could obtain the consent required from all the individuals concerned when it intends to disclose information on a large number of individuals in the due diligence process. Accordingly, the target may consider relying on the Opt-out System outlined above.

Given the confidential nature of many M&A transactions, the issue for the companies involved becomes the scope of the obligation on the target company to put the individuals concerned in a position where they can readily find out about the matters specified in the Opt-out System. While the exception for information provided to

the acquiring company in the context of a succession to business operations, such as a merger, would seem to solve this problem, the METI Guidelines clearly state that although providing personal data after a takeover falls within the exception, providing it to a third party in the process of pre-contractual negotiations (such as due-diligence) can bring the matter within the prohibition in article 23. Accordingly, to comply with the Act, the target company might consider blacking out personal data in its documents or withholding the disclosure of such information and providing the buyer with an alternative document prepared by itself that does not include personal data. Whatever option is used, it seems that the Act will require target companies to take a much more active role in the due diligence process.

Implications for finance transactions

Article 23 also has a potentially significant effect on corporations intending to raise funds by transferring receivables off balance sheet by way of a securitisation or other structured financing method. To address these concerns, the Cabinet Office and the Servicer Guidelines provide clarification that BHPIs can infer the consent of their debtors to the disclosure of personal data on the receivables to the assignee or potential assignees of the receivables, on the basis that such data is necessary for the management of the receivables by the assignee or potential assignees.

Implications for marketing

BHPIs must now inform consumers of the purpose to which their personal information will be put, and the information may not be used for purposes that are not 'reasonably related' to the original purpose without the consent of the individual concerned. It seems unlikely that marketing will be regarded as 'reasonably related' to the original purpose. If it is not, BHPIs will have to specify marketing as one of their original purposes for collecting personal information. While consumers now have the right to require companies to stop using held personal data for purposes other than those originally specified, it remains to be seen how consumers will react to attempts to use personal information for marketing purposes.

Implications for consumers

Most multinational companies operating in Japan already comply with US and/or EU regulatory requirements, but such companies will need to ensure that their Japanese websites give information on the purpose of use of personal information collected online, and the procedures the business has in place to ensure compliance with disclosure requests.

Implications for employees

The most significant impact of the Act on human resources practices might be the requirement to provide employees with information about how personal data is used, and the provisions giving employees rights in the way that their personal data is managed. Employers must ensure that information is only used for the specified purpose, 'reasonably related' purposes or exceptional purposes otherwise permitted by the Act. Employers must establish security control and supervision systems to protect information handled by its employees and procedures for disclosure to interested employees. Disclosure to third parties is prohibited without employee consent, a matter complicated by the ambiguity concerning the definition of third parties. However, personal data can be disclosed to outside contractors, enabling companies to use a sub-contracted administrator, such as a payroll processing company, subject to article 22 and the relevant guidelines.

Conclusion

The Act constitutes a paradigm shift in the regulation of personal information in Japan, providing as it does a single body of legal rules at the national level regulating the ways in which personal information can be acquired, managed and used. It will have a major impact on businesses active in Japan. Although strengthened by the media's ongoing activism and heightened consumer interest in protecting privacy in Japan, the Act does appear somewhat weakened by its want of an efficacious and predictable enforcement procedure. Effective enforcement is arguably the real challenge for the Japanese government in the wake of the Act coming into force; it is this issue more than any other that will determine the success or failure of the legislation in achieving its goal of effectively protecting personal privacy.

AMSTERDAM
Apollolaan 151
1077 AR Amsterdam
T + 31 20 485 7000
F + 31 20 485 7001

BARCELONA
Mestre Nicolau 19
08021 Barcelona
T + 34 93 363 7400
F + 34 93 419 7799

BEIJING
3705 China World Tower Two
1 Jianguomenwai Avenue
Beijing 100004
T + 86 10 6505 3448
F + 86 10 6505 7783

BERLIN
Potsdamer Platz 1
10785 Berlin
T + 49 30 20 28 36 00
F + 49 30 20 28 37 66

BRATISLAVA
Laurinská 12
81101 Bratislava
T + 421 2 5413 1121
F + 421 2 5413 1123

BRUSSELS
Bastion Tower
Place du Champ de
Mars/Marsveldplein 5
1050 Brussels
T + 32 2 504 7000
F + 32 2 504 7200

BUDAPEST
Oppenheim és Társai
Freshfields Bruckhaus
Deringer
1053 Budapest
Károlyi Mihály u. 12.
T + 36 1 486 22 00
F + 36 1 486 22 01

COLOGNE
Heumarkt 14
50667 Cologne
T + 49 221 20 50 70
F + 49 221 20 50 79 0

DÜSSELDORF
Feldmühleplatz 1
40545 Düsseldorf
T + 49 211 49 79 0
F + 49 211 49 79 10 3

Mailing address
Postfach 10 17 43
40008 Düsseldorf

FRANKFURT AM MAIN
Taunusanlage 11
60329 Frankfurt am Main
T + 49 69 27 30 80
F + 49 69 23 26 64

HAMBURG
Alsterarkaden 27
20354 Hamburg
T + 49 40 36 90 60
F + 49 40 36 90 61 55

Mailing address
Postfach 30 52 70
20316 Hamburg

HANOI
#05-01
International Centre
17 Ngo Quyen Street
Hanoi
T + 84 4 8247 422
F + 84 4 8268 300

HO CHI MINH CITY
#1108 Saigon Tower
29 Le Duan Boulevard
District 1
Ho Chi Minh City
T + 84 8 8226 680
F + 84 8 8226 690

HONG KONG
11th floor
Two Exchange Square
Hong Kong
T + 852 2846 3400
F + 852 2810 6192

LONDON
65 Fleet Street
London EC4Y 1HS
T + 44 20 7936 4000
F + 44 20 7832 7001

MADRID
Fortuny 6
28010 Madrid
T + 34 91 319 1024
F + 34 91 308 4636

MILAN
Via dei Giardini 7
20121 Milan
T + 39 02 625 301
F + 39 02 625 30800

MOSCOW
Kadashevskaya nab 14/2
119017 Moscow
T + 7 (501 or 095) 785 3000
F + 7 (501 or 095) 785 3001

MUNICH
Prannerstrasse 10
80333 Munich
T + 49 89 20 70 20
F + 49 89 20 70 21 00

NEW YORK
Freshfields Bruckhaus
Deringer LLP
520 Madison Avenue
34th floor
New York, NY 10022
T + 1 212 277 4000
F + 1 212 277 4001

PARIS
2 rue Paul Cézanne
75008 Paris
T + 33 1 44 56 44 56
F + 33 1 44 56 44 00

ROME
Piazza di Monte Citorio 115
00186 Rome
T + 39 06 695 331
F + 39 06 695 33800

SHANGHAI
34th floor
Jinmao Tower
88 Century Boulevard
Shanghai 200121
T + 86 21 5049 1118
F + 86 21 3878 0099

SINGAPORE
Freshfields Drew & Napier
20 Raffles Place #18-00
Ocean Towers
Singapore 048620
T + 65 6535 6211
F + 65 6533 5007

TOKYO
Ark Mori Building 18F
1-12-32 Akasaka
Minato-ku
Tokyo 107-6018
T + 81 3 3584 8500
F + 81 3 3584 8501

VIENNA
Seilergasse 16
1010 Vienna
T + 43 1 515 15 0
F + 43 1 512 63 94

WASHINGTON
Freshfields Bruckhaus
Deringer LLP
701 Pennsylvania Avenue, NW
Suite 600
Washington, DC 20004-2692
T + 1 202 777 4500
F + 1 202 777 4555

11704