EU-China Information Society Project

中国欧盟信息社会项目

EU-China Personal Data Protection:

Questions and Answers

中欧个人信息保护：问题及答案

Graham Sutton /格雷汉姆•萨顿
The Constitution Unit, University College, London
英国伦敦大学学院宪法组 • 伦敦

Qi Aimin / 齐爱民
The faculty of law, Chongqing Universtiy,Chongqing
重庆大学法学院 • 重庆

The report was conducted for the
EU-China Information Society Project
(supervised by Dr. Thomas Hart)

由中国-欧盟信息社会项目

法规专家 Thomas Hart 先生指导修订

December 2008
2008 年 12 月

The first part of this paper includes the English version of the report. The Chinese Version appears in the second part.

此报告第一部分为英文，第二部分为中文

The EU-China Information Society project is a joint initiative between the Chinese Government and the European Union. The project started in July 2005 and runs through to the end of June 2009. The project aims to promote economic and social development through Informatization and works closely with the former State Council Informatization Office (SCITO), now Ministry for Industry and Information Technology (MIIT) in China. For more information see www.eu-china-infso.org. For information on the regulatory activities within the project, contact Dr Thomas Hart at thart@eu-china-infso.org or Ms Su Li at suli@eu-china-infso.org.

中国—欧盟信息社会项目是中国政府和欧盟之间的合作项目。项目从 2005 年 7 月开始，到 2009 年 6 月结束。通过与前国务院信息化工作办公室（现已并入工业与信息化部）紧密合作，项目旨在通过信息化推动中国的经济和社会发展。更多详情，请浏览项目网站 www.eu-china-infso.org。有关项目法规对话部分的活动，请联系 Thomas Hart 博士，电子邮箱 thart@eu-china-infso.org 或者 suli@eu-china-infso.org。

Background to the Project

The EU-China Information Society Project was set up between the EU and the Chinese Government in mid-2005 to support informatization[1] in China. One of the Project's aims is to support the development of a regulatory framework for Information Society that provides for reliable investment, economic and social improvement and the maximization of benefits to Chinese citizens through the new opportunities that Information Society brings about.

The Project is designed to improve the process of knowledge exchange between European and Chinese experts and decision-makers in Information Society regulation. The Project supports Chinese government agencies working on their specific pieces of policy and legislation. While this aspect is driven by the needs and requirements of respective Chinese government agencies, the Project aims at the same time to improve European knowledge about Chinese approaches to Information Society regulation and to commonly approach new challenges that are brought about through social and technological change.

The aims of this research were to support the former State Council Informatization Office (SCITO), now the Ministry for Industry and Informatization (MIIT), in the drafting of a Personal Data Protection Law in China; to support MIIT in preparing for the implementation period of such a law; to provide EU experience relevant to establishing a regulatory environment that ensures reliable and safe commercial and private online activities; and to prepare government staff in data protection agencies involved in future implementation of the personal data protection law and acquiring the relevant skills.

On this report:

This report was prepared by EU expert Graham Sutton of The Constitution Unit, University College, London and Chinese expert Qi Aimin of the faculty of law, Chongqing Universtiy. The introduction to the respective EU approach was provided by the EU expert (x.1, x.2, x.3 of each section), the comment from Chinese perspective was provided by the Chinese expert (x.4 of each section). Recommendations were provided by both experts. If both EU and Chinese perspective come to the same conclusion, no further comment is added. If the EU perspective and Chinese perspective differ in focus, the respective perspective is mentioned, and recommendation have been formulated from both sides.

[1] Informatization in China's context is defined as the transformation of an economy and society driven by ICT, involving the process of investments in economic and social infrastructure to facilitate the use of ICT by government, industry, civil society and the general public. The long-term goal of informatization is to build an information society (source: Jim Adams, VP World Bank East Asia and Pacific Region)

FOREWORD

Each time we use our credit cards to purchase goods; whenever we make a call with our mobile phones; if we open and use a bank account or take out insurance; if we get a job, or join a school or university, or seek a service from a government body, or take a plane or cross an international border, we unavoidably reveal and allow others to record information about ourselves. If we wish to participate fully in our modern society, we cannot do otherwise. However, making available our personal information in this way exposes us to threats to our privacy. Moreover, in our increasingly globalised environment, in which information can be transferred world-wide at the touch of a computer key, the threat can come from any country. Others have access to information about our personal lives – sometimes quite intimate information – and could use it to our detriment.

In June 2007 the EU–China Information Society Project published its research report: "Personal Data Protection in Europe and China: What Lessons to be Learned?" Against the background of the legal infrastructure underpinning data protection in the EU and the legislation relating to the protection of privacy in China, that report considered and made recommendations about the general issues that could usefully be taken into consideration in the formulation in China of legislation to protect personal information.

The present report takes that earlier study forward by examining in more detail the approach followed within the EU to a number of specific data protection problems. Data protection is a wide-ranging and complex field of law. It is applicable to all organisations, within both the public and private sectors, that collect and use information about identifiable individuals. It can cover "old" technologies which involve paper-based records, as well as the most up to date forms of information and communication technologies, including the on-line world. It applies to images and sounds as well as to text. This report is not intended – nor could it realistically aspire – to deal with the myriad questions that could be raised in the minds of legislators as they start to think about the issues involved. Rather, it responds to a number of specific questions that have been identified in the discussions between the EU and Chinese experts and government officials as likely to be of particular importance to the law-makers in China.

As well as the objectives, range and substantive content of data protection law, it considers the application of the data protection rules to particular sectors. In relation to each of the issues, it looks first at the provision made by the EU Data Protection Directive (and in some cases other international instruments). It then goes on to consider how the individual EU Member States have dealt with these issues in their national data protection laws. No one country has a monopoly of wisdom or experience, and the report gives examples drawn from the laws of many Member States. The report includes comments and recommendations on each issue from both the EU and the Chinese perspectives.

In October 2008, at their 30th international conference in Strasbourg in France, the data protection supervisory authorities from around the world stressed the need for binding data protection rules in a globalised world. Without such international rules for all players, they said in their closing press release, it will not be possible to tackle the privacy challenges of the future. In identifying how some of the data protection challenges have been addressed in the EU, it is hoped that the present report will help China in considering how to respond to the international privacy concern voiced by the data protection commissioners.

1 The object of data protection laws

1.1 The Directive

The EU Data Protection Directive (95/46/EC), as a measure designed to enhance the effectiveness of the EU's single market, requires individuals' information privacy to be protected while at the same time permitting the free flow of personal data within the single market.

> *Article 1: Object of the Directive*
>
> 1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
>
> 2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1."

1.2 Member States' laws

Some, but not all, of the data protection laws of the EU Member States specify the object of the laws early on. Where they do so, the laws most frequently make a simple statement to the broad effect that the object is to protect individuals' personal data or information privacy. The second element in Article 1 of the Directive, (ie the requirement not to restrict the free follow of personal data) is not generally mentioned. For example, section 1(1) of the Federal German law says:

> "The purpose of this Act is to protect the individual against his right to privacy being impaired through the handling of his personal data".[2]

Article 1 of the Greek law says:

[2] The quotations in English from legal texts whose original is in another language are taken from unofficial translations and should not be regarded as providing a definitive statement of the law. Only the original language texts in the form officially approved by the country in question can do this.

> "The object of this law is to establish the terms and conditions under which the processing of personal data is to be carried out so as to protect the fundamental rights and freedoms of natural persons and in particular their right to privacy."

Section 1 of the Swedish law introduces a slightly different concept, that of "personal integrity":

> "The purpose of this Act is to protect people against the violation of their personal integrity by processing of personal data."

Section 1 of the Finnish law goes a little further:

> "The objectives of this Act are to implement, in the processing of personal data, the protection of private life and the other basic rights which safeguard the right to privacy, as well as to promote the development of and compliance with good processing practice."

Finally it is worth mentioning the French law which adopts an altogether different approach by setting out in Article 1 the function and limitations of information technology. However, in so far as personal data processing and hence data protection depend upon information technology, this article with its reference to international co-operation perhaps comes closest to dealing with the two limbs of Article 1 of the Directive.

> "Information technology should be at the service of every citizen. Its development shall take place in the context of international co-operation. It shall not violate human identity, human rights, privacy, or individual or public liberties."

1.3 Comment from the EU perspective

Article 1 of the Directive establishes that data protection is about finding a balance. It says that the balance is between protecting human rights, and in particular information privacy, on the one hand, and allowing the free flow of personal data between the EU Member States on the other. That is clearly one important objective. However, in practice a broader balance needs to be struck. Complex modern societies increasingly depend upon the use of personal data, in both the public sector and the private sector, to provide the services and facilities that citizens need. It is not the function of data protection to stop organizations using personal data where the uses are legitimate. Its role is, rather, to provide a regulatory framework in which information about individuals is used properly and responsibly. The broader balance is, therefore, between organizations' legitimate uses of personal data (which would include but not be limited to the transfer of personal data across national boundaries), and individuals' right to have those data handled with due respect for their information privacy.

1.4 Comment from the Chinese perspective

Neither the broader nor the narrower balance may need to be highlighted when it comes to China. In processing personal information, conflicting interests include but are not limited to organizations' legitimate uses of personal information, individuals' right to have that information handled with due respect for their information privacy, fundamental rights and freedoms of natural persons, and the free flow of personal information between States. All the interests cannot be concluded by "organizations' legitimate uses of personal information" and "individuals' right". A good case in point is the status of consumers. If the "broader" balance is struck, these interests will be ignored.

As regards the object of legislation, it may as well be for legislators to take the traditional path. In accordance with the traditional rule in Chinese legislation, various social interests should be identified and protected by legislators. When interests conflict, compromises will be applied. Take, for example, the case of the announcer giving out the list of names of runners in an athletics competition. The rights of the runners will be restricted in that the athletics competition is related to the national interest.

Recommendation:
In developing data protection legislation and laying out rules regulating specific areas such as consumption, journalism and electronic commerce, legislators in China should have regard to this broader balance.

2 The way to define “personal data”: generalization or enumeration

2.1 The Directive

The Directive’s definition of “personal data” is found in Article 2(a):

> “ “personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.

This definition is elaborated upon in recital (26):

> “Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; ….”

Recital (14) which deals with sound and image data is also relevant:

> “Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data”.

2.2 Member States’ laws

Many Member States’ laws simply reproduce the definition from the Directive, either as it stands or with small amendments. Article 6 of the Polish law, for example, specifies that identification of the data subject should not require excessive resources.

> “1. Within the meaning of the Act personal data shall mean any information relating to an identified or identifiable natural person.
> 2. An identifiable person is the one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors

specific to his/her physical, physiological, mental, economic, cultural or social identity.
3. A piece of information shall not be regarded as identifying where the identification requires an unreasonable amount of time, cost and manpower."

On the other hand, Article 2 of the French law says that the means used to identify individuals are very broad:

> "Personal data means any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him. In order to determine whether a person is identifiable, all the means that the data controller or any other person uses or may have access to should be taken into consideration."

Several Member States' laws take only the first part of the definition, and do not include the list of factors permitting identification. For example, Article 1 of the Dutch law says:

> "a. "personal data" shall mean: any information relating to an identified or identifiable natural person."

Some laws are more specific about the type of information that is included within the definition. For example, Section 3 of the German law says that it is limited to "personal and material circumstances":

> (1) "Personal data" means any information concerning the personal or material circumstances of an identified or identifiable individual (the data subject)".

Section 1(1) of the law of the United Kingdom specifies that it is the data controller who must be capable of identifying the data subject from information that he has or is likely to obtain:

> ""personal data" means data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual".

Like a number of other Member States' laws, the United Kingdom law makes clear that the law applies only to "living individuals". The references to opinions about and intentions towards the data subjects are included to make clear that "soft" information of this kind is included within the definition.

2.3 Comment from the EU perspective

As this question suggests, there are two broad approaches to defining what constitutes "personal data": generalization or enumeration. The Directive, along with other international instruments such as the Council of Europe Data Protection Convention and

the OECD Data Protection Guidelines, follows the first approach. Its starting point is that where an individual has been, or can be, identified, any information relating to that individual constitutes “personal data”.

While this approach has long been established as the European data protection norm, experience has shown that it is not without problems. One of the main ones, which is illustrated in the examples of Member States’ Laws given above, relates to the meaning of “identifiable”. Everybody is identifiable by somebody .How far is it necessary to go in order to relate a particular piece of information to a specific individual? If a business has a digitized picture of an individual whom the business cannot identify does that picture constitute personal data of which the business is the data controller? The individual’s family or friends will be able to identify him. Is that sufficient to make the individual “identifiable” for the purposes of the legislation? The Directive helps only to the extent of making clear that information comprising sounds and images can come within the scope of the definition.

Another problem lies with the words “relating to”. Again, it is unclear what their precise scope is. The German law seeks to give more precision by specifying that only the individual’s “personal or material circumstances” come within the scope of the definition. On the other hand, the definition in the UK law spells out that opinions and intentions affecting the individual are covered.

Because of these difficulties, and the central importance of the definition of “personal data” to determining the scope of data protection law and hence the consistency of application of the Directive among the Member States, in June 2007 the Article 29 Working Party of EU Data Protection Commissioners adopted a paper discussing and giving guidance on the meaning of the term. The paper looks at each of what it calls the four “building blocks” of the definition: “any information”; “relating to”; “identified or identifiable”; “natural person”; and with extensive use of examples gives the Working Party’s interpretation of their meaning. It thus helps to establish a consensus on this difficult issue. The paper can be viewed at:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

The alternative approach would be to list those categories of information which, when linked to an individual, are deemed to be “personal data” and thus subject to protection. Categories not listed would not be “personal data” and would thus be outside the scope of the law. To the extent that it would clarify what information was, and what information was not, covered by the law, this approach could seem attractive. However, it would not remove all the problems associated with the current EU definition, since it would still be necessary to link the information to an identifiable individual. Moreover, this approach would probably be less protective of individuals’ information privacy. The strength of the approach – that it is more specific and therefore clearer – is also its weakness. It would presumably be necessary to produce a list of the information covered, and legislating by means of lists is notoriously unreliable since it is very easy to overlook things that should be included.

2.4 Comment from the Chinese perspective

As two sides of the same coin, merits and drawbacks coexist in both ways of defining "personal data": generalisation and enumeration. The adoption of the way of generalization makes the statute more explicit on the one hand, but adding detailed expertise makes the term more difficult to understand.

A good case in point is the term "identifiable" in this context: everybody is identifiable by somebody. The same thing can be said about the method of enumeration. By this way the statute will be clearer and can be better understood by readers. It has drawbacks, however: The statute is bound to be excessively lengthy, and it is a waste of legislative resource; for another, any information not mentioned in the statute will not be protected by law.

Recommendation (EU Perspective): China should adopt a "generalized" definition of "personal data", having regard to the guidance in the Article 29 Working Party paper.

Recommendation (CH Perspective): The advisable way for China is to combine the way of generalization and enumeration. Thus the statute will be both explicit and inclusive. Moreover, the latest information such as the address of DNS that can identify individuals can be included. The definition in Article 2 of the Directive can be adopted by Chinese legislation. In order to make some terms such as "identified", "identifiable" and "information subject" much easier to be understand, the supreme court in China should lay out relevant explanatory statutes.

Sensitive information should be identified and protected in a special way, because this kind of information is much more important to individuals. Compared to non-sensitive personal information, the processing and protecting of it is therefore much more demanding. And in China, legislators have already been advised to give special attention and protection to sensitive information.

3 Should data protection law apply to data controllers in both the public and private sectors?

3.1 The Directive

The Directive applies to the processing of personal data in both the public sector and the private sector. However, it does not apply to activities which fall outside the scope of Community law. The only other exception is for processing of a purely personal nature carried out by individuals.

> "Article 3.2
>
> This Directive shall not apply to the processing of personal data:
>
> - in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law;
>
> - by a natural person in the course of a purely personal or household activity."

The EU are considering proposals for a new legal instrument which would apply data protection rules to some of the activities which fall outside the scope of Community law.
The draft proposal as first brought forward by the European Commission can be viewed at:
http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0475en01.pdf

3.2 Member States' laws

All Member States' laws apply to both the public and private sectors, to the extent required by the Directive. Most, if not all, Member States' laws also apply to those activities which are excluded from the scope of the Directive because they are outside the scope of Community law. However, the laws contain exemptions necessary to protect important public interests. These exemptions are considered later in this paper. Some Member

States' laws differentiate between the public and the private sectors. These differences are also considered later in this paper.

3.3 Comment from the EU perspective

Risks to individuals' information privacy that come from the processing of personal data exist irrespective of the sector in which the processing is carried out. The risks are inherent in the fact that personal data are collected, recorded and used. Wrong decisions and handling errors can be made just as easily in the private sector as in the public sector, with equally harmful consequences for the individuals concerned. Moreover, the distinction between the public and private sectors is becoming blurred, as some State functions are either transferred or contracted out to the private sector. There is often a need for personal data to be shared between private sector and public sector bodies. It would be self-defeating for an individual's personal data to be given legal protection while they were being processed within one sector, but for those same data to forfeit all protection the moment they were passed to the other sector. A data protection regime which provided for this would be both difficult to justify in theory and ineffective in practice.

3.4 Comment from the Chinese perspective

As to the sphere of effect of the personal information law, applying the law to both the private and public sectors is relevant to China to some extent. In the EU personal information law is applied to both public and private sectors. However, the different conditions of China and the EU member states cannot be overlooked. In the former, the power of the public sector is much stronger than that of the private sector. In the processing of personal information, administrative and judicial power is constantly applied. Under these circumstances, individuals' rights risk being infringed much more severely without special restrictions in the public sector. In this sense, the public sector requires special regulation.

Recommendation (EU Perspective): China should apply its data protection law to both the private and public sectors.
Recommendation (CH Perspective): In China the rules can be applied to both public and private sectors in principle, but some of the former should take more obligations, and the procedure for them must be stricter.

4 Automatic and manual data processing

4.1 The Directive

The Directive applies both to the automatic processing of personal data and to some processing of personal data held in manual form. Article 3.1 of the Directive says:

> "This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system".

Article 2(c) defines "filing system:

> ""personal data filing system" ("filing system") shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis".

These provisions need to be read with Recital (27) which gives more detail on the meaning of "filing system":

> " (27) Whereas the protection of individuals must apply as much to automatic processing of data as to manual processing; whereas the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention; whereas, nonetheless, as regards manual processing, this Directive covers only filing systems, not unstructured files; whereas, in particular, the content of a filing system must be structured according to specific criteria relating to individuals allowing easy access to the personal data; whereas, in line with the definition in Article 2(c), the different criteria for determining the constituents of a structured set of personal data, and the different criteria governing access to such a set may be laid down in each Member State; whereas files or sets of files as well as their cover pages, which are not structured according to specific criteria, shall under no circumstances fall within the scope of this Directive".

4.2 Member States' laws

In order to define those categories of manual records to which they apply, most Member States' laws broadly follow the definition in Article 2(c) the Directive, often with some minor variations and in some cases omitting that part of the definition which deals with the centralization or otherwise of the filing system.

The definition in Article 3(3) of the Finnish law takes a different approach. It applies to both automatically processed and manually processed data, and, for manual files, requires the information they contain to be easy and inexpensive to retrieve, thus limiting its scope:

> "(3) *personal data file* means a set of personal data, connected by a common use and processed fully or partially automatically or sorted into a card index, directory or other manually accessible form so that the data pertaining to a given person can be retrieved easily and at reasonable cost".

The detailed definition in Article 4 (1)(g) of the Slovakian law also applies to both automatic and manual processing and, like the Finnish definition, contains an illustrative list of the sorts of manual systems that are covered. Unlike the Finnish definition, its scope is very wide:

> "g) filing system shall mean any structured set, system or database containing one or more personal data, which are systematically processed for the needs of achieving the purpose according to specific criteria and conditions, while using automated, partially automated or other than automated means of processing, disregarding the fact whether the system is centralised, decentralized or dispersed on a functional or geographical basis, e.g. card index, list, register, file, record or a system containing files, documents, contracts, certificates, references, assessments, tests".

The much briefer definition in Article 3(b) of the Spanish law achieves similarly comprehensive coverage:

> "b) File: any structured set of personal data, whatever the form or method of its creation, storage, organisation and access".

On the other hand, the definition in Article 1(1) of the United Kingdom law, which is similar to that in the Irish law, is intentionally much more restrictive in its scope:

> " "relevant filing system" means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily available".

4.3 Comment from the EU perspective

The main driver for the introduction of data protection laws in Europe in the 1970s was the proliferation of powerful computers which could manipulate personal information easily and quickly. Information about people had always been collected by Governments and businesses, but, with some exceptions, of which medical confidentiality is perhaps the most notable, little attention had been paid to the risks to personal privacy to which the

improper use or disclosure of that information could give rise. Certainly, despite the fact that Article 8 of the European Convention on Human Rights had provided, since 1950, for the right to private life, there had been no systematic process of legislating for the protection of personal information held in manual form. Manual systems are, compared with computerized systems, cumbersome and slow, and any risks were, and by many still are, perceived to be proportionately low.

The first European international instrument to deal with data protection, the 1981 Council of Europe Data Protection Convention, is expressly limited to the automated processing of personal data. Parties to the Convention are given the discretion whether or not to apply the Convention's rules also to manually held records. Some countries chose to do so, others did not. One reason for not doing so were the practical difficulties and cost of applying the rules to manual records.

The main reason for applying data protection rules to manually held records as well as to automated processing is given in Recital (27) of the Directive, quoted above. It is the risk of circumvention. If data protection rules apply only to automatic processing, organisations which, for whatever reason, wish not to be subject to the rules, have only to hold their records containing personal information in manual form for them to be exempt.

The risk is undoubtedly a real one, although how great it is must be open to question. Even in 1995, when the Directive was adopted, legitimate questions were raised about the likelihood of organizations choosing to use outdated information handling processes in order to circumvent the Directive, given the sophisticated technology that was already available. Information and communications technologies have developed immeasurably since then and the likelihood of organizations choosing to forfeit the real gains to be achieved by using them in order to avoid having to comply with data protection rules must be slight.

On the other hand, that argument can be turned on its head. The amount of non-automatic processing that is done nowadays is small and getting smaller. Any practical difficulties and cost to organizations that would flow from requiring the rules to be applied to manual processing would, therefore also be small and diminish proportionately. There is, therefore, little reason of practicality not to apply the rules to manual processing, especially when it is clearly morally right for organizations to apply the same standards of protection to all the personal information they hold and use irrespective of the medium in which it is held.

Deciding that the rules should be applied to manual records is one thing. Finding the right formula for defining those records to which the rules are to apply is quite another. It is significant that the Directive does not apply to all personal information held in non-automated form. It applies only to those sets of records which have a structure which permits the ready identification and retrieval of selected information. In other words, it applies to manual collections of personal information which can be manipulated, to some extent, in the same way as automated information can be manipulated, albeit more laboriously. This ability to manipulate the data is crucial, since it would be wholly impractical to require the data protection rules to be applied to incidental pieces of personal information held, for example, on isolated pieces of paper or in unstructured notebooks. A clear example of the sort of records that could be caught is the traditional card-index system comprising a set of cards each of which contains the same categories of information about a named individual, and with the cards arranged in alphabetical order

of the individuals' names. Other collections of personal information held in different forms but where the collections are structured in a similar way could also be caught. An example would be a collection of loose-leaf folders, each of which contains the same categories of specific information about a particular individual, with the individual's name on the cover, and where the collection is held in alphabetical order of the individuals' names.

4.4 Comment from the Chinese perspective

The processing of personal information by manual means still extensively occurs in China, especially in the west region and the countryside. Therefore manual processing can by no means be ignored by Chinese legislators. In legislation, the manual and automatic processing of personal information must have the same attention of Chinese legislators. However, considering the different level of risks individuals may encounter as between manual and automatic processing, the regulations concerning the two ways should differ. That is, the obligations imposed on manual processing should be fewer than those imposed on automatic processing. Besides, before automatic processing the individuals should explicitly agree with the act, which is not necessarily the case in manual processing.

Recommendation: China should apply its data protection law to those manual records which are structured in such a way as to permit ready the ready access to and retrieval of specific information about particular individuals. However, the rules that apply to the processing of manual records should be fewer than those that apply to automatic processing. The manual records that are caught by the law term will not necessarily need a separate definition, since "personal information" should be defined as the information that can be retrieved in the first chapter of the Chinese law.

5 What kinds of personal data can be public and open data (such as address and telephone number)?

5.1 The Directive

The Directive does not recognize any category of personal data as being "public and open". If information constitutes personal data, it is subject to the requirements of the Directive.

5.2 Member States' laws

The same applies to Member States' laws.

5.3 Comment from the EU perspective

It is by intention, not oversight, that there is no category of personal data that is considered to be "public and open". Even personal data that are frequently disclosed to others, such as addresses and telephone numbers, can be processed in such a way as to pose a threat to privacy. Many individuals are content for their addresses and telephone numbers to be known to their intimate circle of family and friends, and to some outside that circle, such as their employers or those providing them with a service, but they are strongly opposed to the wider dissemination of that information.

The fact that there is no category of "public and open" personal data does not mean that personal data may not be published where publication is legitimate. Article 9 of the Directive requires Member States to provide exemptions from many (but not all) of the provisions in the Directive "…for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression". The clearest example of the sort of activity that this exemption permits is the publication of personal data in newspaper or magazine articles, or by the broadcasting media. But it would also permit such things as exhibitions of portraits or the publication of biographies.

In other cases, where the exemption provided by Article 9 of the Directive is not available (for example, the production of telephone directories) publication is still possible if the requirements of the data protection rules are met. This normally means having a lawful basis for processing (of which the consent of the data subject is one, but not the only, possibility) and ensuring that the data protection principles are complied with.

In the United Kingdom, for example, the register of individuals entitled to vote in elections is a public document. Each year, every household receives a form from the electoral authority seeking information about the people living in the household who are entitled to vote. One of the questions on the form asks whether the individuals concerned consent to their names and addresses being published in the electoral register. Two versions of the register are produced. One which has the names and addresses of all those entitled to vote, and the other which omits the names and addresses of people who have refused their consent. The former may be used only for electoral and other approved purposes. The latter is a public document which may be consulted by anybody and used for any purpose, the individuals' consent being the legal base for the disclosure of their personal data in this way.

It is a common misapprehension that personal data obtained from published sources, such as telephone directories or other public registers, are exempt from the data protection rules in any future use. That is not so. The data protection rules apply to personal data collected from such sources in exactly the same way as they apply to any other personal data. So, for example, a business that used the United Kingdom's publicly accessible electoral register to obtain the names and addresses of prospective customers for direct marketing purposes, would be obliged to respect the data protection rules in processing those personal data for such purposes.

5.4 Comment from the Chinese perspective

Undoubtedly all personal information, whether it is non-sensitive or sensitive relates to the personal interests of individuals, and even personal information that is frequently disclosed to others, such as addresses and telephone numbers, can be processed in such a way as to pose a threat to privacy. However, the degree of threat varies widely according to the degree of sensitivity of the information. For example, disseminating individuals' telephone numbers can do greater harm to individuals than stealing and disseminating certain other sorts of data.

On the other hand, processing even information such as telephone numbers needs to be allowed in principle if public interest is affected. Besides, in accordance with current law in China, even sensitive personal information can never be completely protected, not to mention low risk information. The idea of forbidding all the personal information to be public and open is impractical.

Recommendation (EU-Perspective): There is no need for the Chinese law to identify special categories of personal data as “public and open”. The desired degree of openness can be achieved within the data protection rules.
Recommendation (CH-Perspective): The Chinese legislators should settle this issue in two ways in accordance with the principle of public interest protection, by making public the information related to public interests on the one hand, and forbidding making other information in public on the other hand. To implement the advice, the law may provide that: “All the personal information, no matter sensitive or low risk, fall into the object of the personal right. Unless the law otherwise provides (such as that personal information processing is related to public interests), all the personal information can not be processed without the permission of individuals.”

6 How many data protection principles are there in the rules of other countries and international organizations? Are there any material differences?

6.1 International Instruments

6.1.1 The Directive

Within Europe, the expression "data protection principles" has come to have a precise meaning[3]. Rather than describing all the data protection rules, it is used to refer to a sub-set: those provisions which regulate the collection, subsequent processing and quality of personal data. They are found in Article 6 of the Directive:

> "1. Member States shall provide that personal data must be:
>
> (a) processed fairly and lawfully;
> (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
> (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

[3] In this paper the term "data protection principles" is used with this meaning, unless otherwise specified.

2. It shall be for the controller to ensure that paragraph 1 is complied with."

These principles are at the heart of the data protection rules, but they need to be complemented by other provisions. The Directive contains the following additional main elements:

- provisions setting out acceptable legal bases for processing personal data (Articles 7 and 8)
- a requirement for individuals to be informed of the processing of their personal data (Articles 10 and 11);
- a requirement for individuals to be able to gain access to their personal data and to have them corrected or erased if necessary (Article 12);
- a requirement for appropriate security (Article 17);
- a requirement for any person to be able to find out whether a particular organization is processing personal data (Article 21);
- provisions relating to enforcement (Articles 22 to 24);
- provisions regulating the transfer of personal data to third countries (Articles 25 and 26);
- a requirement for an independent supervisory authority (Article 28).

Some of these elements, as well as the provisions found in Article 6 of the Directive, are referred to as "Principles" in some other international instruments and some national laws.

6.1.2 Council of Europe Convention

Article 5 of the Convention served as the model for Article 6 of the Directive, which elaborated upon it:

"Personal data undergoing automatic processing shall be:
a. obtained and processed fairly and lawfully;
b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
c. adequate, relevant and not excessive in relation to the purposes for which they are stored;
d. accurate and, where necessary, kept up to date;
e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored."

Most of the key additional elements from the Directive described above are also found in the Convention or its Additional Protocol. The exceptions are the specification of possible legal bases for processing, and an express requirement for individuals to be informed of the collection and further processing of their personal data. Making the individuals concerned aware of what is happening to their personal data is considered to be a necessary ingredient of fairness, and it is thus covered by the first data protection principle (Article 5.a of the Convention).

6.1.3 OECD Guidelines

Part Two of the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data is headed “Basic Principles of national Application” and contains paragraphs dealing with the following principles, whose content is summarised:

Collection Limitation Principle

The amount of personal data collected should be limited, and collection should be fair and lawful, and individuals should be informed.

Data Quality Principle

Personal data should be relevant to the purpose of collection, and, to the extent necessary, accurate, complete and kept up to date.

Purpose Specification Principle

The purposes of personal data collection should be specified and the personal data should not to be used for incompatible purposes.

Use Limitation Purpose

Personal data should not be disclosed or used otherwise than in accordance with paragraph 9, except with the individual’s consent or by the authority of law.

Security Safeguards Principle

Personal data should be protected by reasonable security safeguards.

Openness Principle

Developments concerning personal data should be transparent. Anyone should be able to find out about the processing of personal data.

Individual Participation Principle

Individuals should be able to gain access to their personal data and to have them corrected or erased if necessary.

Accountability Principle

The controller should be accountable for complying with these measures.

Part Three of the Guidelines is headed: “Basic Principles of International Application: Free Flow and Legitimate Restrictions”. It encourages Member countries not to use data protection as an excuse for unnecessary restrictions on the transborder flows of personal data. Specifically it says that:

> "A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent domestic privacy legislation."

Provisions relating to the national implementation of the Guidelines are dealt with in Part Four of the Guidelines. Unlike the Directive (and the Additional Protocol to the Convention) the Guidelines do not require the establishment of a national supervisory authority. They simply call for Member countries, in implementing the Guidelines, to "establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data".

6.1.4 APEC Privacy Framework

The core provisions of this instrument are set out in Part iii which is headed "APEC information privacy principles". In summary, the principles are as follows:

I. Preventing Harm

Protection should be designed to protect misuse of personal information. Specific obligations should take account of the risk of harm and remedial measures should be proportionate to the likelihood and severity of harm.

II. Notice

Controllers should provide clear statements to individuals including information about the fact their personal information is collected and certain key additional information including opportunities for limiting disclosure and gaining access.

III. Collection Limitation

Personal information should be relevant to the purposes of collection. It should be obtained fairly and lawfully and, where appropriate, individuals should be informed or their consent should be sought.

IV. Uses of Personal Information

Personal information should be used only for the purpose for which it was collected and other compatible or related purposes except with the individual's consent, to provide a service requested by the individual, or by the authority of law.

V. Choice

Where appropriate, individuals should be provided with clear mechanisms to exercise choice as regards the collection, use and disclosure of their personal information.

VI. Integrity of Personal Information

Personal information should be accurate, complete and, where necessary, kept up to date.

VII. Security Safeguards

Personal information should be protected with appropriate safeguards

VIII. Access and Correction

Individuals should be able to gain access to their personal information and to have it corrected or erased if necessary.

IX. Accountability

The controller should be accountable for complying with these measures. Where personal information is transferred to another controller, whether domestically or internationally, the individual's consent should be obtained or the controller should take reasonable steps to ensure that the recipient will protect the information consistently with these Principles.

Part iv of the paper deals with national implementation. It recognizes that different approaches to implementation will be needed in different countries and allows wide flexibility. It makes no recommendation for a supervisory authority.

6.2 Member States' Laws

Most Member States' laws incorporate the data protection principles from Article 6 of the Directive in broadly the form in which they are set out in that article. Often they are included in a single article, or a group of articles, whose heading sometimes contains the word "principles" but also uses other terms such as "Conditions for lawful processing of personal data" (Cyprus) or "Characteristics of Personal Data" (Greece). In some Member States' laws, the provisions of Article 6 of the Directive are not grouped together but inserted at different points in the text. Two Member States' laws have no provisions clearly corresponding to the contents of Article 6 of the Directive, the required provision presumably being made elsewhere or in another form.

Some Member States' laws group the provisions transposing Article 6 of the Directive together with other provisions under a heading including the word "principles". This is the case, for example, with the Spanish law whose Title II is called "Principles of data protection" and includes, in addition to an article transposing Article 6 of the Directive called "Quality of the data", provisions dealing with informing the data subjects, consent, sensitive data, data security, the duty of secrecy, the communication of data, and access on behalf of third parties. Schedule 1 to the UK law which is called "The data Protection Principles" includes, in addition to provisions for Article 6 of the Directive, provisions dealing with the conditions for making processing lawful, information for data subjects, the

right of access, data security and the transfer of personal data to third countries.

Some Member States' laws make more precise certain of the provisions of Article 6 of the Directive. For example, Section 6 of the Finnish law, which deals with the definition of the purpose of processing, says:

> "It must be appropriate and justified to process personal data in the operations of the controller. The purpose of the processing of personal data, the regular sources of personal data and the regular recipients of recorded personal data shall be defined before the collection of the personal data intended to be recorded in the file or their organisation into a personal data file. The purpose of the processing shall be defined so that those operations of the controller in which the personal data are being processed are made clear."

Section 5 of the law of the Czech Republic expresses the provisions of Article 6 of the Directive as duties which fall on the data controller. Paragraph (1)(f) deals with the purposes for which personal data may be processed. Rather than allowing further processing for purposes which are compatible with the purpose for which the personal data were collected (which is what the Directive permits) it requires the data controller to:

> "process personal data only in accordance with the purpose for which the data were collected. Personal data may be processed for some other purpose only within the limits of the provisions of Article 3(6) *[which provides exemptions for matters of substantial public interest]* or if the data subject granted his consent herewith in advance."

The concept of "compatibility" is one of the most difficult in the data protection rules. There is little jurisprudence about it. Article 9.2 of the Dutch law addresses this by specifying factors that must be taken into account in deciding whether further processing is incompatible with the original purpose.

> "For the purposes of assessing whether processing is incompatible … the responsible party shall in any case take account of the following:
> a. the relationship between the purpose of the intended processing and the purpose for which the data have been obtained;
> b. the nature of the data concerned;
> c. the consequences of the intended processing for the data subject;
> d. the manner in which the data have been obtained, and
> e. the extent to which appropriate guarantees have been put in place with respect to the data subject."

6.3 Comment from the EU perspective

Shakespeare said: "That which we call a rose by any other name would smell as sweet." Whether they are called "principles" or described in some other way, the key elements of the substantive data protection rules (as opposed to those elements which relate to the arrangements for giving the substantive rules teeth) are essentially the same in all the four international instruments considered above. Rather than in their content, the significant

difference is in their form. The provisions of the Directive and the Council of Europe Convention are expressed as binding rules, which indeed they are, at least for the 27 Member States' of the European Union which have also adopted the Convention. The OECD and APEC instruments, on the other hand, are expressed as guidelines, which countries are able to choose whether to take up or not.

The language in the APEC instrument, in particular, differs from that in the two European instruments. For example the concept of "choice" does not figure in the (narrowly defined) data protection principles in the European instruments, but has an important place in the APEC Principles. Even here, though, this difference of language masks a broad similarity of effect. In some respects the APEC principles are more detailed than the data protection principles (as narrowly defined) in the European Instruments. An example is in Principle IV dealing with the uses of personal information. This gives more detail than does the equivalent European provision of the circumstances in which personal information collected for one purpose may be used for another purpose. But, as we have seen, some EU Member States' laws have also gone down this road. Such elaborations aside, the differences within the EU Member States' laws on this centrally important issue, are not such as to suggest that there are any significant weaknesses in the data protection principles as long established in the Directive and the Council of Europe Convention.

Although the international transfer of personal data is outside the data protection principles as set out in Article 6 of the Directive, this is an important element of the data protection rules and it is worth drawing attention to the difference in approach between the Directive on one hand, and the APEC instrument on the other. Subject to some exemptions, the Directive provides for a strict prohibition on the transfer of personal data to countries which do not provide an "adequate" level of data protection, and sets out elaborate arrangements for monitoring the application of this rule at the EU level. The APEC instrument deals with international transfers as part of what it calls the "Accountability" principle, and does not distinguish them from domestic transfers between one organization and another. The rule in the case of both international and domestic transfers is that the controller should either seek the consent of the individual concerned, or take "reasonable steps" to ensure that the recipient will protect the personal information consistently with the APEC Principles.

6.4 Comment from the Chinese perspective

Pursuant to the traditional rule of Chinese legislation, principles just work as guidelines in laying out and applying the rules which are the basis on which cases are judged. Unless loopholes exist, principles cannot be applied directly. Principles must embody the basic value criterion of personal information: that is to protect personal information rights and other related interests in this field, and to permit compromise when conflict occurs.

Recommendation (EU-Perspective): The data protection principles as set out in Article 5 of the Convention and Article 6 of the Directive are the core of the European model for data protection. They are broadly replicated in the OECD Guidelines and the APEC principles. They are an essential component for any future Chinese data protection law.

Recommendation (CH-Perspective): The principles of Chinese protection law should include:

1) Identification of rights principle, The individual's rights should be protected by law completely.
2) Limitation of rights principle. Due to important interests, the rights of the individual should be restricted proportionately.
3) Collection limitation principle. The amount of personal information collected should be limited, and collection should be fair and lawful, and individuals should be informed.
4) Information quality principle. Personal information should be relevant to the purpose of collection, and, to the extent necessary, accurate, complete and kept up to date.
5) Purpose specification principle. The purposes of personal information collection should be specified and the personal information should not to be used for incompatible purposes.
6) Use limitation principle**.** Personal information should not be disclosed or used except with the individual's consent or by the authority of law.
7) Security safeguards principle. Personal information should be protected by reasonable security safeguards.
8) Openness principle**.** Developments concerning personal information should be transparent. Anyone should be able to find out about the processing of personal information.
9) Individual participation principle. Individuals should be able to gain access to their personal information and to have them corrected or erased if necessary.
10) Accountability principle. The controller should be accountable for complying with these measures.

7 Should the rules be applied differently in the public and private sectors?

7.1 The Directive

The rules in the Directive, including the data protection principles in Article 6, apply in the same way to both the public sector and the private sector

7.2 Member States' laws

Almost all Member States' laws follow the approach in the Directive in having a single set of substantive data protection rules, including the data protection principles, that apply to both the public and private sectors. A few Member States' laws complement these general provisions with additional provisions that apply differentially to the public and private sectors.

7.2.1 Germany

The most significant exception to the approach of having a single set of substantive data protection rules is the German law.[4] The German federal law makes a clear distinction between the public and private sectors. Part I sets out those provisions of the law which apply to both public and private bodies. Many of these deal with procedural matters (such as registration, in- house data protection officials and the use of sub-contactors), specialist techniques (such as video-surveillance of public places) or aspects of compliance (such as compensation and data protection audit). However, some provisions deal with substantive data protection rules. They include:

- a requirement for data processing systems to use as little personal data as possible;
- the establishment of the individual's consent as a legal base for processing personal data;

[4] Germany is a federal country. Data protection laws exist at both the federal and provincial levels. The federal law applies to public bodies of the Federation and to private bodies. It also applies to public bodies of the provinces in two sets of circumstances: where there is no provincial data protection law; and where the public bodies of the provinces act in a judicial rather than an administrative capacity. Otherwise provincial laws apply to public bodies of the provinces.

- the provision of information to the data subjects from whom personal data are collected;
- the regulation of international transfers of personal data;
- confidentiality.

To the extent that the substantive rules required by the Directive are not covered by the common provisions in Part I they are dealt with separately for the public sector in Part II and for the private sector in Part III.

Part II sets out detailed rules for the collection of personal data (Section 13), the storage, modification and use of personal data (Section 14), the transfer of personal data to other public bodies (Section 15) and to private bodies (Section 16), and makes general provision for the implementation of the law within the public administration(Section 18). It goes on to deal with the right of subject access (Section 19), the data subject's right to be informed when personal data are collected from third parties (Section 19a), the correction, erasure and blocking of personal data, and the right of objection (Section 20), and appeals to the federal supervisory authority (Section 21). Finally, Part II deals with the establishment and functions of the federal supervisory authority (Chapter III).

Part III sets different rules for the collection and further processing of personal data by a private sector organisation for its own business purposes (Section 28) from those that apply when personal data are collected and further processed for the purposes of "transfer", in particular advertising, the activities of credit inquiry agencies, trading in addresses, and opinion or market research (Section 29). (According to the definition in Section 3, "transfer" means disclosing the personal data to a third party, or allowing a third party to gain access to the data.) There are separate rules for data intended to be transferred in anonymised form (Section 30). There are provisions dealing with the data subject's right to be informed when personal data are collected from third parties (Section 33), the data subject's right to obtain information about the processing of his personal data (Section 34), the right to have data corrected, erased or blocked (Section 35), the supervisory authority (Section 38) and codes of conduct (Section 38.a).

(It is worth noting in passing that the German law is one of those mentioned above that do not expressly include the data protection principles as described in Article 6 of the Directive. These principles are largely not covered by Part I. The provisions of both Part II and Part III must, therefore, both find ways of giving effect to them unless they are covered in another legal instrument.)

7.2.2 Italy

The Italian law distinguishes between the public and private sectors for certain limited purposes. Section 18 provides that public sector bodies may only process personal data in order to discharge their institutional functions. It expressly provides that individuals' consent is not necessary. Section 23, on the other hand, makes clear that the primary ground for processing personal data in the private sector is individuals' consent. However, Section 24 goes on to set out a long list of circumstances in which consent is not necessary. Other provisions applying specifically to the public sector cover the

communication of personal data (Section 19), and the processing of sensitive data (Sections 20 and 21)

The Italian law takes the form of a Personal Data Protection Code. Part II of the law sets out detailed provisions which apply to particular sectors. These include many public sector functions such as the courts, the police, state defence and security, processing operations in the public sector more generally (covering matters such as access to administrative records; public registers and professional registers; registers of births, deaths and marriages, census registers and electoral lists; purposes in the substantial public interest; and specific permits); as well as activities in areas which may at least in part be in the public sector such as health and education.

7.2.3 Slovenia

The Slovenian law contains separate articles setting out the legal grounds for the processing of personal data in the public sector (Article 9) and in the private sector (Article 10). However, the differences in the grounds may be considered slight.

The law contains special rules for the processing of biometric data, and again distinguishes between the public and private sectors. In both cases the restrictions on the processing of such data are tight. Article 79 provides that the public sector may process such data only where authorised by statute and for limited purposes (except where the processing is necessary to meet international treaty obligations, or the purposes of passport control). Article 80 makes similar provision (other than the exception) for the private sector, and contains the added requirement that employees must be informed in writing in advance if their biometric data are to be processed. Where no statute is applicable, Article 80 sets out a procedure allowing public sector controllers to seek an authorisation to process biometric data from the supervisory authority.

7.2.4 Spain

The Spanish law also distinguishes between the public and private sectors for some purposes. One example is the grounds for the “creation of files” (which can be understood as the grounds for processing personal data). Article 20 specifies that files of the public administrations may only be created, modified or deleted in accordance with a general provision published in the official state journal. The Article lays down the following list of information that must be provided:

> “a) The purpose of the file and its planned use.
> b) The persons or bodies on which it is planned to obtain personal data or which they are obliged to submit data.
> c) The procedure for collecting the personal data.
> d) The basic structure of the file and a description of the personal data included in it.
> e) The intended transfers of personal data and, where applicable, the intended transfers of data to third countries.

f) The officials in the administrations responsible for the file.
g) The services or units with which the rights of access, rectification, cancellation and objection may be exercised.
h) The security measures, indicating the basic, medium or high level required."

The article also requires the provision of information about the "fate" of the files or, where applicable, the timetables to be adopted for their destruction.

The requirements for the creation of private sector files are much simpler. Article 25 says:

> "Files in private ownership containing personal data may be created when it is necessary for the success of the legitimate activity and purpose of the person, undertaking or body owning them and the guarantees laid down by this Law for the protection of persons are respected."

Other special provisions for the public sector cover communication of data between public administrations (Article 21), files of the security agencies (Article 22, which imposes heavy restrictions on the collection and processing of personal data for police purposes), and exceptions to individuals' rights (Articles 23 and 24). On this last point, it is interesting to note that there are no equivalent exemptions for the private sector. This seems to mean that individuals cannot be refused access to their personal data in the private sector, even though allowing access could harm an important public interest (for example the prevention or detection of crime).

7.3 Comment from the EU perspective

The substantive data protection rules, including the data protection principles, are equally relevant and can be applied equally effectively to the processing of personal data in the public sector and the private sector. For the most part, the rules set minimum standards and some countries may wish to enlarge upon them. In doing so they may find it expedient for the additional provisions to take a somewhat different form in the public and private sectors. Some EU Member States, for example Italy, Slovenia and Spain, have chosen to do this to a limited extent. But their laws remain solidly based upon a common set of basic rules, including the data protection principles, that are applicable across the sectors.

Germany has chosen to follow a different approach. The reasons are not clear, although they may have something to do with Germany's federal structure. The approach seems to pre-date the Directive. Prior to the Directive's adoption, Germany's data protection law made a similar distinction between the public and private sectors. Indeed, the German approach seems to have had some influence over the initial choice of a model for the Directive. The first draft of the Directive, brought forward in 1990, made separate provision for the public sector and for the private sector. However, the revised draft of 1992 abandoned this approach in favour of a single set of provisions that apply to all processing of personal data.

7.4 Comment from the Chinese perspective

Together with most European states, China falls into the civil law family, in accordance with whose tradition statutes must be laid out in a logical and united way. In this sense, it is possible, indeed essential, for Chinese legislators to lay down a unified law that applies to processing in both the public and private sectors. However, as has been explained in Chapter 3, the different conditions of China and EU member states cannot be overlooked, with the public sector playing a much more powerful part.

Recommendation (EU-Perspective): The simplest approach is to apply a common set of data protection rules to both the public and private sectors, augmented as necessary with any desired sectoral provisions. China should follow this approach.
Recommendation (CH-Perspective): It is advisable for the Chinese government to lay down the substantive information protection rules, which include the information protection principles, the rights of individuals, the obligations and duties of processors. These rules are equally relevant and can be applied equally effectively to the processing of personal information in the public sector and the private sector. These general provisions should be complemented with additional provisions that apply differentially to the public and private sectors.

8 The need for exemptions and restrictions

8.1 The Directive

In order to safeguard important interests, the substantive data protection rules may need to be entirely disapplied or to be restricted in their effect in certain circumstances. A number of provisions in the Directive provide for such exemptions or restrictions. (In this paper the word "exemption" is used to mean both full disapplication and partial restriction.)

The main provision for exemptions is made by Article 13. Within the limits that it imposes, Article 13(1) applies to the processing of personal data for any purpose.

> "1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21[5] when such a restriction constitutes a necessary measure to safeguard:
> (a) national security;
> (b) defence;
> (c) public security;
> (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
> (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
> (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
> (g) the protection of the data subject or of the rights and freedoms of others."

Article 13.2 is more limited in its scope. It provides an exemption only from individuals' right of access to their personal data under Article 12, and is available only for processing for the purpose of scientific research or creating statistics:

> "2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in

[5] Article 6(1) establishes the data protection principles. Articles 10 and 11(1) deal with the provision of information to data subjects whose personal data are collected. Article 12 establishes individuals' right of access to their personal data. Article 21 requires information about the processing of personal data to be made available to the public.

> personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics."

Other articles of the Directive also make specific provision for exemptions. It is worth mentioning two in particular.

Article 9 recognises the need for exemptions in order to balance privacy with freedom of expression:

> "Member States shall provide for exemptions or derogations from the provisions of this Chapter *[Chapter II, the substantive data protection rules]*, Chapter IV *[international transfers of personal data]* and Chapter VI *[supervisory authority]* for the processing of personal data carried out solely for journalistic purposes or the purposes of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression."

Significantly, this article does provide an exemption from Chapter III of the Directive which deals with judicial remedies, liability and sanctions.

Although Article 11.1 (which deals with the collection of personal data otherwise than from the data subject) is within the scope of Article 13, it specifies that the information does not have to be provided if the data subject already has it, and further exemptions from its requirements are permitted by Article 11.2:

> "2. *[Article 11.1]* shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards."

(Article 10 deals with the collection of personal data from the data subject. While it permits the information not to be given if the data subject already has it, it does not permit exemptions similar to those available under Article 11.2. The reason for this is that it should always be possible to provide the information relatively easily when personal data are collected directly from the data subject.)

Article 26 provides for exemptions from the rules governing the transfer of personal data to third countries. These arrangements are dealt with later in this paper.

8.2 Member States' laws

The perceived need for exemptions, and their form and extent, vary among the Member States.

8.2.1 Subject access: general

There is very wide recognition of the need, in certain circumstances, to restrict data subjects' right to gain access to their data. However, the way in which this is done differs across the Member States. Some Member States' laws set out the grounds on which the exemption is available in a general way:

The exemption in Section 26 (2) of the Austrian law is expressed in very general terms: It says:

> "(2) *[Subject access]* shall not be given insofar as this is essential for the protection of the data subject for special reasons or insofar as overriding legitimate interests pursued by the controller or by a third party, especially overriding public interests, are an obstacle to furnishing the information. Overriding public interests can arise out of the necessity
>
> 1. to protect the constitutional institutions of the Republic of Austria or
> 2. to safeguard of the operational readiness of the federal army or
> 3. to safeguard the interests of comprehensive national defence or
> 4. to protect important foreign policy, economic or financial interests of the Republic of Austria or the European Union or
> 5. to prevent and prosecute crimes.
>
> The right to refuse *[access]* for the reasons stated in sub-paragraphs 1 to 5 is subject to control by the Data Protection Commission pursuant to section 30 paragraph 3 and the special complaint proceeding before the Data Protection Commission pursuant to section. 31 paragraph 4."

The exemption in Section 27 of the Finnish law, while still general, is more specific:

> " (1) There is no right of access, as referred to in section 26 above:
>
> (1) if providing access to the data could compromise national security, defence or public order or security, or hinder the prevention or investigation of crime;

(2) if providing access to the data would cause serious danger to the health or treatment of the data subject or to the rights of someone else;

(3) if the data in the file are used solely for historical or scientific research or statistical purposes; or

(4) if the personal data in the file are used in the carrying out of monitoring or inspection functions and not providing access to the information is indispensable in order to safeguard an important economic interest or financing position of Finland or the European Union.

(2) If only a part of the data on a data subject is such that it falls within the restriction on the right of access provided in paragraph (1), the data subject shall have the right of access to the remainder of the data."

The United Kingdom law, on the other hand, makes no general provision of this kind. The law identifies each activity for which an exemption is required and makes express provision for an exemption for that activity. For example, Article 31(1) provides an exemption for the activities mentioned in Article 31(2):

"(2) Subsection (1) applies to any relevant function which is designed—

(a) for protecting members of the public against—

(i) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate,

(ii) financial loss due to the conduct of discharged or undischarged bankrupts, or

(iii) dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorised to carry on any profession or other activity,

(b) for protecting charities against misconduct or mismanagement (whether by trustees or other persons) in their administration,

(c) for protecting the property of charities from loss or misapplication,

(d) for the recovery of the property of charities,

(e) for securing the health, safety and welfare of persons at work, or

(f) for protecting persons other than persons at work against risk to health or safety arising out of or in connection with the actions of persons at work."

Other similarly detailed exemptions are provided elsewhere in the legislation. Among other things they cover: national security; the prevention and detection of criminal offences and the apprehension and prosecution of offenders; the assessment and collection of tax; the functions of the Ombudsman; the combat effectiveness of the armed forces; the appointment of judges; the processing of personal data concerning health, social work or education in order to protect individuals from serious harm

In some Member States' laws, where the data subject him/herself is prevented from having access, provision is made for access by the supervisory authority. This is the case with Article 11.2 of the Portuguese law, which says:

> "2 – In the case of the processing of personal data relating to State security and criminal prevention or investigation, the right of access may be exercised by means of the CNPD *[the data protection supervisory authority]* or another independent authority in whom the law vests verification of compliance with legislation on the protection of personal data."

The Portuguese law goes on to specify that the information must not then be disclosed to the data subject by the supervisory authority. Article 11.4 says:

> "4 – In the cases provided for in (2) … , if communication of the data might prejudice State security, criminal prevention or investigation and freedom of expression and information or the freedom of the press, the CNPD shall only inform the data subject of the measures taken."

Article 11.5 of the Portuguese law also requires the right of access to health data to be exercised by the intermediary of the individual's doctor:

> "5 – The right of access to information relating to health data, including genetic data, is exercised by means of the doctor chosen by the data subject."

A similar provision is also found in other Member States' laws, although in some cases individuals are allowed to choose whether to seek access themselves or to ask their doctor to do so on their behalf. For example, Article 43 of the French law says:

> "Whenever the exercise of the right of access applies to medical personal data, the data may be disclosed to the data subject, as the person chooses, directly or through a doctor that he designates for this purpose, in conformity with the provisions of Article L1111-7 of the Code of Public Health."

The United Kingdom law allows individuals to gain access to their health data under the normal subject access arrangements. However, it provides an exception from the right of subject access where granting access would be likely to cause serious harm to the physical or mental health of the data subject or any other person.

8.2.2 Subject access: research and statistics

Article 23(2) of the Maltese law provides an example of an exemption, based on Article 13.2 of the Directive, for research and statistics.

> "(2) The provisions of article 21 *[the right of subject access]* shall not apply when data is processed solely for purposes of scientific research or is kept in personal form for a period which does not exceed the period necessary for the sole purpose of compiling statistics:
> Provided that the provisions of this sub-article shall not apply where the data is

used for taking measures or decisions regarding any particular individual or where there is a risk of breaching the privacy of the data subject."

Section 33(4) of the United Kingdom law provides slightly different safeguards:

> "Personal data which are processed only for research purposes are exempt from section 7 *[the right of subject access]* if –
> (a) they are processed in compliance with the relevant conditions, and
> (b) the results of the research or any resulting statistics are not made available in a form which identifies data subjects or any of them."

Section 33(1) defines "research purposes" as including statistical or historical purposes; and the "relevant conditions" as:

> "(a) that the data are not processed to support measures or decisions with respect to particular individuals, and
> (b) that the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be , caused to any data subject."

Article 44 of the Dutch law applies the exemption for research and statistics to the duty to provide information to individuals as well as to the right of access:

> "1. Where processing is carried out by institutions or services for the purposes of scientific research or statistics, and the necessary arrangements have been made to ensure that the personal data can only be used for statistical or scientific purposes, the responsible party shall not be required to provide the information referred to in Article 34 *[the duty to provide information to individuals]* and may refuse to comply with the requests referred to in Article 35 *[the right of subject access]*.
>
> 2. Where personal data are being processed which form part of archive records transferred to an archive storage place under Articles 12 or 13 of the Archives Act 1995, the responsible party shall not be required to provide the information referred to in Article 34."

8.2.3 Information for data subjects

Many Member States' laws follow the Directive in permitting exemptions based on Article 11.2 of the Directive. Article 29 of the Danish law, which deals with the circumstances in which personal data are collected from sources other than the data subjects, provides the following exemptions:

> "(2) The rules laid down in subsection (1) *[the requirement to provide information to data subjects]* shall not apply where the data subject already has the information referred to in paragraphs 1 to 3 or if recording or disclosure is expressly laid down by law or regulations.

(3) The rules laid down in subsection (1) shall not apply where the provision of such information to the data subject proves impossible or would involve a disproportionate effort."

The Danish law also provides a general exemption from controllers' duty to inform data subjects about the collection of their personal data similar to that applying to subject access. Article 30 says:

"(1) Section 28 (1) *[collection of data from the data subject]* and section 29 (1) shall not apply if the data subject's interest in obtaining this information is found to be overridden by vital private interests, including the interests of the subject data himself.

(2) Derogations from section 28 (1) and section 29 (1) may also take place if the data subject's interest in obtaining this information is found to be overridden by vital public interests, including in particular:

1. national security;
2. defence;
3. public security;
4. the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for regulated professions;
5. an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; and
6. monitoring, inspection or regulatory functions, including temporary tasks, connected with the exercise of official authority in cases referred to in paragraphs 3 to 5."

The exemption in the Greek law, on the other hand, is more restrictive. It is available only for limited purposes and requires a decision of the supervisory authority. Article 11.4 says:

"4. By virtue of a decision by the Authority, the obligation to inform, pursuant to paragraphs 1 and 3, may be lifted in whole or in part, provided that data processing is carried out for reasons of national security or for the detection of particularly serious crimes. In a state of emergency said obligation may be lifted by way of a provisional, immediately enforceable judgment by the President, *[of the supervisory authority]* who shall convene as soon as possible the Board in order that a final judgment on the matter may be issued."

Some countries deal with the exemptions from the duty to provide information to data subjects, and from the right of access together. As well as doing this, Article 36 of the Slovenian law also provides an exemption from the right to rectify personal data:

(1) The rights of an individual from the third and fourth paragraphs of Article 19, *[Information for data subjects]* Articles 30 *[Right of subject access]* and 32 *[Right to have data rectified]* of this Act may exceptionally be restricted by statute for reasons of protection of national sovereignty and national defence, protection of national security and the constitutional order of the state, security, political and economic interests of the state, the exercise of the responsibilities of the police,

> the prevention, discovery, detection, proving and prosecution of criminal offences and minor offences, the discovery and punishment of violations of ethical norms for certain professions, for monetary, budgetary or tax reasons, supervision of the police, and protection of the individual to whom the personal data relate, or the rights and freedoms of others.
>
> (2) Restrictions from the previous paragraph may only be provided in the extent necessary to achieve the purpose for which the restriction was provided."

A noteworthy feature of this article is the express requirement, in paragraph (2), only to apply the exemption to the extent necessary to achieve the desired purpose. This requirement for proportionality is an essential, but often unstated, element in applying exemptions.

8.2.4 Data protection principles

Member States' laws contain fewer specific exemptions from the data protection principles. However, following the model in Article 13(1) of the Directive, some Member States' laws apply the general exemptions to the data protection principles as well as to subject access and other provisions. An example is Article 23 of the Maltese law which says:

> **"23.** (1) The provisions of articles 7, 19, 20 (1), 21 and 35 shall not apply when a law specifically provides for the provision of information as a necessary measure in the interest of:
> (*a*) national security;
> (*b*) defence;
> (*c*) public security;
> (*d*) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
> (*e*) an important economic or financial interest including monetary, budgetary and taxation matters;
> (*f*) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority referred to in paragraphs (*c*), (*d*) and (*e*); or
> (*g*) such information being prejudicial to the protection of the data subject or of the rights and freedoms of others."

(Article 7 creates the data protection principles. Articles 19 and 20 deal with the duty to provide information to data subjects. Article 21 creates the right of subject access. Article 35 deal s with publicity for processing.)

Similar provisions are found in Article 43 of the Dutch law, and in Article 3(6) of the law of the Czech Republic. In the latter case, the exemptions are only available where a special Act applies.

The data protection principles place restrictions on the extent to which personal data may be disclosed by the data controller. Where disclosures are necessary for one of the reasons set out in Article 13.1 of the Directive, it may, therefore, be necessary to provide

an exemption from the data protection principles. Article 8 of the Irish law reflects this. It says:

> "8.-Any restrictions in this Act on the processing of personal data do not apply if the processing is-
>
> (a) in the opinion of a member of the Garda Siochana *[the police]* not below the rank of chief superintendent or an officer of the Permanent Defence Force who holds an army rank not below that of colonel and is designated by the Minister for Defence under this paragraph, required for the purpose of safeguarding the security of the State,
>
> (b) required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the State, a local authority or a health board, in any case in which the application of those restrictions would be likely to prejudice any of the matters aforesaid,
>
> (c) required in the interests of protecting the international relations of the State,
>
> (d) required urgently to prevent injury or other damage to the health of a person or serious loss of or damage to property,
>
> (e) required by or under any enactment or by a rule of law or order of a court,
>
> (f) required for the purposes of obtaining legal advice or for the purposes of, or in the course of, legal proceedings in which the person making the disclosure is a party or a witness,
>
> (g) [deleted]or
>
> (h) made at the request or with the consent of the data subject or a person acting on his behalf."

As originally enacted in 1988 the introductory words of this Section referred to "disclosure" rather than "processing". The amendments to the wording, and the deletion of paragraph (g), were made by the Act of 2003 giving effect to the Directive. A similar, although not identical, provision was found in the previous UK law dating from 1984. It was included there in order to remove the possible obstacles to necessary disclosures imposed by the data protection principles.

8.2.5 Freedom of expression

Member States' laws vary greatly in the way they give effect to the exemption permitted by Article 9 of the Directive..

Section 2(10) of the Danish law contains a very wide exemption for processing for journalistic, artistic or historical purposes. It says:

> "(10) Processing of data which otherwise takes place exclusively for journalistic purposes shall be governed exclusively by sections 41, 42 and 69 of this Act. The same shall apply to the processing of data for the sole purpose of artistic or literary expression."

(Section 41 deals with security, section 42 with the sub-contracting to data processors and section 69 with compensation for damage.)

Article 9 of the Luxembourg law, on the other hand, is more specific and the scope of the exemptions is narrower:

> "(1) Without prejudice to legal provisions on freedom in mass communications methods, and in as far as the under mentioned derogations are necessary to reconcile the right to privacy to the rules governing freedom of expression, processing carried out solely for journalistic, artistic or literary expression are not subject:
>
> (a) - to the prohibition on processing the specific categories of data provided under Article 6, paragraph (1);
>
> - to the limitations concerning the processing of legal data stated in Article 8, if the processing is in connection with data that have manifestly been made public by the data subject, or to data which are closely related to the public character of the data subject or the event in which he is involved;
>
> (b) to the condition that the adequate protection required in the case of processing of data that is transferred to a third country as stated in Article 18 paragraph (1) should be provided;
>
> (c) to the information obligation of Article 26, paragraph (1) if its application would compromise the collection of data from the data subject;
>
> (d) to the information obligation of Article 26, paragraph (2) if its application would either compromise the collection of data, or a planned publication, or public disclosure in any form whatsoever of the said data, or would provide information that would make it possible to identify the sources of information;
>
> (e) to the data subject's right of access which may be deferred or limited in accordance with Article 28, paragraph (4) and Article 29.
>
> (2) When notification of processing carried out for the purposes of journalism or artistic or literary expression is made, the notification will state only the name(s) and address(es) of the controller or his representative."

Article 67 of the French law is even more specific, in that it also sets certain procedural requirements, including a requirement for journalistic media bodies to appoint a formal data protection office, and deals with sanctions. It also deals with the right of reply.

> "Sub-section (5) of Article 6 *(limitation of the period of storage of data)*, Articles 8 *(prohibition of processing of political data…)* 9 *(prohibition of processing of offences)* and 22 *(obligation of notification)*, Sub-section (1) *(authorisation by the*

CNIL of statistical, political…processing) and Sub-section (3) *(authorisation by the CNIL relating to offences)* of Section I of Article 25, Articles 32 *(prior information)*, 39 *(right of access)*, 40 *(right of rectification)* and 68 to 70 *(transfer of data)* shall not apply to processing of personal data carried out for the sole purpose of:

(1) literary and artistic expression; and

(2) professional journalism, according to the ethical rules of this profession.

However, for processing mentioned in subsection (2), the exemption from the obligation to make a declaration as provided for in Article 22 is conditional on the appointment, by the data controller, of an officer responsible for data protection who belongs to a media undertaking, who maintains a register of processing carried out by the data controller and who independently ensures the proper application of the provisions of this Act. This appointment shall be notified to the "Commission nationale de l'informatique et des libertés". *[The supervisory authority.]*

In the event of non-compliance with the provisions of the Act that apply to the processing provided for in this Article, the data controller shall be ordered by the "Commission nationale de l'informatique et des libertés" to bring matters into conformity with the Act. In the event of a failure to perform his duties, the officer is discharged from his functions at the request, or after consultation, of the "Commission nationale de l'informatique et des libertés".

The provisions of the preceding paragraphs shall not prevent the application of the provisions of the Civil Code, the laws relating to the media and the Criminal Code that provide for the conditions of the exercise of the right of reply and that prevent, limit, compensate and, if necessary, sanction violations of privacy and attacks on the reputation of individuals."

8.3 Comment from the EU perspective

The main justification for providing exemptions from the substantive data protection rules is the need to safeguard important public interests (including the protection of individuals). This is the objective of Article 13.1 of the Directive.

The fact that the interests to be safeguarded are "public" interests does not mean that the exemptions are only available for processing that is carried out in the public sector. As this paper has already recognized, many activities that were formerly within the exclusive competence of the State are now carried out by private sector bodies. In the field of enforcement of the criminal law, for example, there is significant private sector involvement in the management of the arrangements for attaching electronic tags to offenders to allow them to remain in the community under supervision; and some prisons are run by the private sector. The private sector's involvement in other activities which affect important public interests has always been significant. For example, a State's financial and economic stability and development depend to a large extent upon the efficient functioning of banks and other private sector bodies.

In order to safeguard these interests it is sometimes necessary to limit the effect of the

data protection rules. The right of subject access provides the clearest examples. Organisations often hold information about individuals for the purpose of taking decisions about them. A trivial example is that of a small shopkeeper who holds information about the purchases made on account by his customers, so that he can send them their bills at the end of the month. If one of the customers made a subject access request, no harm would be caused by the shopkeeper providing the customer with the information from his account. A more serious example, though, would be that of the police who hold information about individuals whom they suspect of carrying out criminal offences. If the suspects were able to gain access to that information by exercising their right of subject access and find out that they were under suspicion, they might alter their behaviour in an attempt to undermine the efforts of the police to obtain sufficient evidence to apprehend them. Providing an exemption from the right of subject access would help prevent this undesirable outcome. Many similar examples could be given across the range of public interests to which Article 13.1(a) to (f) of the Directive applies.

It is equally important to protect individuals, and this is permitted by Article 13.1(g). Sometimes, allowing individuals to see their own personal data can have harmful effects, either for the individual or for other people. A doctor, for example, may have information that a patient has a life-threatening condition, which is unknown to the patient himself. In the doctor's clinical judgment the shock of disclosing the information to the patient would be likely to make the patient's physical condition much worse. In such circumstances it might be desirable to withhold the information should the patient make a subject access request. Another example from the health sector would be that of a psychiatric patient whose health record contains personal data which, if known to the patient, would be likely, in the doctor's clinical judgment, to cause him to harm himself or to attack his wife or another family member.

As noted above, exemptions from the data protection principles themselves are less common, although it is necessary to make provision for them. Possibly the clearest demonstration of the need for exemptions from the data protection principles comes in the areas of national security and criminal law enforcement. To take just one example, activities of the relevant agencies often involve the gathering of intelligence information much of which comprises personal data. Intelligence information by its nature is uncertain and may well be inaccurate. Applying the data protection principles, which include a requirement for personal data to be accurate, could mean that the agencies would no longer be able to collect intelligence information in the form of personal data. This would seriously prejudice their activities.

The right to privacy and the right to freedom of expression are both fundamental rights established in the European Convention on Human Rights. Neither has priority over the other. It is essential, therefore, to ensure that an appropriate balance is struck between them. That is the purpose of Article 9 of the Directive. Deciding on the extent to which it is necessary to provide exemptions is a delicate and difficult matter. As shown above, some Member States laws' provide very wide exemptions from almost all the substantive data protection rules, while others are more restrictive. A good case can certainly be made that the data protection principles, the right of access and the duty to inform data subjects that their data are collected can all have a "chilling" effect, particularly on investigative journalism. On the other hand, Europe is not short of examples of the media's publishing stories which include intimate personal details where it is difficult to discern a legitimate "public interest". This approach may sell newspapers. However, as has often been said, that which interests the public is not always the same as that which is

in the public interest.

The exemptions permitted by Article 13.2 and Article 11.2 of the Directive are more straightforward. The first case is justified by the fact that the processing in question does not risk breaching the data subjects' privacy, which is a mandatory condition for the exemption. The second is partly based on the severe practical realization that providing the information to the data subjects may sometimes simply be impossible or disproportionately burdensome. In both cases, safeguards are needed where the exemptions are applied.

8.4 Comment from the Chinese perspective

Exemptions from the main information protection rules will be necessary in any Chinese information protection law which is based on the European model, and it will be necessary to identify carefully where the need for exemptions is likely to arise. The reasons are as follows. First and foremost, the processing of personal information, especially in the public sector, is often in the public interest. And pursuant to the principle of balancing interests, the rights of individuals must be restricted to the extent that public policy requires. Secondly, the granting of rights often makes social costs increase sharply, so that overall income will decrease and the welfare of social participants, including individuals, will be harmed. In addition, In China the social sphere is dominated by the public will and interests and private rights often give way to it. Although this is changing gradually, the public will and interests are still strong.

Recommendation (EU-Perspective): Exemptions from the main data protection rules will be necessary in any Chinese data protection law which is based on the European model. It will be necessary to identify carefully where the need for exemptions is likely to arise. The scope of each exemption should be proportionate to the need identified.
Recommendation (CH-Perspective): Chinese legislators should clearly define the conditions in which the exemptions and restrictions occur. They include, but are not limited to, those set out in Article 13.1 of the Directive. In deciding whether personal rights should be restricted, judiciaries must apply the principle of balancing interests: that is to weigh the interests of individuals and public interests. When exemptions and restrictions apply, compensation for the individual according to the value of personal information is essential.

9 Consent: Opt-in and Opt-out

9.1 The Directive

Article 2 (h) of the Directive defines consent as follows:

> " "the data subject's consent" shall mean any freely given, specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."

The data subject's consent is just one of a number of legal bases for processing personal data. Both Article 7, which sets the legal bases for processing non-sensitive data, and Article 8 which does the same for sensitive data, establish several alternatives to consent.

Where consent is the legal base for the processing of non-sensitive personal data, Article 7(a) requires that it be "unambiguously given". Where consent is used as the legal base for processing sensitive data, Article 8.2(a) requires that consent be "explicit".

The Directive does not use the terms "opt-in" and "opt-out".

9.2 Member States' laws

Most, but not all, Member States' laws include a definition of "consent". Most of the definitions broadly follow that in the Directive, although there are some variations in the language used. Where this is so, the definitions tend to stress the need for the data subject's active involvement in giving consent. For example, the definition in Section 3(7) of the Finnish law says that consent is "…any voluntary, detailed and conscious expression of will…". Section 2(2) of the Latvian law says that consent involves "… a freely, unmistakeably expressed affirmation of the wishes of a data subject…". Article 7(5) of the Polish law expressly rules out consent being given implicitly:

> " 5) the data subject's consent - shall mean a declaration of will by which the data subject signifies his/her agreement to personal data relating to him/her being processed; the consent cannot be alleged or presumed on the basis of the declaration of will of other content."

The German law is particularly precise. Section 4a says:

> "Consent shall be effective only when based on the data subject's free decision. He shall be informed of the purpose of collection, processing or use and, in so far as the circumstances of the individual case dictate or at his request, of the consequences of withholding consent. Consent shall be given in writing unless special circumstances warrant any other form. If consent is to be given together with other written declarations, it shall be made distinguishable in appearance."

As with the Directive, all Member States' laws provide a range of permissible legal bases for processing both non-sensitive and sensitive personal data of which consent is just one. With the exception of Germany, whose law gives primacy to the active involvement of the data subject, most Member States' laws do not expressly attach greater importance to consent than to the other legal bases.

In dealing with the legal bases for processing non-sensitive data, many Member States' laws simply refer to "consent" as being one of the permissible legal bases, and do not specify, as does the Directive, that consent must not be "ambiguous". However, where sensitive data are concerned, most Member States' laws specify that consent, where it is the legal base, must be "explicit" or "express". Some go further, and specify that consent must be "written". Article 7 of the Spanish law requires consent to the processing of sensitive data to be both explicit and written. Moreover, since in Spain the Constitution says that nobody may be obliged to state his ideology, religion or beliefs, Article 7 makes clear that, in relation to the processing of such data the data subject must be informed of his right to refuse consent.

Like the Directive, Member States' laws do not use the terms "opt-in" and "opt-out".

9.3 Comment from the EU perspective

As noted above, the data subject's consent is one of a number of legal bases for processing personal data. Neither the Directive nor, for the most part, Members States' laws, focus on consent as the central basis for establishing a lawful regime for processing personal data. Consent is just one option among others. This is important. While the individual's consent can be a safeguard, to construct a regime around consent with no alternative grounds for making the processing of personal data lawful would be wholly impracticable. Obtaining consent can be difficult and is often not feasible. The provision of essential services, for example, should not be dependent upon organisations' ability to contact individuals and the individuals' willingness to consent. Nonetheless, where consent is relied upon, it is important that it should meet certain standards of reliability. It should be given freely by the individual, specific to the proposed activity and based on adequate information.

Neither the Directive nor Member States' laws use the terms "opt-in" and "opt-out". In identifying the degree of the data subject's involvement in giving consent, they prefer to rely on terms such as "explicit", "express" or "written". Consent is capable of being given implicitly. For example, a person who responds to a newspaper advertisement for a product by purchasing the product by mail, is implicitly giving his consent to the advertiser to process his name, address and other personal data needed to complete the purchase. However, if the advertisement contains a form which the purchaser is invited to complete and return to the advertiser, agreeing that his personal data may be processed, the consent becomes express, explicit, and, in this case, written.

The terms "opt-in" and "opt-out" are most frequently used to describe situations in which individuals are given a choice. The choice can be offered in one of two ways: the individual is told that something will happen to him unless he actively shows his opposition

(opt-out); or the individual is told that the event will only happen to him if he actively shows his support (opt-in). With "opt-out" individuals have to take steps to stop something happening. With "opt-in" they must take steps if they want something to happen.

Direct marketing provides a clear example of the use of "opt-in" and "opt-out" consent. Businesses carrying out direct marketing have access to databases containing contact information for large numbers of people. They wish to use those databases to contact the people to offer them goods or services for sale. Under Article 14 of the Directive, individuals are entitled to be able to object to the use of their personal data for direct marketing purposes. With their mail-shots, therefore, businesses include information about this right. This can take the form of a statement that the individual's personal data will continue to be used for direct marketing purposes unless the individual objects. That is "opt-out". It puts the burden on the individual to take positive steps to avoid receiving further marketing material. Alternatively, and much less frequently, the statement may say that the individual's personal data will not be used for further mail-shots unless the individual responds giving his consent. That is "opt-in". If individuals do nothing, their personal data will not be used for direct marketing purposes. Most Member States' laws contain provisions giving individuals the right to "opt-out" from direct marketing.

9.4 Comment from the Chinese perspective

A requirement for consent to be freely given, specific and informed is idealistic, in view of the emphasis attached to the need for efficiency in the processing and matching of information, especially in the field of electronic commerce. Under these circumstances, it may not be feasible for the individual to consent in an expressed and informed way. This issue has been hotly debated among Chinese academics. Some experts hold the view that individuals should give consent in an express way (that is, opt-in); others believe that individuals should give consent in an implied way (that is, opt-out); still others suggest a compromise. On one view, before sensitive personal information is possessed, the individuals should, in principle, consent in an express and informed way, pursuant to the principle of identification of rights, subject to there being an exception where the processing of the personal information is an urgent need, Only in this way can a compromise between the value of efficiency and equity be achieved. In all cases, consent should be freely given and specific.

The impact of applying encryption technology can cause uncertainty in determining whether an individual gives express consent. Pursuant to Chinese practice, the act of providing the code to processors can be considered to be express consent.

Recommendation: China's data protection law will need a number of legal bases for processing personal data of which the individual's consent should be one. Where it is required, consent should be freely given, specific and informed.

10 Data subjects' rights and data controllers' obligations

10.1 The Directive

10.1.1 Rights of data subjects

The Directive expressly identifies the following rights for individuals:

- the right to obtain from the controller
  - specified information about the processing of their personal data;
  - access to the personal data themselves;
  - information about the logic underpinning the automated processing of their personal data;
  - where necessary, the rectification, erasure or blocking of their personal data;
  - the notification of third parties to whom personal data have been disclosed, of any rectification etc; (Article 12)
- the right to object, in certain circumstances, to the lawful processing of their personal data; (Article 14(a))
- the right to object to their personal data being used for the purposes of direct marketing; (Article 14(b))
- the right not to be subjected to certain fully automated decisions; (Article 15)
- the right to a judicial remedy for a breach of the other rights provided for by the Directive; (Article 22)
- the right to compensation from the data controller for damage caused by unlawful processing of their personal data; (Article23)

10.1.2 Obligations of data controllers

The basic premise of the Directive is that data controllers are responsible in law for ensuring that the substantive data protection requirements are complied with. The Directive expressly identifies the following obligations for data controllers:

- to ensure that the data protection principles are complied with; (Article 6.2)

- to provide information pro-actively to data subjects about the processing of their personal data; (Articles 10 and 11)
- to provide adequate security, including in their choice of data processors; (Article 17)
- to notify the supervisory authority of the processing of personal data that they carry out; (Article 18)
- to provide to any person on request with information about the controllers' processing of personal data that is not subject to notification; (Article 21.3).

10.2 Member States' laws

Subject only to variations in drafting techniques, all Member States' laws give effect to the rights and obligations outlined above.

Some Member States laws' specify additional, underpinning rights. For example, Section 1 of the Austrian law provides that:

> **"**Everybody shall have the right to secrecy for the personal data concerning him, especially with regard to his private and family life, insofar as he has an interest deserving such protection. Such an interest is precluded when data cannot be subject to the right to secrecy due to their general availability or because they cannot be traced back to the data subject."

Section 1 is found in Article 1 of the Austrian law, which is called a "Constitutional Provision". It also establishes the right for individuals to information about the processing of their personal data, and the right to have incorrect data rectified and illegally processed data erased, thereby confirming that these rights have the status of constitutional provisions.

Article 2 of the Belgian law also establishes a general right:

> "During the processing of his personal data, every natural person has the right to the protection of his fundamental freedoms and rights, in particular the protection of his private life."

This is a tacit acknowledgement of Article 8 of the European Convention on Human Rights which guarantees every person the right to respect for his private life, and in which international data protection instruments and national data protection laws on the European model have their ultimate origin.

Other Member States' laws, including the Italian (Section 1), the Latvian (Section 6) and the Polish (Article 1), establish a right for individuals to the protection of their personal data.

In most Member States' laws, the form in which the rights and obligations are expressed follows that in the Directive. In other words, where the Directive refers to rights on the one hand and to obligations on the other, the Member States' laws do likewise. However, to suggest that there is a clear distinction between rights and obligations would be

misleading. For example, Article 9 of the Belgian law puts an obligation on data controllers to provide information to data subjects (Articles 10 and 11 of the Directive), but Article 9 itself is found in Chapter III which is headed "Data subject's rights".

Often the statement of a right for the data subject is accompanied by an obligation on the data controller to do what is necessary to give effect to the right. Article 10 of the Czech law establishes a general obligation for the controller (and processor) to ensure that data subjects' rights are respected:

> "In personal data processing, the controller and processor shall ensure that the rights of the data subject are not infringed upon, in particular, the right to preservation of human dignity, and shall also ensure that the private and personal life of the data subject is protected against unauthorized interference."

Section 31 of the Danish law is in Part 9 which is headed "The data subject's right of access to personal data", but it expresses the right as a set of obligations on the data controller.

> "**31.** – (1) Where a person submits a request to that effect, the controller shall inform him whether or not data relating to him are being processed. Where such data are being processed, communication to him shall take place in an intelligible form about:
>
> 1. the data that are being processed;
> 2. the purposes of the processing;
> 3. the categories of recipients of the data; and
> 4. any available information as to the source of such data.
>
> (2) The controller shall reply to requests as referred to in subsection (1) without delay. If the request has not been replied to within 4 weeks from receipt of the request, the controller shall inform the person in question of the grounds for this and of the time at which the decision can be expected to be available."

This example also shows that some of the rights and obligations may require elaboration. In the case of the right of subject access, for example, several Member States' laws set out detailed procedural arrangements (dealing with matters such as the method of submitting a request, the fee for making a request, the time limit for responding, and the method of providing the information). These arrangements vary among the Member States.

10.3 Comment from the EU perspective

As is shown in the examples from Member States' laws above, there is no clear distinction between data subjects' rights on the one hand, and the obligations on data controllers on the other. A right for one person is often an obligation for another person. That they are two sides of the same coin is seen with the provisions relating to the accuracy of personal data. The fourth data protection principle in Article 6.1(d) of the Directive requires

personal data to be “accurate and, where necessary, kept up to date”. Article 6.2 requires data controllers to ensure that the data protection principles are complied with. So data controllers have an obligation to ensure the accuracy of personal data. But, at the same time, Article 12(b) of the Directive gives data subjects the right to have inaccurate data corrected.

How “rights” and “obligations” are described in national law will depend, among other things, upon cultural traditions and legislative drafting technique. The important thing is that, whatever they are called, the substantive provisions should achieve the desired effect. As an absolute minimum the following are required:

- data controllers should be responsible in law for complying with the data protection principles and other substantive data protection rules including the pro-active provision to data subjects of basic general information about the processing;
- any person should be able to find out whether a particular organization is processing personal data, the purposes of the processing and the identity and address of the controller;
- individuals should be able, on request, to gain access to information about the processing of their own personal data, and to the personal data themselves;
- individuals should be able to have those data rectified, erased or blocked, as appropriate, where they are inaccurate or unlawfully processed, and to have those to whom their personal data have been disclosed notified of the rectification etc;
- individuals should be able to secure the effective enforcement of, and remedies for the violation of, the above provisions, through the courts or an independent supervisory authority.

Whether it is necessary to go beyond this is a matter of judgment. Individuals’ express right to object to the lawful processing of their personal data was an innovation of the Directive. It is probably little used, but where it is used it may offer a particularly important safeguard. An example could be that of an individual whose neighbour, with whom he was on bad terms, worked as a doctor in a hospital where the individual was being treated. The individual might wish to ask the hospital to ensure that the neighbour was not given access to the individual’s sensitive personal data.

The express provision dealing with the processing of personal data for direct marketing purposes, on the other hand, although also new, is very widely used. Many individuals object very strongly to having their personal data used for this purpose.

The right not to be subjected to certain fully automated decisions is of uncertain usefulness.

10.4 Comment from the Chinese perspective

The subjects’ rights and controllers’ obligations offer a particularly important safeguard for individuals and effective restrictions on the processors. The system of rights and

obligations is not an innovation of Chinese legislation, in that every object, especially personality and property is protected through this system. With this in mind, it is clear that the rules relating to information subjects' rights and information controllers' obligations are the core of information protection law of China.

The rights of information subjects on the one hand, and the obligations on information controllers on the other hand, perform sharply different functions: the rights work as a safeguard for the subjects of personal information; the obligations work as restrictions on information controllers, the infringing of which will have consequences. The obligations include those laid down in private law and those laid down in public law. The latter do not correspond to information subjects' rights. Therefore, in Chinese law the rules of information subjects' rights and information controllers' obligations should be laid out separately.

The rules as to information subjects' rights and information controllers' obligations in the EU Directive and the Member States' laws are essential as well as adjustable to the Chinese context The sole drawback is that the information subjects' rights are not complete. In accordance with the theory of personal data protection law, the information subject has the fundamental right to determine whether and how his information will be processed, and without his consent or other legal basis the controller is in no position to collect and store personal information. From the Chinese perspective, the right of determination plays a leading role in the rules of rights and obligations.

It is suggested that the information subjects' rights should be as follows

- The right to determine whether and how their information will be processed.
- The rights to obtain from the controller specified information about the processing of their personal information, access to the personal information themselves, information about the logic underpinning the automated processing of their personal information, where necessary, the rectification, erasure or blocking of their personal information, the notification of third parties to whom personal information have been disclosed, of any rectification etc.
- The right to object, in certain circumstances, to the lawful processing of their personal information.
- The right to a judicial remedy for a breach of the other rights provided for by information protection law.
- The right to compensation from the information controller for damage caused by unlawful processing of their personal information.

The duties of information processors should be as follows:

- To ask for the information subjects' consent before information processing.
- To be responsible in law for complying with the information protection principles and other substantive information protection rules including the pro-active provision of information to information subjects.
- To ensure any person is able to find out whether a particular organization is processing personal information, the purposes of the processing and the identity and address of the controller.
- To ensure individuals are able, on request, to gain access to information about the processing of their personal information, and to the personal information themselves and have those information rectified, erased or blocked, as appropriate, where they

are inaccurate or unlawfully processed, and to have those to whom their personal information have been disclosed notified of the rectification.

Recommendation: The minimum provisions set out above, in the section headed "Comment from the EU perspective" should be included in any future Chinese data protection law. Serious consideration should be given to including a right to object to certain lawful processing and to processing for direct marketing purposes. How the rights and obligations are expressed is less important than achieving the desired effect.

11 Enforcement

11.1 The Directive

Under the Directive, enforcement of national data protection laws is to be achieved by using a combination of powers exercisable by Member States' data protection supervisory authorities and judicial remedies. The Directive specifies the general requirements.

- Article 22 says that, in addition to any administrative remedies, there must be a right for every person to a judicial remedy for any breach of his rights under national data protection law.
- Article 23 says that any person who suffers damage as a result of unlawful processing or acts incompatible with national data protection law shall be entitled to compensation from the data controller. The data controller is exempt from liability if he proves that he is not responsible for the act or omission in question.
- Article 24 requires Member States to adopt "suitable measures" to ensure the full implementation of their national data protection laws. In particular they must provide sanctions for breach of those laws

Later, in Article 28.3, the Directive goes on to set out the required powers of the data protection supervisory authorities to investigate and enforce the law.

> "Each authority shall in particular be endowed with:
>
> - investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,
>
> - effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20 *Prior Checking]*, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,
>
> - the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.
>
> Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts."

11.2 Member States' laws

Within the general limits laid down by the Directive, the detailed arrangements for enforcement in the different Member States vary quite widely. The following are examples of the way in which Member States laws make the necessary provision.

11.2.1 Austria

Section 30 of the Austrian law gives the supervisory authority the power to examine processing operations if there is reasonable suspicion of an infringement of the law. The supervisory authority can order the controller or processor to give all necessary clarifications and to grant access to data processing and relevant documents. Reasonable suspicion of a breach of the law is not needed in the case of the limited categories of processing which are subject to checking before they may begin, and to certain public sector processing.

After having informed the controller and the owner of the premises where the processing is taking place, the supervisory authority has the right to enter the premises, to operate data processing equipment, to run the processing to be examined and to make copies of the storage media. The controller is required to give the assistance necessary for the examination. The supervisory authority must exercise its powers in the way that least interferes with the rights of the controller and third parties.

Subject to an exemption relating to the investigation of certain crimes, the information acquired by the supervisory authority may be used only for the purposes of data protection supervision.

Where there has been a breach, the supervisory authority has the power to issue recommendations for remedial action to be taken within an appropriate period. If a recommendation is not complied with within the set period, the supervisory authority has the power, among other things, to bring a criminal charge, or, in the case of a serious breach by a private sector controller, to initiate civil court proceedings.

Where private sector data controllers are concerned, section 32 allows data subjects to take action in the civil courts for breach of the right to secrecy, or for rectification or erasure of unlawfully processed or inaccurate data. Where large numbers of data subjects are involved, the supervisory authority may intervene to support them.

Section 33 provides for controllers and processors who have culpably processed personal data contrary to the provisions of the data protection law, to indemnify data subjects "pursuant to the general provisions of the civil law". It is not known whether the indemnification under the relevant provisions of the civil law are limited to compensation for damage caused or whether, as in some jurisdictions, it goes wider to include, for example, compensation for distress. As provided for in the Directive, there is an exemption where the data controller can show that he was not responsible for the circumstances causing the problem.

Section 51 provides for certain processing carried out with the intention of making a profit for the data controller or with the intention of causing harm to the data subject to be punishable by a court with imprisonment of up to one year.

Section 52 provides for certain acts to be treated as administrative offences punishable with fines, in some cases with a maximum of 9,445 Euros and in others with a maximum of 18,890 Euros. District Administrative Authorities have the power to deal with these cases. These provisions apply only where the acts are not punishable by the courts as criminal offences under other legal provisions.

11.2.2 France

Article 44 of the French law gives the supervisory authority the power to enter premises used for the processing personal data for professional purposes between the hours of 06.00 and 21.00. Entry to premises used for private purposes is expressly excluded. The local public prosecutor must be informed before entry. In the case of an objection by the person in charge of the premises, the entry must be authorised by the President of the High Court or by a judge mandated by him. In such a case, if the entry is authorised, it takes place under the supervision of the judge who may go to the premises himself, and who has the power to halt or suspend the entry at any time.

The supervisory authority has the power to request the communication of all the documents needed for the investigation and to take a copy of them; to collect all useful information; to gain access to electronic data processing programmes and data, and to ask for their transcription into
documents that they can use for the for the purposes of the investigation. Only a doctor may ask for communication of personal medical data.

Under Article 45 the supervisory authority may issue a warning to a data controller who does
not comply with his obligations under the law. It may also order the data controller to take remedial action within a time limit that it determines. If the data controller does not comply with this order, the supervisory authority has the power, after due process, to impose a financial penalty (except where the processing is carried out by the State); or to issue an injunction to cease the processing or, where authorization by the supervisory authority for the processing was needed, to withdraw the authorization.

In urgent cases (where there has been a violation of human identity, human rights, privacy, or individual or public liberties) after proceedings in which both parties are heard the supervisory authority may suspend the processing or block certain data for up to three months, except in the case of certain public sector processing, where the supervisory authority may notify the Prime Minister for him to decide on the measures to be taken. In the case of “serious and immediate” violations of the rights and liberties mentioned in the previous sentence, the Chairman of the supervisory authority may ask the relevant court to order any security measure necessary to protect those rights and freedoms.

Article 46 provides that, except in the case of blocking of data, the cases referred to the Prime Minister, and the “serious and immediate” violations, the supervisory authority’s sanctions are to be based on a report by one of the authority’s members. The data controller must be informed of the report and has the right to be heard when the supervisory authority is considering it.

The supervisory authority may make public the warnings that it issues. It may also, in the case of bad faith on the part of the data controller, order the publication, at the expense of the data controller, of any other penalties imposed. The supervisory authority must give reasons for its decisions under Article 45, which must be notified to the data controller. An appeal against the penalty on grounds of both facts and law may be made before the “Conseil d’Etat” (France’s highest administrative court).

Article 47 requires the financial penalties provided for in Article 45 to be of an amount that is proportional to the gravity of the breaches, having regard to any profits obtained from the breach.
In case of a first breach, the penalty may not exceed €150,000. For a second breach within five years, it may not exceed €300,000 or, in case of a legal entity, 5% of gross turnover for the latest financial year, subject to a maximum of €300,000. The financial penalties are collected as State debts.

Article 50 of the law refers to Articles 226.16 to 226.24 of the French Criminal Code which set out those acts relating to the processing of personal data which are criminal offences. The following are examples.

> From Article 226.18
>
> “The collection of data by fraudulent, unfair or unlawful means, or the processing of name-bearing information relating to a natural person despite this person's opposition, where this objection is based on legitimate grounds, is punished by five years' imprisonment and a fine of € 300,000.”
>
> From Article 226.19
>
> “Apart from the cases set out by law, the recording or preserving in a computerised memory, without the express agreement of the persons concerned, of name-bearing data which, directly or indirectly reveals the racial origins, political, philosophical or religious opinions, trade union affiliations or the sexual morals of the subjects, is punished by five years' imprisonment and a fine of € 300,000.”

Other offences are punishable with less severe penalties.

11.2.3 United Kingdom

Section 43 of the law gives the supervisory authority the power to issue “information notices” requiring data controllers to provide specified information within a specified period. An information notice may be issued where the supervisory authority has received a complaint, or where the supervisory authority reasonably requires any information to

decide whether the data controller has complied with the substantive data protection rules[6].

Section 50 gives the supervisory authority the power, with the consent of the data controller, to assess processing for the following of good practice. If the supervisory authority wishes to carry out an investigation on the data controller's premises without consent, he must seek a warrant from a judge. Before a warrant may be issued, Schedule 2 to the law requires the judge to be satisfied that there are reasonable grounds for suspecting that the data controller has contravened the substantive data protection rules, or that an offence under the data protection law has been committed, and that evidence is to be found at the premises in question. A warrant entitles the supervisory authority, within seven days, to enter the premises, to search them, to inspect, examine, operate and test any equipment that is used for processing personal data, and to inspect and seize any documents or other material which may constitute relevant evidence. A warrant may only be issued if the judge is satisfied that the supervisory authority has previously given the data controller seven days notice in writing demanding entry, and that either access was unreasonably refused or the controller unreasonably refused to co-operate. The controller must be notified of the application for the warrant and must be given the opportunity of being heard by the judge.

Under section 40, if the supervisory authority is satisfied that a data controller has contravened the substantive data protection rules, he may serve the controller with an "enforcement notice". This requires the controller to take (or refrain from taking) such action as may be specified in the notice to remedy the breach. The action includes, but is not limited to, blocking, erasing or destroying personal data, or suspending processing.

Data controllers have a right of appeal to the Information Tribunal[7] against information notices and enforcement notices. Neither notice normally takes effect until the time for lodging an appeal has expired. However, in urgent cases either notice may specify that it is to take effect a minimum of seven days from the date on which it was issued.

Failure to comply with the substantive data protection rules is not a criminal offence. However, non-compliance with an information notice or an enforcement notice is a criminal offence. Other offences under the law include failure by data controllers to comply with the requirements for notifying the supervisory authority of the processing that they carry out, and unauthorised disclosure or obtaining of personal data. The supervisory authority has the power to prosecute the criminal offences created by the data protection law. The maximum penalty for most offences in the higher courts is an unlimited fine. Imprisonment is not available.

Under section 13, data subjects have the right to take (civil) court action to seek

---

[6] The UK law refers to compliance with the "data protection principles". However, in the UK law that term includes, in addition to the five principles set out in Article 6.1 of the Directive, the following duties on the controller: to ensure that processing has a proper legal base; to provide information pro-actively to data subjects; to respect individuals' rights; to provide proper security; and to comply with the requirements for the transfer of personal data to countries outside the European Union.

[7] The Information Tribunal is a judicial body that hears appeals against notices issued by the Information Commissioner under the Data Protection Act 1998. Its Chairman and Deputy Chairmen are legally qualified. Among its members are some who represent the interests of data subjects and some who represent the interests of data controllers. It can consider cases "on the papers" or in hearings. Its decisions may be appealed against, on points of law only, to the High Court. The Tribunal also hears appeals against notices issued by the Information Commissioner under the Freedom of Information Act 2000.

compensation for damage caused by any breach of the Act, and for any accompanying distress. Compensation for distress alone may be sought where the processing is for journalistic literary or artistic purposes. There is a defence where the controller can show that he took reasonable care to comply with the requirements of the Act.

Data subjects also have the right to take (civil) court action where the data controller has failed

- to comply with a subject access request;
- to rectify inaccurate data;
- to comply with a notice from the data subject requiring him to cease processing which would cause the individual substantial harm or substantial distress;
- to comply with a request from the data subject not to process the data subject's data for the purposes of direct marketing;
- to comply with a request from the data subject not to take certain fully automated decisions about the data subject.

In each case, the court may order the data controller to take the relevant action.

Unlike many of his EU counterparts, the Information Commissioner does not currently have the power to impose administrative fines. However, a recent amendment to the Data Protection Act 1998 will provide him with the power to impose fines for deliberate or serious breaches of the data protection principles. The maximum penalty will be set by the Government. At the time of writing this paper, the power was not yet in force.

11.3 Comment from the EU perspective

As is customary in European law, the Directive leaves the detailed arrangements for enforcing national data protection laws to be determined by the individual Member States. The arrangements, including the make-up and methods of working of the data protection supervisory authorities, vary widely across the Member States of the European Union.

Some supervisory authorities, as in France, are multi-person Commissions with a collegiate approach to decision-making. Others, as in the United Kingdom, comprise a single Commissioner who has sole responsible for decision-making under the law[8]. The number of staff also varies between over 100 in the United Kingdom, to no more than a handful in some of the smaller Member States. The powers of enforcement, and the manner in which they are exercised, reflect not only the disparate nature of the supervisory authorities themselves, but also the varied legal and administrative traditions of the Member States.

Similarly, the mix of administrative, civil and criminal legal sanctions varies considerably across the Member States. The provisions in each Member State's law will have been

[8] A recent report ("Data Sharing Review" published on 11 July 2008) of which the Information Commissioner was one of the joint authors, recommends that the supervisory authority should be reconstituted as a multi-member Information Commission.

drawn up in such a way as to mesh seamlessly with each country's underlying legal and institutional framework. Indeed, in some cases (including France, from among the examples given in this chapter) it is necessary to refer to other legal texts to find out the precise nature of the sanctions available.

Against this background there is, and can be, no single model of best practice for enforcement powers and procedures. What works well in one country may not be suitable for another with a differently constituted supervisory authority and a different legal system. The important thing is that the supervisory authority should have adequate powers to carry out its enforcement functions effectively. As a minimum the supervisory authority needs to have the powers identified in the Directive: to find out what is happening in a particular case or with a particular data controller; to take steps to put right any infringement that it discovers; to ensure that data controllers can be taken to court where necessary, where dissuasive sanctions, and compensation, should be available.

This chapter deals only with the supervisory authority's enforcement powers. It should be borne in mind, however, that the supervisory authority's functions go well beyond enforcement. The wide range of functions is well illustrated by Article 23 of the Portuguese law:

"1 - The CNPD *[the National Data Protection Commission]* is responsible in particular for:

(a) issuing opinions on legal provisions and on legal instruments in preparation in Community or international institutions relating to the processing of personal data;
(b) authorising or recording, as applicable, the processing of personal data;
(c) authorising in exceptional cases the use of personal data for purposes not giving rise to their collection, with respect for the principles laid down in Article 5 *[the data protection principles]*;
(d) authorising the combination of data processed automatically in the cases provided for in Article 9 *[special rules for the combination of personal data]* ;
(e) authorising the transfer of personal data in the cases provided for in Article 20 *[transfers to other countries]*;
(f) establishing the time for keeping the personal data according to their purpose, issuing directives for particular sectors of activity;
(g) ensuring the right of access to information and the exercise of the right of rectification and updating;
(h) authorising the establishment of costs or frequency for exercising the right of access and establishing the maximum periods for compliance in each sector of activity with the obligations which are incumbent upon the controller by virtue of articles 11 to 13;
(i) acting on an application made by any person or by an association representing that person concerning the protection of his rights and freedoms in regard to the processing of personal data and informing them of the outcome;
(j) checking the lawfulness of data processing at the request of any person whenever such processing is subject to restricted access or information, and informing the person that a check has taken place;
(k) assessing the claims, complaints or applications of private individuals;
(l) waiving the security measures according to Article 15 (2), issuing directives for particular sectors of activity;

(m) ensuring representation in joint supervisory proceedings and in Community and international meetings of independent personal data protection supervisory bodies, and taking part in international meetings within the scope of its responsibilities, in particular exercising representation and monitoring functions under the Schengen and Europol systems *[EU-wide legal instruments which include systems for exchanging information about crime]* according to the applicable provisions;
(n) deliberating on the application of fines;
(o) promoting the drawing up of codes of conduct and assessing them;
(p) promoting the disclosure and clarification of rights relating to the protection of data and periodically publicising its activity, in particular by means of the publication of an annual report;
(q) exercising other legally established responsibilities."

Particular attention should be drawn to paragraphs 1(i), (j) and (k), which deal with the supervisory authority's functions in relation to complaints and other requests which it receives from individuals about the processing of their personal data. One of the most important functions of the supervisory authority is to look after the interests of individuals. On the European model, the supervisory authority provides individuals with a readily accessible and inexpensive means of having their queries about the processing of their personal data investigated and any shortcomings put right. The courts have an important part to play, but, for an individual, taking court action can be intimidating and procedurally difficult, and is often costly. Moreover, dealing with complaints provides the supervisory authority with a rich source of intelligence about the activities of data controllers, and helps direct the thrust of its enforcement activities.

11.4 Comment from the Chinese perspective

As a saying goes: "No relief, no rights". When the information subject's rights are infringed by other parties, especially the information controller, some enforcement measures must be applied. As to how they should be applied, the EU (including its Member States) follows the judicial and administrative model, where the supervisory power is exercised by judicial and administrative organs. The United States of America, on the other hand follows a self-regulatory (or decentralized) model, by which the activities of personal information processors are supervised chiefly by trade associations. How to lay down the enforcement system in China should depend on the legal system and general situation of this country. Considering the statute-and-public-power-based tradition in China, the enforcement arrangements for a future Chinese information protection law should ensure that the enforcement body has adequate powers of investigation and enforcement and to bring cases to court. Therefore, the judicial and administrative model should be the ultimate choice for China. Drawing up a personal information protection law is likely to take a long time, and the judicial and administrative supervisory system can not be established in the short term. During this period of time the self-regulatory (or decentralized) model may play an important part.

In order to improve the effect and efficiency of judicial remedies in settling cases involving personal information protection in China, several measures should be taken. Of most importance, specific administrative bodies which have adequate powers of investigation

and enforcement and to bring cases to court should be established to supervise the activities of personal information processors. In addition, in hearing disputes involving personal information processing, the courts, lawyers and principals should abide by special litigation rules such as a requirement to keep personal information secret.

Recommendation (EU-Perspective): The enforcement arrangements for a future Chinese data protection law should ensure that the enforcement body has adequate powers of investigation and enforcement and to bring cases to court. The enforcement body should also be responsible for dealing with complaints and other requests from individuals. The courts should have the power to impose dissuasive sanctions and order compensation.
Recommendation (CH-Perspective): The judicial and administrative model should be the ultimate choice for China. There should be special administrative bodies with adequate powers of investigation and enforcement and to bring cases to court. While these arrangements, which will take time to implement, are being set up, enforcement should be achieved by self-regulation.

12 The Legal Status and Functions of Codes of Conduct

12.1 The Directive

Article 27 of the Directive requires the Member States to promote the preparation of codes of conduct by trade associations and other bodies, and to provide for the data protection supervisory authorities to be able to consider draft codes of conduct which are submitted to them.

> "1. The Member States … shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.
>
> 2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.
>
> Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the

> national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives."

Article 27 contains a further paragraph which sets the procedure for the consideration of EU wide codes of conduct drawn up by the European Commission.

12.2 Member States' laws

Not all Member States' laws deal expressly with codes of conduct. Among those that do, some do little more than state that organisations may prepare codes of conduct and that the supervisory authority may review them. An example is Section 42 of the Finnish law:

> "Controllers or their representatives may draft sectoral codes of conduct for the application of this Act and the promotion of good processing practice, and send these to the Data Protection Ombudsman. The Data Protection Ombudsman may check if the code of conduct is in conformity with this Act and the other provisions relating to the processing of personal data."

A few laws make more elaborate provision. The Irish law, in particular, deals in a very thorough way with what it refers to as "codes of practice" (which is the more commonly used term in English for instruments of this kind). Section 13 of the law puts a duty on the supervisory authority to encourage the relevant bodies to prepare codes of practice; to consider codes that have been submitted to it, in consultation as appropriate with the relevant bodies and representatives of data subjects; if it finds that the codes provide "a measure" of data protection that is in conformity with the data protection law, to approve the codes and to encourage their dissemination to the data controllers concerned.

Going beyond the strict requirements of the Directive, Section 13 of the Irish law also empowers the supervisory authority, after consultation as mentioned above, to draw up codes itself and to disseminate them as appropriate. It also provides for any code that has been approved by the supervisory authority to be laid before Parliament by the Minister. If approved by both Houses of Parliament, the code has the force of law and is regarded as subordinate legislation. Section 13 also expressly provides that codes that have been approved by the supervisory authority may be taken into account in court proceedings.

In addition to placing on the supervisory authority the duty to encourage the preparation of codes of conduct and to verify their compliance with the data protection law, Section 12 of the Italian law makes the supervisory authority responsible for having the codes published in the Official Journal of the Italian Republic, and requires the codes to be included in Annex A to the law, by Ministerial decree. At the time of the preparation of this paper, codes on the following topics appeared in Annex A.

- Processing of personal data in the exercise of journalistic activities.
- Processing of personal data for historical purposes.
- Processing of personal data for statistical purposes within the framework of the

national statistical system.
- Processing of scientific data for statistical and scientific purposes.
- Information systems managed by private entities with regard to consumer credit, reliability, and timeliness of payments.

Section 12 of the Italian law also specifies that compliance with the codes is "…a prerequisite for the processing of personal data by public and private entities to be lawful."

Section 51 of the United Kingdom law provides for the supervisory authority, like its Irish counterpart, to draw up codes itself, in consultation with the relevant interests, as well as considering those prepared by representative bodies. However, the law stops short of providing for codes that have not been prepared by the supervisory authority to be formally "approved" by the supervisory authority. It merely empowers the supervisory authority to notify the relevant body whether in the supervisory authority's opinion "…the code promotes the following of good practice". The codes so far drawn up by the supervisory authority include the following:

- Framework code of practice for sharing personal information.
- Employment practices' code.
- Quick guide to the employment practices code: ideal for small businesses.
- Code of practice on telecommunications directory information and fair processing.
- CCTV code of practice.

12.3 Comment from the EU perspective

The reasons why some Member States data protection laws do not include express provision relating to codes of conduct are not clear. What does seem clear, however, is that the use of codes of conduct as quasi-legislative instruments is more common in the public administration at large in some Member States than in others. This is, perhaps, reflected in the varied provision that is made in Member States' data protection laws.

Codes of conduct can play a useful part in supporting legislation by setting out good practice measures for specific sectors or kinds of activity that can give much more detail than is possible with a law of general application. By ensuring that the relevant trade bodies or other interests are actively involved in drafting the codes, or are at least consulted when the codes are prepared by the supervisory authority, the likelihood of securing compliance with the codes' recommended practice is likely to be strengthened. This will also thus strengthen compliance with data protection law.

The legal status of codes varies across the Member States. Some Member States, as in the United Kingdom, stop short of empowering the supervisory authority formally to approve codes that have been prepared by representative bodies. In other Member States formal approval by the supervisory authority is possible, without that approval necessarily giving the codes anything other than an advisory status: in other words, it is advisable to comply with the code, but failure to do so does not necessarily mean failure to comply with the law. This is perhaps the position with Article 11(3)(c) of the French law which empowers the supervisory authority to deliver a "quality label" to data protection products or procedures submitted to it when the supervisory authority finds them to be in

conformity with the data protection law. (Article 11 of the French law does not expressly refer to codes of conduct but the language suggests that they are included.) The Irish law, on the other hand, contains a provision which allows, although it does not require, "approved" codes of practice to be included formally within the body of data protection statutory law. This would appear to mean that failure to comply with the codes of itself constitutes a sanctionable breach of the data protection rules. The Italian law, by including codes of conduct in one of the Annexes to the data protection law, seems to have a similar effect. Which of these approaches is right for a particular country will depend upon the precise effect that it is desired to achieve, as well as the country's wider legal and administrative traditions.

12.4 Comment from the Chinese perspective

Similarities exists between the themes of chapters 11 and 12, that is how to implement the rules of personal data protection, in the way of law-making by government or self-regulation by private sectors. China should make a compromise by laying out statutes and, in the meantime, reinforcing self-regulative rules. When adopting codes of conduct as well as self-regulative rules, the administrators and judges should prevent some terms in these codes and rules that are unfair to personal data subjects taking effect.

Recommendation: Careful consideration should be given to the advantages for sectoral compliance with data protection rules that can be achieved by using codes of conduct, and to the inclusion of a provision in any future Chinese law allowing codes of practice to be prepared.

13 Disclosure and matching of personal data by public sector bodies

13.1 The Directive

With the exception of the provisions on transfers of personal data to third countries and direct marketing, neither of which is dealt with in this chapter, the Directive contains no substantive rules expressly regulating the disclosure or matching[9] of personal data. The

[9] In this paper "disclosure" means making personal data available to the public or a third party, by whatever means this is done. Member States' laws use a variety of terms (for example, exchange, sharing, transfer, dissemination, communication) to describe this activity. "Matching", which is taken to mean bringing together

definition of “processing” includes both disclosure and matching. This means that the general rules in the Directive apply to these activities. In particular the activities must be carried out consistently with the data protection principles. The disclosure and matching of personal data may often not be among the purposes for which the data were collected by the data controller. The second data protection principle, which requires the further processing of personal data not to be “incompatible” with the purpose for which the personal adapt were collected, is, therefore, especially important where data controllers wish to disclose or match personal data. It means that among the criteria that controllers have to apply is whether the intended disclosure or matching is “compatible” with the purpose for which the data controllers collected the data.

13.2 Member States’ laws

13.2.1 Disclosure

Like the Directive, most Member States’ laws contain no special rules of general application governing disclosures. However, some make provision for specific cases. For example, Part 5 (Sections 15 to 18) of the Danish law regulates the disclosure to credit information agencies of data on debts to public authorities. It permits disclosures only where they are required by law or regulations and where certain specified criteria relating to the debts themselves are met. The law specifies the information that the public authority must give the debtor in writing at least four weeks in advance of the proposed disclosure.

Hungary is among the minority of Member States whose laws deals expressly with disclosures in a provision of general application. Article 8 permits disclosures only where the data subject has consented and the general conditions for processing are met.

Section 19 (2) of the Italian law permits disclosures by one public body to another if the disclosures are provided for by laws or regulations, or if the disclosures are necessary to discharge institutional tasks and 45 days advance notice of the disclosures has been given to the supervisory authority.

Article 11 of the Spanish law establishes the general rule that disclosures are permitted “…only for purposes directly related to the legitimate functions of the transferor and transferee with the prior consent of the data subject”. It specifies a number of circumstances in which the requirement for consent is lifted. Article 21 makes more specific provision for disclosures between public sector bodies. Paragraphs 1 and 2 say:

> “1. Personal data collected or drawn up by public administrations in the performance of their tasks shall not be communicated to other public administrations for the exercise of different powers or powers relating to other

---

two or more data sets, may be carried out by a single data controller, and does not necessarily involve disclosure. Various terms, including “combination” and “inter-connection”, are used in Member States’ laws to refer to this process.

matters unless the communication is for the purpose of subsequent processing for historical, statistical or scientific purposes.

2. Personal data which a public administration obtains or draws up on behalf of another administration may be communicated."

The article makes clear that the requirement for consent in Article 11 does not apply in these circumstances.

The German law makes detailed provision for the disclosure of personal data by public sector bodies. Section 15 sets rules for disclosures by one public sector body to another. It permits such a disclosure if it is necessary for the performance of the duties of either the disclosing body or the receiving body, and the general rules on processing set out in Section 14 are complied with. It specifies which of the bodies is responsible for determining whether the disclosure is lawful. It permits the recipient body to process the data only for the purpose for which they were disclosed, unless the data subject has consented to processing for other purposes. Where personal data that may be disclosed are inseparably linked to other personal data, Section 15 permits the disclosure of the additional data also, unless the data subject or a third party has an overriding interest in their not being disclosed. The law specifies that the additional data may not be used by the recipient party.

Section 16 deals with the disclosure of personal data by a public sector body to a private sector body. It permits such a disclosure if it is necessary for the performance of the duties of the disclosing body, and the general rules on processing set out in Section 14 are complied with. Disclosure may also be made if the recipient body "credibly proves a justified interest" in the data to be disclosed and the data subject does not have a legitimate interest in preventing the disclosure. Responsibility for the disclosure lies with the disclosing body. The disclosing body must inform the data subject of the disclosure, unless either he will come to know about it in another way, or providing the information would jeopardize public safety or otherwise be detrimental to the State or a Province. The disclosing body may use the personal data only for the purpose for which they were disclosed, and there is a duty on the disclosing body to inform the recipient body of this condition.

13.2.2 Matching

As with disclosures, only a minority of Member States' laws make express provision for matching.

Article 8 of the Hungarian law, referred to above in connection with disclosures, also applies to matching.

Article 8 of the Cypriot law regulates the "combination of filing systems". It requires every proposal for "combination" to be notified to the supervisory authority. This is to be done jointly by the data controllers concerned if the "combination" involves more than one controller. In some circumstances, for example where sensitive data are involved, a licence from the supervisory authority is required. Article 8 requires the views of the

controllers to be heard and specifies the contents of the licence. These include the purpose of the "combination", the categories of data involved, the length of time for which the "combination" is permitted and any additional conditions to safeguard individuals rights and liberties, especially their privacy. The supervisory authority is required to maintain a "register of combinations".

Broadly similar provision is made in Article 8 of the Greek law.

Article 9 of the Portuguese law also requires authorization by the supervisory authority if the "combination" is not provided for in a legal provision. Paragraph 2 specifies that:

> "The combination of personal data must be necessary for pursuing the legal or statutory purposes and legitimate interests of the controller, must not involve discrimination or a reduction in the fundamental rights and freedoms of the data subjects, and must be covered by adequate security measures and take account of the type of data [that are] subject to combination. "

Article 16 of the law of Luxemburg is similar. It goes on to say that

> "Combination is authorised only where the fact that the filing systems are for the same or related purposes and the professional secrecy to which the controllers are bound, where applicable, are respected. "

Chapter 6 of the Slovenian law deals with what it calls the "linking" of filing systems from official records and public books. Article 84 permits linking only where it is provided for by statute. The data protection supervisory authority must be informed of linking, whether by a single controller or by more than one controller, of two or more filing systems kept for different purposes. If sensitive data are involved, or if the linking requires the use of the same "connecting code", the prior permission of the supervisory authority is required. Article 85 prohibits the linking of filing systems involving criminal records.

13.3 Comment from the EU perspective

The disclosure and matching of personal data are both aspects of processing and thus regulated by the general data protection rules. Most Member States' laws rely on these general provisions to achieve the desired level of regulation rather than making special provision. As noted above, the data protection principles, and in particular the requirement for further processing not to be incompatible with the purpose for which the data were collected, have an important part to play. A drawback with relying on this approach, which applies to all other forms of processing and not just to disclosures and matching, is that it is difficult to give a clear meaning to the word "incompatible". Moreover, there is little or no jurisprudence on the point. A heavy weight of responsibility is, therefore, placed on data controllers in deciding in a particular case whether the disclosure or matching that they intend to carry out meets the requirements of the data protection principles, and, in particular, the test of "compatibility". It may be tempting to overcome this difficulty and ease data controllers' decision-making by setting out in legislation specific rules governing disclosures and matching. However, disclosures, in

particular, are very common and, if they are not to disrupt routine business disproportionately, any specific rules should, as a consequence, be capable of being readily understood and applied. In this connection, it is perhaps significant that the German law, which contains the most detailed special rules for disclosures, does not impose a requirement for the individuals' consent to the disclosures.

The matching of two or more data sets can be seen as posing a particular threat to information privacy. Among the reasons for this is that by merging personal data from different sources, misleading conclusions can sometimes be drawn. Article 20 of the Directive requires processing operations that are likely to prevent specific risks to the rights and freedoms of data subjects to be checked before they begin. The Directive leaves it to Member States to determine which categories of processing are subject to this prior check. While some have chosen to apply this process to matching, most have not felt it necessary to do so.

It is worth noting in passing that the topic of the disclosure of personal data by public bodies, and in particular the "sharing" of personal data among public bodies, has been the subject of extensive debate in the United Kingdom for several years. The matter goes well beyond data protection law and involves other aspects of common and statute law. In the autumn of 2007 the United Kingdom Government established a review of the use and sharing of personal information and the protections that apply when such information is shared. The Information Commissioner, the United Kingdom's data protection supervisory authority, was one of the joint heads of the review. The report of the review, which was published in July 2008, made a number of recommendations for improving the law and "culture" relating to data sharing within the United Kingdom, including strengthening the powers of the Information Commissioner.

13.4 Comment from the Chinese perspective

In a wider definition, if a data controller shares personal data with another controller, that is a also being considered "disclosure", although the data are not available to the public. In a narrow definition, the term "disclosure" means to make personal information open to the public, and the term" "matching" means to correlate and compare two or more information sets stored by computer information bases for special purposes. Since the definition of "processing" means to collect and use personal information by storing, using, disclosing, matching and any other legal measures, "disclosure" and "matching" can be included in "processing" in a logical sense. However, it is worth noting that both disclosure and matching can be seen as posing a particular threat to information privacy. By "disclosing" information, processors place the individual's privacy in the public domain (if the narrow definition of "disclosure" is being applied); on the other hand, by matching personal information from different sources, the public will make misleading or wrong conclusions related to the public.

Therefore, special rules regulating information processing and matching are essential – as is a clear definition of the terms used, in particular when an act of handling data constitutes "disclosure".

Recommendation (EU-Perspective): With a data protection law that has a definition of “processing” that covers disclosures and matching and that enshrines the data protection principles on the European model, special rules for disclosure and matching are not necessary. If China decides to introduce special rules, it should take care to ensure that they can be operated without disproportionately disrupting routine business.
Recommendation (CH-Perspective): Considering the theory and comparative law rules, the principle and rules on rights, obligations and duties in information processing should be applied to information disclosure and matching in future Chinese personal information protection law. Special rules are also necessary. They include but are not limited to the authorization and supervising by the supervisory authority and processors specific duties such as informing subjects and compensating in due conditions. Some rules of U.S. Computer Matching and Privacy Protection Act of 1988 and Computer Matching and Privacy Protection Amendments Act of 1990 can be adopted by Chinese legislators on condition that they are compatible with the tradition of the civil law family.

14 Outsourcing of data processing in the public sector

14.1 The Directive

The relationship between the data controller and any sub-contractor (known in the Directive as a “processor”) whom he may use to carry out processing on his behalf is dealt with in Article 17 of the directive. Where the controller uses a processor, Article 17 requires the controller to choose one who provides sufficient guarantees of technical and organisational security. There must be a written contract between the controller and the processor. The contract must require the processor only to act on instructions from the controller and to respect the security requirements set out in Article 17. The processor, as well as the controller, will thus be legally responsible for ensuring adequate security. These rules apply both to the public sector and to the private sector.

14.2 Member States' laws

All Member States' laws have provisions giving effect to the Directive's requirements, and most do no more than that. An example is Article 14 of the Portuguese law:

> "1 [ ]
> 2 – Where processing is carried out on his behalf the controller must choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures.
> 3 – The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller and that the obligations referred to in 1 shall also be incumbent on the processor.
> 4 – Proof of the will to negotiate, the contract or the legal act relating to data protection and the requirements relating to the measures referred to in 1 shall be in writing in a supporting document legally certified as affording proof."

Sections 10 and 11 of the Austrian law go into rather more detail than many other laws.

> "**10** (1) Controllers may employ processors for their data applications insofar as the latter sufficiently warrant the legitimate and secure use of data. The controller shall enter into agreements with the processor necessary therefore and satisfy himself that the agreements are complied with by acquiring the necessary information about the actual measures implemented by the processor.
>
> (2) [ ]
>
> **11** (1) Irrespective of contractual obligations, all processors have the following obligations when using data for a controller:
>
> 1. to use data only according to the instructions of the controller; in particular, the transmission of the data used is prohibited unless so instructed by the controller;
> 2. to take all required safety measures pursuant to section14 *[which sets the security requirements]*; in particular to employ only operatives who have committed themselves to confidentiality vis-á-vis the processor or are under a statutory obligation of confidentiality;
> 3. to enlist another processor only with the permission of the controller and therefore to inform the controller of this intended enlistment of another processor in such a timely fashion that the controller has the possibility to object;
> 4. - insofar as this is possible given the nature of the service processing - to create in agreement with the controller the necessary technical and

organisational requirements for the fulfilment of the controller's obligation to grant the right of information, rectification and erasure;

5. to hand over to the controller after the end of the service processing all results of processing and documentation containing data or to keep or destroy them on his request;
6. to make available to the controller all information necessary to control the compliance with the obligations according to sub-paragraphs. 1 to 5.

(2) Agreements between the controller and the processor concerning the details of the obligations according to paragraph 1 shall be laid down in writing to perpetuate the evidence."

The requirement for the processor to return to the controller, or to destroy, all personal data and supporting documentation at the end of the contract is found in a number of Member States' laws, including Article 12 of the Spanish law. Article 12.4 of that law also makes clear that if the processor processes personal data in away that does not respect the contract, he is considered to be a controller and liable accordingly:

> "4. If the processor uses the data for another purpose, communicates them or uses them in a way not in accordance with the terms of the contract, he shall also be considered as the controller and shall be personally responsible for the infringements committed by him."

This would, presumably, be the case in any event, but spelling the position out in the law makes it clear. A processor who found himself in this position would be exposed to action both for having breached his contract with the original controller, and for any of the duties of a controller which he had not respected.

Another variant on the Directive's requirements is found in Article 8 of the Czech law, which requires the processor to inform the controller where the processor finds that the law is being breached.

> "If the processor finds out that the controller breaches the obligations provided by this Act, the processor shall be obliged to notify the controller of this fact without delay and to terminate personal data processing. If he fails to do so, the processor and the data controller shall be liable jointly and severally for any damage incurred by the data subject. This shall in no way prejudice his responsibility pursuant to this Act."

14.3 Comment from the EU perspective

The model for the controller/processor relationship in the Directive is a very simple one. The controller is responsible in law for all aspects of the processing of personal data, including things done, or not done, by the processor. This means that action can be taken against the controller, rather than against the processor, for any breach of the data protection law by the processor. The only independent liability that the processor carries in his own right is for compliance with the security requirements of the data protection law. Both the controller and the processor are responsible for ensuring proper security. This attribution of responsibility applies also where the processor is in a third country. Thus, if

a breach of the data protection law of the Member State in which the controller is established is committed by a processor in a country outside the EU, action can be taken against the controller in the EU Member State in which he is established. This is an important safeguard for individuals, since it means that in seeking a remedy they may do so in what is likely to be their own country rather than have to engage with the legal system of a foreign country.

14.4 Comment from the Chinese perspective

Outsourcing of information processing is a newly emerging issue throughout the world and loopholes exist in Chinese regulations. Although the EU model for the relationship between the controller and the processor is a simple one, it is not compatible with the tradition of Chinese legislation. The right of personal information protection is absolute and can be exercised against all the social parties, including the controller and the processor, Therefore, under a Chinese personal information protection law neither of them should be exempted from the rules of obligations and duties. From this point of view, for any breach of the information protection law by the processor, action can be taken against not only controller for breach of contract but also the processor for the reason of tort. Only in this way can legislators provide the necessary safeguards for individuals to seek a remedy.

Recommendation (EU-Perspective): The simple model in the Directive should be followed.
Recommendation (CH-Perspective): Where there is a breach of the rules by a processor, action should be capable of being taken against the processor as well as the controller.

15 Health Data

15.1 International Instruments

15.1.1 The Directive

For the purposes of the Directive, “data concerning health” (a term which is not further defined) comprise one of the categories of what are generally known as sensitive data. Article 8.1 lists the categories of sensitive data and imposes a general prohibition on their being processed. Paragraphs 2 and 3 then set out circumstances in which the prohibition is lifted. Both paragraphs apply to all categories of sensitive data mentioned in paragraph 1. Paragraph 2(a) permits the processing of sensitive data, including health data, if the

data subject has given "explicit" consent. Paragraph 3 has particular relevance to health data. It says:

> "Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy."

Paragraph 4 of Article 8 allows Member States to lay down, either by law or by decision of the supervisory authority, other circumstances in which the processing of sensitive data, including health data, is permitted.

The Directive makes no further express provision in respect of health data.

15.1.2 Council of Europe Recommendation on the Protection of Medical Data

Like the Directive, the Council of Europe Convention includes "personal data concerning health" among the categories of sensitive data set out in Article 6. That article says only that domestic law must provide "appropriate safeguards" for the processing of such data.

The rules governing the processing of health data are amplified in Recommendation No. R(97)5 on the Protection of Medical Data[10]. Although the Recommendation uses the term "medical data", the definition of that term in Principle 1 makes clear that it is intended to cover "personal data concerning health".

> " the expression "medical data" refers to all personal data concerning the health of an individual. It refers also to data which have a clear and close link with health as well as to genetic data".

The Recommendation sets out detailed rules governing various aspects of the processing of health data. Among other things they cover: the rules that should be applied to the collection and further processing of health data; the information about the processing of health data that should be given to the data subject; consent; the communication (or disclosure) of health data; the rights of the data subject; security; the conditions for the retention of health data for periods longer than necessary for the purpose of their collection; transfers of health data to third countries; research. In some instances, the rules that apply to genetic data differ from those applying to other health data.

[10] As their name suggests, Council of Europe Recommendations are not legally binding instruments.

15.2 Member States' laws

15.2.1 General

Most Member States' laws do not define "health data", although some expand that term a little. Section 2(e) of the United Kingdom law uses the expression "physical or mental health or condition". Section 11(4) of the Finnish law refers to "the state of health, illness or handicap of a person or the treatment or other comparable measures directed at the person". Article10.1 of the Lithuanian law applies to "Personal data on the person's health (its state, diagnosis, prognosis, treatment etc.)". Like the Council of Europe Recommendation, Article 2(f) of the Luxembourg law specifies that genetic information is included: "health data" *[means]* any information about the data subject's physical or mental state, including genetic information". Article 6.19 of the Slovenian law lists all the categories of sensitive data, which include information about "health status", and adds the following rider: "biometric characteristics are also sensitive personal data if their use makes it possible to identify an individual in connection with any of the aforementioned circumstances".

On the substance of the rules, most Member States' laws do little more than follow the general approach adopted in the Directive. In other words, they permit the processing of all categories of sensitive data in the circumstances set out in Article 8.2 and 3 of the Directive, and, in some cases, set additional circumstances in which sensitive data may be processed. They do not contain separate rules for health data. The following are among the exceptions.

15.2.2 The Netherlands

Article 21 of the Dutch law is worth quoting in full as it shows the range of circumstances in which it may be necessary to process health data, and the sort of safeguards that can be applied. Article 21 applies in addition to Article 23 which sets out the general rules from the Directive.

> "**Article 21**
>
> 1. The prohibition on processing personal data concerning a person's health, as referred to in Article 16 *[the general prohibition on processing sensitive data]*, does not apply where the processing is carried out by:
> a. medical professionals, healthcare institutions or facilities or social services, provided that this is necessary for the proper treatment and care of the data subject, or for the administration of the institution or professional practice concerned;
> b. insurance companies as referred to in Article 1(1)(h) of the Insurance Supervision Act 1993, insurance companies as referred to in Article 1(c) of the Funeral Insurance Supervision Act, and intermediaries and sub-agents as referred to in Article 1(b) and (c) of the Insurance Mediation Act, provided that this is

necessary for:
1º. assessing the risk to be insured by the insurance company and the data subject has not indicated any objection thereto, or
2º. the performance of the insurance agreement;
c. schools, provided that this is necessary with a view to providing special support for pupils or making special arrangements in connection with their state of health;
d. institutions for probation, child protection or guardianship, provided that this is necessary for the performance of their legal duties;
e. Our Minister of Justice, *[in other words, the Minister of Justice of the Netherlands]* provided that this is necessary in connection with the implementation of prison sentences or detention measures, or
f. administrative bodies, pension funds, employers or institutions working for them, provided that this is necessary for:
1º. the proper implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the state of health of the data subject, or
2º. the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.
2. In the cases referred to under (1), the data may only be processed by persons subject to an obligation of confidentiality by virtue of office, profession or legal provision, or under an agreement. Where responsible parties personally process data and are not already subject to an obligation of confidentiality by virtue of office, profession or legal provision, they are required to treat the data as confidential, except where they are required by law or in connection with their duties to communicate such data to other parties who are authorised to process such data in accordance with (1).
3. The prohibition on processing other personal data, as referred to in Article 16, does not apply where this is necessary to supplement the processing of personal data concerning a person's health, as referred to under (1)(a), with a view to the proper treatment or care of the data subject.
4. Personal data concerning inherited characteristics may only be processed, where this processing takes place with respect to the data subject from whom the data concerned have been obtained, unless:
a. a serious medical interest prevails, or
b. the processing is necessary for the purpose of scientific research or statistics.
In the case referred to under (b), Article 23(l)(a) *[the data subject's consent]* and (2) *[safeguards for processing of sensitive data for research purposes]* shall likewise be applicable."
5. More detailed rules may be issued by general administrative regulation concerning the application of (1)(b) and (f)."

Paragraph 4 deals with data concerning inherited characteristics. Since this provision is found in an article which otherwise deals only with health data, this suggests that genetic data are considered to be included among health data.

15.2.3 France

Article 8 of the French law sets the general rules for the processing of sensitive data,

including health data, on the model of those in the Directive. However, this provision is complemented by more detailed rules that apply in specific circumstances.

Chapter IX (Articles 53 to 61) of the French law deals with the "Processing of Personal Data for the Purposes of Medical Research". (It should be noted that this chapter applies to all personal data, and not just to health data. However, it may be assumed that many of the data will be health data.) Article 54 requires each proposal for medical research to be considered by an expert advisory committee and authorized by the data protection supervisory authority. Article 55 sets the conditions under which health-care professionals may disclose personal data for the purposes of medical research. Article 56 deals with issues of confidentiality, consent and the personal data of dead people. Article 57 sets out the information that must be given to individuals before their personal data are processed for the purposes of medical research. Article 58 deals with persons who lack legal capacity. The remaining provisions in the chapter deal with procedural matters.

Chapter X (Articles 62 to 66) deals with the "Processing of Personal Medical Data for the Purposes of Evaluation or Analysis of Care and Prevention Practices or Activities". (In other words, it deals with the evaluation of the effectiveness of treatment and prevention measures.) Article 63 sets the general rule that specified categories of health data may only be disclosed for these purposes in an anonymised form. Otherwise the authorisation of the data protection supervisory authority is required, and even then the names or identification numbers of the individuals may not be used. Articles 64 and 65 deal with the supervisory authority's procedures in assessing requests for authorization. Article 66 says that processing authorized by the supervisory authority may not be used for the purpose of finding or identifying individuals. It specifies that results of evaluation or analysis may not be published or otherwise disclosed if they permit the identification of individuals.

15.2.4 Italy

Like other Member States' laws, the Italian law contains general rules for the processing of all sensitive data, including health data. However, it has separate rules for the public sector and the private sector. Among the general rules that apply to the public sector, Section 22 makes limited special provision for health data. Paragraphs 6 and 7 specify that such data held in lists, registers or data banks must be encrypted; and paragraph 8 says that health data may not be "disseminated". Similarly, Section 26.5, which deals with processing by the private sector, says that health data may not be "disseminated".

Title V (Articles 75 to 110) of the Italian law makes extensive provision for the "Processing of Personal Data in the Health Care Sector". (Again, it should be noted that like Chapter IX of the French law, this Title applies to all personal data, and not just to health data, although some provisions apply only to health data.) Section 76 says that health care professionals and health care bodies may process health data either with the data subject's consent, if the processing is "indispensable to safeguard the data subject's bodily integrity and health", or if authorized by the data protection supervisory authority. Sections 77 to 80 make special arrangements for the provision of information by different health care professionals and bodies to data subjects about the processing of their personal data. Section 81 establishes a simplified procedure for giving consent to the processing of health data. Section 82 makes special provision in relation to the giving of

information to data subjects and the granting of consent in the case of medical emergencies. Section 83 establishes further rules to protect data subjects' rights. Section 84 requires heath care professionals and bodies to communicate health data to data subjects only through the intermediary of a doctor, or, in some situations, another health care professional. Sections 85 and 86 designate certain purposes within the health care sector as being "in the substantial public interest", (thus permitting sensitive data to be processed for these purposes). Sections 87 to 89 deal with medical prescriptions. Section 90 deals with genetic data. It permits such data to be processed only with the specific authorization of the data protection supervisory authority, which is required to consult the Minister of Health, who, in his turn, must seek the opinion of the Higher Health Care Council. The remaining provisions cover a variety of miscellaneous matters.

15.3 Comment from the EU perspective

Like other international data protection legal instruments, the EU Directive classes health data as one category of sensitive data, whose processing is subject to tighter rules than those that apply to non-sensitive data. However, the Directive does not single out health data for any special treatment, as compared with other categories of sensitive data. Nor, for the most part, do EU Member States' data protection laws. In most Member States' laws no significant special provision is made, and the processing of health data is subject to the general rules that govern the processing of all categories of sensitive data. The most notable exceptions are outlined earlier in this chapter. Some further exceptions that apply to the exercise of the subject access right in respect of health data, are mentioned in Chapter 8.2.1.

One of the circumstances in which the Directive and Member States' laws permit the processing of sensitive data, including health data, is if the data subject has given his "explicit" consent. In this connection, it should be emphasized that, in the context of the provision of medical treatment to the data subject, data protection consent should not be confused with consent to treatment. If an individual consents to the processing of his data, that does not mean that he consents to treatment. Consent to treatment must be sought separately.

Health data and individuals' perception of privacy are closely bound up. Many people consider information about their health to be among their most "private" personal data. Surveys consistently put health data at or very near the top of lists of categories of personal information that individuals feel are the most sensitive. That is unsurprising given the very intimate nature of some information about the illnesses and other conditions that some people suffer from. However, not all information about ill-health is particularly sensitive. For example, when a school records that a child is absent because he has a cold, the school is processing health data. Yet the risks to privacy from the processing of that information are slight. Moreover, it should not be forgotten that "health" is not just about illness. Information about good health also technically comes within the scope of the term "health data". So, for example, an individual who completes a questionnaire about his health by saying that he suffers from none of the illnesses mentioned on the form is providing health data.

Health data are not processed only by doctors and other health care providers for the purpose of treating patients or for carrying out medical research. As the extract from the

Dutch law quoted above shows, there are many circumstances outside the health care sector where health data need to be processed. One example is the insurance sector, where information about individuals' health is often relevant to the insurance companies' assessment of risk. In this context genetic data are particularly sensitive, since genetic information can be used with greater reliability than other information as a predictor of future health. Armed with that information, insurance companies are in a very powerful position in determining whether or not to grant particular types of insurance. A result could be that no insurance company was willing to provide life assurance to individuals whose genetic make-up showed them to have low life expectancy. In these circumstances, this form of processing of health data would not only be a significant detriment to the individuals concerned, it would also change the nature of the insurance market.

Other data controllers who have a legitimate need to process health data for some purposes include: employers; schools and other educational establishments; social workers; lawyers; courts; prisons; children's homes; old people's homes; immigration authorities; benefits agencies. There are doubtless many others.

15.4 Comment from the Chinese perspective

As is illustrated in this report, specific rules should be laid out concerning personal information processing in specific fields, and health care is one of them. However, not all personal information related to health care can be considered to be sensitive personal information. Take, for example, the sufferer's name, address, telephone number, and hobbies are non-sensitive personal information. Besides, sensitive personal information related to the field of health care and any others can be given special protection by the general rules governing sensitive personal information such as that the information subject should give his "explicit" consent before processing. In other words, specific issues in the field of health care should not necessarily be settled by laying out and applying special rules.

Recommendation (EU-Perspective): In considering whether special rules should be applied to the processing of health data, and, if so, what those rules should be, China should have regard to the varying degrees of sensitivity of health data, which depend on both the nature of the data and the purposes for which they are processed. China should bear in mind that health data need to be processed not just by health care professions, but also by many other categories of data controller.
Recommendation (CH-Perspective): It is advisable to apply the general rule of personal protection law to health care on the one hand, and apply some special rules in the medicine law to the protection of sensitive information on the other hand.

16 Financial Data

16.1 The Directive

The Directive makes no special provision as regards the processing of financial data[11].

16.2 Member States' laws

Like the Directive, Member States' laws make no special provision as regards the generality of financial data. However, some do make special provision for particular categories of financial data, mostly relating to credit and debt.

16.2.1 Prior Checking

It is a requirement of Article 20 of the Directive that Member States must specify processing "likely to present specific risks to the rights and freedoms of data subjects" and to require it to be checked in advance by the data protection supervisory authority. Member States are free to determine which categories of processing to specify. Some Member States have chosen to apply this prior checking requirement to certain categories of financial data. For example, Article 14(1)(d) of the Luxembourg law and Article 28.1(b) of the Portuguese law both require the prior authorization by the supervisory authority of processing relating to the credit status and solvency of data subjects. Article 31(1)(a) of the Hungarian law requires the prior checking of customer files of financial organisations or public utility providers.

16.2.2 Credit Information

A few Member States laws make more detailed provision in relation to personal data concerning credit and debt.

16.2.2.1 Denmark

As noted in Chapter 13.2.1 above, Part 5 of the Danish law regulates the disclosure to credit information agencies of data on debts to public authorities.

[11] For the purpose of this paper, "financial data" is taken to mean information relating to the financial situation of an individual.

Part 6 of the Danish law regulates credit information agencies. Section 19 defines a credit information agency as a "business involving processing of data for assessment of financial standing and creditworthiness for the purpose of disclosure of such data", and requires prior authorization of such processing by the data protection supervisory authority. Section 20 permits credit information agencies to process only data which by their nature are relevant for the assessment of financial standing and creditworthiness. It expressly prohibits the processing of sensitive data, including criminal history data. Data indicating lack of creditworthiness which are more than five years old may not be processed, unless they are of "decisive importance". Section 22 establishes special arrangements for subject access to data held by credit information agencies. Section 23 specifies how the data held by credit information agencies may be disclosed to subscribers to their service. Section 24 requires errors or misleading information to be corrected or erased "without delay", and Section 25 requires the data subject and third parties who received the erroneous information within the previous six months to be notified immediately. Section 26 deals with the procedure where data subjects seek rectification or erasure.

16.2.2.2 Finland

Section 20 of the Finnish law also deals with the processing of personal credit data. It specifies the categories of information about defaults in payment or performance that may be recorded by those engaged in credit data activity, and says that the data may be disclosed only to a controller engaged in credit data activity or to a person needing the data for purposes of granting credit or credit monitoring, or for another comparable purpose.

16.2.2.3 Italy

As noted in Chapter 12.2 above, Annex A to the Italian law contains a code of conduct and professional practice applying to information systems managed by private entities with regard to consumer credit, reliability, and timeliness of payments. This code of conduct sets out detailed rules governing every aspect of the processing of personal data in private credit information systems.

16.2.2.4 Lithuania

Article 16 of the Lithuanian law deals with the processing of personal data for the purposes of evaluation of a person's solvency and management of his debt. It permits the disclosure of personal data of debtors to data controllers who process "consolidated debtor files" (who are referred to in this paper as "debtor file controllers"). Debtor file controllers may process the data with a view to disclosing them to third parties with a legitimate interest in evaluating the solvency of the data subject and managing the debt. Processing by debtor file controllers is subject to prior checking by the data protection supervisory authority. Article 16 sets out the circumstances in which personal data about debt may be disclosed, and prohibits the disclosure of sensitive data, including information about criminal convictions. It also prohibits personal data about debt from being combined with personal data that are processed for other purposes. It specifies the information that the debtor file controller must provide to the data subject on receiving personal data about debt. Personal data about debt may not be processed for longer than ten years after the settlement of the debt. Finally, the article deal with the handling of

requests for loans made to banks and other financial institutions. It permits such institutions to exchange specified personal data about data subjects who have taken out loans from them in order to evaluate the solvency of the data subjects. Requests by these institutions for the disclosure of these data may only be made with the consent of the data subjects who have applied for loans. The data may not be stored by the receiving institution for more than two days, and must not be combined with other personal data.

16.2.2.5 Spain

Article 29 of the Spanish law also deals with credit information. It allows credit information agencies to process only personal data obtained from registers and sources accessible to the public and set up for that purpose or based on information provided by the data subject or with his consent. Processing is also allowed of personal data relating to the fulfillment or non-fulfillment of financial obligations provided by the creditor or by someone acting on his behalf. The article specifies the information that must be provided to data subjects in such cases, and sets out special arrangements for subject access. It also limits the personal data processed to those which are necessary for assessing the economic capacity of the data subjects and which, in the case of adverse data, do not go back for more than six years, always provided that they give a true picture of the current situation of the data subjects.

16.3 Comment from the EU perspective

Surveys show that people rank information about their financial circumstances alongside health data as being among the categories of personal data that they are most concerned about protecting. Unlike health data, however, financial data do not come within the definition of “sensitive data” for the purposes of the Directive or other international legal instruments. Nor, for the most part, do Member States’ data protection laws make special provision for the handling of financial data. Part of the reason for this may be that the financial services sector, in particular, is heavily regulated by other legislation.

The special rules that are found in the data protection laws of some Member States are concerned almost exclusively with the processing of personal data for the purposes of checking creditworthiness. This is clearly an area where intimate personal data are used to take decisions that can have far-reaching consequences for individuals, and it is important to ensure that the handling of the data is properly regulated. The fact that not all Member States’ data protection laws make special provision in this regard does not mean that data protection rules do not have an impact. In the United Kingdom, for example, the personal data handling practices of what are known as “credit reference agencies” have been significantly improved over the years under encouragement from the data protection supervisory authority in reliance on the general data protection rules. It should also be said, though, that the credit sector in the United Kingdom is heavily regulated by other legislation. This is also likely to be the case in other Member States.

Some Member States require the processing of certain financial data (again, mainly data relating to creditworthiness) to be checked by the data protection supervisory authority before the processing may begin. In effect, this is a requirement for the supervisory

authority to authorize the processing. As noted above, prior checking of certain categories of processing is a requirement of the Directive. However, Member States are free to choose to which categories of processing they apply the prior checking procedure. That the Directive does not itself specify those categories is significant. Had it been felt, for example, that processing for the purpose of assessing individuals' creditworthiness, or, indeed, other processing of financial data, inherently merited the prior authorization of the data protection supervisory authority, it seems likely that a general requirement to this effect would have been included in the Directive. Instead, no stipulation of this kind was made, and discretion was given to Member States. Many have clearly taken the view that prior authorization by the data protection supervisory authority of the processing of financial data, let alone the licensing of data controllers who process financial data, is not necessary. Those Member States which have legislated for prior checking in this sector, have done so in the light of domestic circumstances, having regard to the fact that any system of prior checking necessarily imposes a delay for the business activity in question. A judgment needs to be made whether the benefits to individuals' information privacy that might flow from a prior checking or licensing system, justify the additional regulation.

In addition to assessing creditworthiness, financial data are processed by many different categories of institutions for a wide range of purposes. Apart from purely cash transactions, much of the business carried out by retailers involves the processing of financial data of customers, and possibly also of suppliers. All employers process financial data about their employees for the purpose of paying them, and, in some Member States, for the purposes of assessing deductions for taxation, social insurance and trade union levies. Banks process financial data of their customers for the purpose of providing personal banking services and other facilities. The processing of financial data by insurance companies is, likewise, an integral part of their functions. Indeed, increasingly financial services institutions provide a range of banking, insurance and other services. In the public sector, taxation authorities and benefits agencies are just two prominent examples of institutions that process financial data. There are many more. Given the very wide range of purposes for which financial data are processed, the categories of data that need to be processed alongside the financial data will also be very varied. It is rare in any context, and not just as regards processing involving financial data, for the processing of specified categories of personal data to be prohibited. The data protection principles, which require personal data to be "adequate, relevant and not excessive" are normally sufficient to achieve the necessary effect.

16.4 Comment from the Chinese perspective

The term "financial information" refers to information relating to the financial situation of an individual. In general, the processing of personal information in the financial field should be regulated by the general rules in the information protection law. Information processing in various fields, whether they be health care, finance or social activity should abide by the principle of information protection, the rules on individuals' rights and the obligations of processors as well as the trans-border flow of personal information. Regulating these matters by way of laying down a unified statute can make legislation not only more efficient but also in line with the traditional rule of law-making in the civil law family. In the meantime, it is worth noting that some special matters related to finance, such as credit and debt, are linked with public interests and social affairs. Therefore some specific rules

should be laid out. Up to now, in China the law against money-laundering has been taken into effect, in pursuant to which the processors should abide by some specific rules in processing the personal information of their clients. These rules include the supervisory organ and its power as well as a time limitation on information processing. These rules can meet some urgent needs in combating money-laundering and the finance field. However, their drawbacks may be significant. On the one hand, further rules (especially that of individuals' rights) cannot go into effect or be enforced; on the other hand the sphere of effect is rather narrow since it excludes some important sub-fields of finance such as creditworthiness assessing.

Recommendation (EU-Perspective): China should consider whether, in the light of its domestic circumstances, special data protection rules are needed for the processing of financial data for the purpose of assessing creditworthiness. Prior checking of such processing, or, indeed, any other processing of financial data, by a data protection supervisory authority is not likely to be needed. The data protection principles provide the necessary degree of regulation for the generality of processing of financial data.
Recommendation (CH-Perspective): For the reasons given in the section headed "Comment from the Chinese perspective", specific provisions related to personal information in the field of finance are essential. These provisions may be placed in the unified personal information protection law and in some specific laws such as the law on banking and the law against money-laundering, which may include the supervisory agency and its power, special rights, obligations and duties in this field.

17 Data protection in social activity

17.1 The Directive

The rules which the Directive establishes are applicable to all activities. The Directive does not focus on the processing of personal data in particular sectors or for particular purposes. Specifically, it makes no special provision for processing in connection with social activity. (In this paper, "social activity" means the general ebb and flow of individuals' daily lives, and covers the range of circumstances in which individuals interact with each other and with institutions, for example while at work, while travelling or while engaging in leisure activities.) Perhaps the closest it comes is through the special provision made for processing for journalistic, artistic or literary purposes, so as to balance the right to privacy with the need to guarantee freedom of expression (Article 9); the requirement for individuals to be given the opportunity of opting in or opting out of their personal data being used for direct marketing purposes Article 14(b); and the requirement for individuals to be given the right not to be subjected to certain fully automated decisions (Article 15).

17.2 Member States' laws

In giving effect to the Directive in their national laws, most Member States have broadly followed the Directive's approach. For the most part, their laws apply in a uniform way to all processing of personal data, irrespective of the purpose for which the data are processed, the only special provision being that required or expressly permitted by the Directive. Some exceptions to this general approach have been noted in the chapters of this paper dealing with health data and financial data. Some other, very limited, exceptions are also found.

17.2.1 Data protection in the workplace

Employers are in a position to collect a great deal of personal data about their employees, and some Member States' laws expressly regulate this.

Finland has perhaps gone furthest in this respect. In addition to its general data protection law, it has a separate law entitled "Act on the Protection of Privacy in Working Life". The scope of that Act is set out in Section 2 (1).

> "(1) This Act lays down provisions on the processing of personal data about employees, the performance of tests and examinations on employees and the related requirements, technical surveillance in the workplace, and retrieving and

opening employees' electronic messages."

It is also worth quoting section 3 which makes very clear the limits to the processing of personal data by employers.

> "(1) The employer is only allowed to process personal data directly necessary for the employee's employment relationship which is connected with managing the rights and obligations of the parties to the relationship or with the benefits provided by the employer for the employee or which arise from the special nature of the work concerned.
>
> (2) No exceptions can be made to the necessity requirement, even with the employee's consent."

The Act goes on to stipulate the precise provisions which apply. It also makes clear that it applies in addition to the general law on data protection.

More limited provision is made by Article 11 of the Luxembourg law which specifically regulates supervision (or monitoring of employees) at the workplace. The prior authority of the data protection supervisory authority is required, and the processing may be carried out

> "…only if it is necessary: (a) for the safety and health of employees, or (b) to protect the company's property, or (c) to control the production process relating solely to machinery, or (d) to temporarily control production or the employee's services if such a measure is the only way of determining the exact earnings, or (e) in connection with the organisation of work under a flexible hours scheme in accordance with the law."

17.2.2 Other specified purposes

Some Member States' data protection laws include provisions regulating the processing of personal data for general monitoring purposes, which will frequently be carried out in public places by using CCTV or video cameras.

The Luxembourg law is one example. Article 10(1) sets out the circumstances in which such monitoring may take place. It is permitted only

> "(a) if the data subject has given his consent, or
>
> (b) in surroundings or in any place accessible or inaccessible to the public other than residential premises, particularly indoor car parks, stations, airports and on public transport, provided the place in question due to its nature. Position, configuration or frequentation presents a risk that makes the processing necessary for the safety of users and for the prevention of accidents, or
>
> (c) in private places where the resident natural or legal person is the controller."

The law limits the circumstances in which personal data collected by such monitoring may be disclosed to others by the data controller, and sets special penalties for breach of the provisions.

The Slovenian data protection law is another which contains special rules for video surveillance. In additional to a provision of general application, it deals specifically with video surveillance of access to office and business premises, apartment buildings and work areas. The law also contains special provisions on the processing of biometric data for various purposes, and on processing of personal data for the purpose of recording entry to and exit from premises.

As noted in a previous chapter, the Italian law, which takes the form of a Personal Data Protection Code and is therefore necessarily more detailed than a simple law, contains many provisions applying to specific sectors. These include (but are not limited to) the judicial sector, the police, the health care sector, education, occupational and social security issues, and banking, financial and insurance systems.

17.3 Comment from the EU perspective

The data protection rules established by the Directive are capable of being applied to all activities involving the processing of personal data across all sectors. However, when the Directive was adopted, it was envisaged that it would need to be complemented in time by other Directives setting more precise data protection rules for particular sectors. Indeed, on its introduction the draft Directive was accompanied by the draft of a separate Directive dealing with data protection in the telecommunications sector. This latter Directive was adopted and, following subsequent amendment, now has effect as the Directive on privacy and electronic communications (2002/58/EC). In the 13 years since the principal data protection Directive was adopted, no further sectoral data protection Directives have been passed into law. A draft Directive regulating the protection of personal data in the workplace was brought forward, but was abandoned after a brief period.

Member States' data protection laws likewise remain strongly focused on provisions of general application, and have not developed a complementary range of activity-specific legal measures. The most significant exception is Finland with its special, substantive law on the protection of privacy at work. This is not to say that Member States do not see a need for special rules applying to particular activities. However, where that need has been identified, the preference has been to tackle the issue by non-legislative means such as the development of codes of practice.

There may be a number of reasons why this should be so. The general data protection provisions found in the Directive are in themselves a very powerful instrument, and sufficiently flexible to be applied effectively in a wide range of circumstances. Arguably, there is little need for them to be complemented by more detailed measures. Where, however, it is felt that additional regulation is necessary, it is generally quicker and simpler to bring forward non-legislative measures such as codes of practice than to enact legislation; and non-legislative measures are simpler to amend in the light of changing circumstances.

17.4 Comment from the Chinese perspective

“Social activity” is not a legal concept and the term can be used only in a sociological sense. When laying out specific provisions or even a statute regulating personal information processing in “social activities”, it is difficult to identify its sphere of effect. Therefore for the most part a Chinese statute should apply in a uniform way to all processing of personal information, irrespective of the purpose for which the information is processed. In addition, some specific rules could be laid out related to information processing in some special fields such as journalism and telecommunication. The special information such as e-mail, telephone numbers and directories in electronic commerce must be identified as personal information as long as they can be stored and identify the subject. Considering the principle of equity in the civil law, this information should be protected to the same standard as other personal information in principle. As to special rules regulating journalism, this is still a developing issue for Chinese legislators and jurists.

Recommendation: In legislating on data protection, China should, at least initially, focus on measures of general application which can be effective for all activities whether in the public or private sectors.

18 Transfer of Personal Data to Third Countries

18.1 The Directive

Article 25.1 of the Directive establishes the basic rule that personal data may only be transferred to third countries [12] which ensure "an adequate level of protection". "Adequate" is not defined, but Article 25.2 sets out the factors that must be taken into account in assessing adequacy:

> "The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country."

Article 25 goes on to establish the procedures for determining collectively within the EU whether a third country does or does not ensure an adequate level of protection. A number of formal decisions by the European Commission that third countries, in whole or in part, provide an adequate level of protection have been made.

Article 26.1 provides exemptions from the basic rule. It permits transfers of personal data to third countries that do not ensure an adequate level of protection where:

> "(a) the data subject has given his consent unambiguously to the proposed transfer; or
>
> (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
>
> (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

[12] "Third countries" are all countries outside the European Economic Area (EEA). The EEA comprises the European Union, Iceland, Norway and Liechtenstein. By virtue of their status within the EEA, the three named countries are obliged to have data protection law at the level set by the Directive.

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case."

Article 26.2 permits Member States to authorise transfers of personal data to third countries that do not ensure an adequate level of protection where the data controller provides adequate safeguards for individuals' privacy and other rights and freedoms. As an example, it says that such safeguards may be provided by appropriate contractual clauses.

The remaining paragraphs of Article 26 establish procedures for collective assessment within the EU of the authorisations granted by Member States, and for the approval of standard contractual clauses that offer the safeguards required by Article 26.2. A number of sets of standard contractual clauses have been formally approved by the European Commission.

18.2 Member States' laws

Member States' laws follow the provisions of the Directive in permitting transfers of personal data only to those third countries which ensure an adequate level of protection, or where the exemptions set out in Article 26 of the Directive apply. However, the procedural arrangements vary from one Member State to another.

Most Member States' laws set out the criteria to be taken into account in assessing whether a third country ensures an adequate level of protection. However, most do not specify which body is responsible for making that assessment. Some say that the assessment is to be made by the data protection supervisory authority. An example is Article 27(3) of the Maltese law. Section 18 of the Luxembourg law, on the other hand, says that it is in the first instance for the data controller to assess whether or not a third country ensures an adequate level of protection. The controller need only consult the supervisory authority in cases of doubt.

Most Member States' laws provide expressly for the prior authorisation by the supervisory authority of transfers in the circumstances set out in Article 26.2 of the Directive. Some Member States' laws go beyond this, and expressly require the prior authorisation of the supervisory authority in other circumstances also. For example, Article 28 of the Lithuanian law requires an authorisation from the supervisory authority for all transfers except those based on the exemptions in Article 26.1 of the Directive. A small minority of Member States' laws (for example Greece and Cyprus) require the prior authorisation of the supervisory authority for all transfers, except where the European Commission has made a decision that the destination country provides an adequate

level of protection.

18.3 Comment from the EU perspective

18.3.1 Procedure

The number of transfers of personal data from one country to another made each day is huge. If international business is not to be disrupted, it is important that the procedural arrangements for the data protection regulation of such transfers allow decisions whether or not transfers may be made to be taken as quickly and easily as possible. The Directive gives little guidance on the procedures to be applied by Member States. It makes clear that decisions to make transfers based on Article 26.2 of the Directive require the prior authorisation of the Member State. (In practice, in most Member States this means the data protection supervisory authority.) However, aside from that, the Directive leaves it to the Member States to decide what their decision-making arrangements should be. Many have chosen procedures which involve the prior authorisation of some categories of transfers in addition to those made under Article 26.2 of the Directive. However, given the vast number of transfers that take place, it is questionable how effective any system of prior authorisation can be.

It is unclear from the Directive whether the assessment about the adequacy of the protection in a third country must be made for the destination country as a whole, or whether it can be made for different categories of transfer or even for individual transfers. This is an important issue. If the assessment of adequacy applies to the third country as a whole, in such a way that any transfer of personal data for any purpose may be made to that country, the third countries that receive positive assessments are likely to be limited to those which apply comprehensive data protection rules similar to those found in the European Union. This would mean that transfers to other countries could take place only if they were based on the exemptions in Article 26.1 of the Directive or the arrangements envisaged in Article 26.2. This is very restrictive. A more practical approach is to assess the adequacy of protection on a case by case basis. In this way, individual transfers can take place to any country, provided that enforceable arrangements are made in each case for the protection of the personal data transferred.

For this approach to work most effectively, the decision about the level of protection in the third country in question needs to be made in each case by the data controller wishing to make the transfer rather than by the supervisory authority. Some Member States' laws expressly give the responsibility for making the decisions about adequacy of protection in third countries to the supervisory authority. That is effectively a requirement for prior authorisation by the supervisory authority. Permitting decisions about "adequacy" to be made by the data controller, as expressly set out in the Luxembourg law, and as happens in practice in the United Kingdom and probably elsewhere, eliminates the risk of procedural delays to what may well be time-sensitive international business transactions.

18.3.2 Assessing "adequacy"

The earlier paper "Personal Data Protection in Europe and China: What Lessons to be Learned?" discusses the criteria that are likely to be applied by the EU in assessing whether a third country ensures an adequate level of protection. As that paper also explains, there is no guarantee that, even after adopting and giving effect to data protection legislation, China, or any other country, will be given a formal "adequacy" finding by the European Commission. Adequacy findings are made by the European Commission with the assistance of the Article 31 Committee of representatives of Member States' Governments.[13] The Commission has the key role, since it decides whether or not to bring the matter before the Committee. There is no set procedure for a country seeking an "adequacy" decision to bring the matter to the attention of the Commission. However this is done, it may be supposed that the Commission will make its own assessment of the case before bringing it before the Committee. It will also certainly wish to seek the opinion of the Article 29 Working Party (see Annex A). The main criterion for deciding whether or not a formal "adequacy" finding should be made will be the level of protection afforded by the data protection rules in place in the applicant country. However, having sound rules is not of itself enough. The applicant country will also have to show to the satisfaction of the decision-makers in the EU that the rules are complied with in practice.

18.3.3 The Safe Harbour

The United States does not have data protection legislation covering both the public and private sectors that applies throughout the country at both federal and state level. A finding that the United States ensures adequate protection for all the purposes for which personal data may be transferred from the European Union is, therefore, unlikely. When the Directive was adopted in 1995, there was concern about the consequences of its implementation for the flow of personal data from the European Union to the United States. Discussions opened between the European Commission and the United States Government with a view to discovering whether there was any way in which the Directive's restrictions could be eased. The outcome of those discussions was the "safe harbour" arrangements.

The arrangements permit participating organisations in the United States to import personal data freely from the European Union. Organisations are free to decide whether or not to participate. Those that choose to do so must agree to comply with a specially drafted set of data protection "principles". These cover: notice; choice; onward transfers; access; security; data integrity; and enforcement. Participating organisations must have in place mechanisms for dealing with complaints, verifying compliance and remedying problems. They can achieve this by subscribing to a private sector "seal programme" that incorporates and satisfies the safe harbour principles, or by agreeing to co-operate with EU data protection supervisory authorities. Underpinning enforcement is provided by US Government agencies. So far, the Federal Trade Commission and the

[13] This is the committee of representatives of Member States' Governments set up under Article 31 of the Directive to assist the Commission in its decision-making on matters relating to the transfer of personal data to third countries.

Department of Transportation are the only US Government agencies that have committed themselves to take enforcement action where necessary. This means that only those organisations that are subject to oversight by those two agencies may currently participate in the safe harbour.

The European Commission has made a formal finding under Article 25 of the Directive that the safe harbour arrangements ensure an adequate level of protection.

18.3.4 Binding Corporate Rules

As noted above, Article 26.2 of the Directive allows the transfer of personal data to third countries which do not ensure an adequate level of protection where the data controller in the EU provides adequate safeguards. One way in which the safeguards can be provided is by including conditions governing the way in which personal data are to be handled in a contract between the EU-based data controller who is transferring the data, and the recipient organisation in the third country. However, the use of contracts for this purpose is not possible when the transfer takes place within a single company or group of companies, since a legal entity cannot enter into a contract with itself. In such cases, binding corporate rules (BCR) may be used.

BCR comprise a legally enforceable set of undertakings in respect of the handling of personal data that a single company or group of companies makes when personal data are transferred from one part of the organisation that is within the EU to another part of the same organisation in a third country. An organisation wishing to use BCR as the basis for the transfer of personal data from the EU to a third country must seek the approval of the data protection supervisory authority of the EU Member State in which it is based. If personal data are to be transferred from more than one EU Member State the approval of all the relevant supervisory authorities is needed. A procedure has been established for co-operation among the supervisory authorities of the Member States in considering requests for authorisation for transfers from more than one Member State. The Article 29 Working Party has also drawn up a framework for the structure of BCR (see http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp154_en.pdf).

18.4 Comment from the Chinese perspective

With the rapid growth of globalization, the trans-border flow of personal information plays a more and more important role in personal information processing. In view of the restrictions on overseas transfers imposed by the Directive, China should include in its information protection law provision having comparable effect. Otherwise, the personal information flow between China and European Union will be restricted.

In order to facilitate the international flow, Chinese legislators should take various measures: for one thing, the fundamental rules of personal information protection must be laid out; for another, special rules as to international flow of personal information

should be made. An important element is the procedural and supervisory body for trans-border flows. The supervision can be exercised by a guiding branch of the government such as commerce department of central government in China. The body which wishes to transfer personal information to foreign states should put applications to the supervisory body. After investigation, the body should make its decision.

The Chinese government and enterprises will face challenges brought by the rules made by European Union and its member states. Apart from governments, enterprises and their trade associations should develop self-regulation rules according to the BCR model.

Recommendation: China should include in its data protection law provision regulating the transfer of personal data to third countries, so as to ensure the proper protection of the personal data once they have been transferred.

Afterword

The consideration of the data protection issues in this paper is set against the background of the EU Data Protection Directive. The Directive was adopted more than 10 years ago in October 1995. Information and communications technologies involving the processing of personal data have moved on rapidly since then. Applications not thought of when the Directive was adopted are now commonplace. The future holds the prospect of equally rapid and far-reaching developments. It can be asked whether the Directive remains apt to match such changes. Arguably, as an instrument of social policy that is not directly tied to any particular form of technology, it provides a legal framework suitable for responding to any present or conceivable future challenges. That is a bold assertion. Given the speed and magnitude of technological change, it is, surely, prudent to review the framework to ensure its continuing effectiveness. The European Commission have embarked on such a review. In 2008 they launched an invitation to tender for a "comparative study on different approaches to new privacy challenges, in particular in the light of technological developments" whose purpose was to "…give guidance on whether the legal framework of the Directive provides appropriate protection or whether amendments should be considered…". They also announced their intention to set up a group of experts to reflect on the data protection legal framework in the European Union. It is likely to be some considerable time before the outcome of that initiative is known, and even longer before any changes to the Directive that may be found necessary are implemented. Meanwhile, from the EU perspective, the Directive continues to offer an appropriate starting point for analysis of the data protection challenges confronting China, some of which are discussed in this paper.

Annex A

EU-level Arrangements

European Data Protection Supervisor

The institutions and bodies of the European Union (for example the European Commission, the European Parliament and the European Central Bank) are not subject to the national law of any Member State and they are not covered by the Data Protection Directive. To ensure that their processing of personal data is carried out according to the standards that apply within the Member States a special legislative instrument has been enacted. This is Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. This Regulation establishes data protection rules and procedural provisions that apply to the EU's institutions and bodies. They are broadly the same as those found in the Directive.

Article 41 of the Regulation establishes the post of European Data Protection Supervisor and places on him the responsibility of

> "… monitoring and ensuring the application of the provisions of this Regulation and any other Community act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Community institution or body, and for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data."

Article 44 of the Regulation requires the Supervisor to act independently in carrying out his duties, and specifies that he must neither seek nor take instructions from anybody. Article 45 imposes a duty of professional secrecy on the Supervisor and his staff both during and after their terms of office. Article 46 sets out the Supervisor's duties and Article 47 his powers. These are extensive and comparable to those available to national supervisory authorities. Article 48 requires him to produce and make public an annual report about his activities.

The first Supervisor and his deputy, the Assistant Supervisor, were appointed in December 2003. Their mandates are for 5 years and are renewable.

Article 29 Working Party

Article 29 of the Data Protection Directive provides for the establishment of a Working Party on the Protection of Individuals with regard to the Processing of Personal Data. The working party comprises a representative from a data protection supervisory authority from each of the Member States, the European Data Protection Supervisor and a representative of the European Commission. The secretariat is provided by the Commission.

The working party's remit is set out in Article 30 of the Directive. It is to:

> "(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;
> (b) give the Commission an opinion on the level of protection in the Community and in third countries;
> (c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;
> (d) give an opinion on codes of conduct drawn up at Community level."

The working party must advise the Commission if it finds significant divergences in the data protection laws and practices of Member States. It may make recommendations on all matters relating to data protection within the EU. The working party must produce and publish an annual report.

Over the years the working party has produced opinions, recommendations and other papers on many different aspects of data protection. Much of its work deals with the transfer of personal data outside the EU, including responding to current issues under consideration by the European Commission, for example the preparation of model contractual clauses for use by data controllers in sending personal data to third countries, or the assessment of the level of data protection in a particular third country with a view to a formal finding that that level is "adequate". However, the work of the working party has also covered topics ranging from video surveillance, to the enforcement of data protection laws, and the processing of personal data in the employment context.

The working party's opinions and recommendations are sent to the European Commission and to the Article 31 Committee[14]. The Commission must produce a report setting out the action it has taken. The working party's opinions and recommendations are not binding. However, as the national representatives of the data protection supervisory authorities, their collective experience and understanding of data protection law and practice are unparalleled and their views carry a great deal of weight. Moreover, since the supervisory authorities which they represent play an important part in determining national data protection policy, they are in a position to take forward the thinking of the working party in developing data protection practice domestically.

[14] This is the committee of representatives of Member States' Governments set up under Article 31 of the Directive to assist the Commission in its decision-making on matters relating to the transfer of personal data to third countries.

Annex B

The United Kingdom Information Commissioner

The Information Commissioner is the United Kingdom's independent supervisory authority for data protection and freedom of information. He is appointed by the Queen on the advice of the Government. The mandate is for up to 5 years and he may be re-appointed once. In exceptional circumstances, where a further term is desirable in the public interest, he may be re-appointed for a further maximum 5 year period. He may not serve beyond the age of 65, or for more than 15 years in total. The Queen may remove him from office at the request of both Houses of Parliament. The Commissioner's salary and pension are set by a resolution of the House of Commons.

The Commissioner's formal decisions are made by him alone. Although this is not required by law, he is assisted by a management board comprising six senior members of his permanent staff, and four other people who are not members of his staff.

The Commissioner is required by law to appoint two deputies who have the power to act for him when he is, for any reason, unable to act himself. One of the deputies has responsibility for work on data protection, and the other has responsibility for work on freedom of information. Subject to approval by the Government (in practice the Ministry of Justice), the Commissioner has responsibility for deciding how many staff he needs and for appointing them and determining their pay and pensions. At the time of preparing this paper, the Commissioner had a total of 270 staff. At the headquarters office 114 staff work full-time on data protection and 59 on freedom of information. There are 82 staff who provide common services (for example legal advice and human resources support). There are 15 staff in regional offices who work on both data protection and freedom of information. Neither the Commissioner nor his staff are civil servants.

The Commissioner's activities in connection with data protection are funded from the income from notification fees. (Each data controller who is required to notify the Commissioner of the processing that he does must pay an annual fee of £35 (490 RMB).) In 2006/7 the fee income was about £10 million (140 million RMB). (Expenditure on activities in connection with freedom of information is funded by a grant from the Government. In 2006/7 the grant was about £5.5 million (77 million RMB).)

The Commissioner's statutory functions in relation to data protection include:

- a duty to promote the following of good practice and the observance of the requirement of the data protection law by data controllers;
- powers to take enforcement action (see Chapter 11);
- a duty to arrange for the dissemination of information to the public about the data protection law, good practice and any other matter within the scope of his functions;
- a power to give advice to any person about the above matters;
- a duty to consider complaints;

- a duty to prepare and disseminate codes of practice where he is required to do so by the Government or where he otherwise considers it appropriate to do so;
- a duty to encourage trade associations to prepare and disseminate codes of practice and, where such codes are submitted to him, to give his opinion whether they promote good practice;
- a duty to disseminate European Commission findings about the adequacy of data protection in third countries, and any other relevant information about data protection in third countries;
- a power to assess whether the processing of personal data follows good practice, with the consent of the data controller;
- a duty to present a report on his activities to both Houses of Parliament every year;
- a power to present such other reports as he sees fit;
- a power to assist individuals in court proceedings which involve processing for the purposes of journalism, literature or art[15];
- a duty to carry out specified international functions.

[15] The law establishes special rules for processing of such data, in order to balance data protection with freedom of expression. The rules are complex.