GERMANY EXTENDS DATA PROTECTION RIGHTS TO SECRET POLICE FILES

January 1st 1992 marks the opening up of the files held by the disbanded State Security Police (the Stasi) to the individuals on whom the records were kept. This decision by the Bundestag (Parliament) marks the climax in data protection terms of: the unification of the German state on October 3, 1990; the passing of the new Data Protection Act and of laws on the intelligence services on December 29th 1990; and from June 1st 1991 the entry into force of the new Data Protection Act in the whole country. The former German Democratic Republic was a prominent example of a centralized state power manipulating personal information for political control purposes. The Stasi employed 90,000 full-time and 150,000 part-time staff to compile files on four million East Germans and two million West Germans.

The following edited report from Germany's Federal Data Protection Commission examines how it is meeting the twin challenge of transforming the closed record-keeping culture of a generation in East Germany into a transparent accountable process; and supervising the implementation of the new law's stronger principles across the country.

Establishment of German Unity

The aspirations of the citizens of the former German Democratic Republic (GDR) for freedom were also aimed at achieving protection of personal rights and protecting the private sphere against government interference.

Data Protection in a Communist Regime

Data protection in the sense of legal protection of personal rights was entirely neglected under the Communist regime.

In the former GDR, the term *data protection* was defined in such a way as to refer only to data security, and thus lent itself for use as an instrument preventing the citizen from inspecting his/her own data.

Given this background, problems concerning data protection law have emerged in the five new Federal States (Lander) in almost all spheres of life. This is particularly the case with the large central databases of the former GDR, for example, the Central Residents' Register, the labour database, the police, the Central Judicial Records of the former Chief Public Prosecutor and the National Cancer Register.

The personnel files of workers/employees often include too much information, for example, their health and their political views. But many items of personnel data have, mostly with official approval, been "adjusted" in the transitional period leading up to German unification.

Further questions arise from the existence of provisions intended to enhance administrative efficiency in the Communist state. The Uniform Personal Identification Number, for example, or the ID card for employment and social insurance used in the GDR contains plenty of social and health data requiring particular protection. In legal and human terms, the problem which is the most difficult to solve is that posed by the data files and records of the former Ministry for State Security (MFS).

Unification Treaty makes changes

Important changes for data protection were made in the Unification Treaty between the Federal Republic of Germany (FRG) and the GDR, including the following provisions:

- The Federal Data Protection Act should apply in the area of the former GDR from October 3 1990
- Immediate erasure of all data which is no longer required or which, under federal law would not have been allowed to be stored, unless such erasure would prejudice any of the data subjects' interests entitled to protection

- The Federal Commissioner will supervise and enforce data protection as applied by Land and local authorities until the appointment of Land Commissioners or until 31 December 1991 at the latest
- Erasure of personal ID numbers at the earliest time possible; with the obligation to immediately rearrange existing data files in both public and private sectors according to different criteria
- Provisional arrangements governing handling of records held by the State Security Service, including the appointment of an independent Special Commissioner, and safeguarding of data files and records for the time being pending specific legal provisions.

The Federal Data Protection Commission has been allocated twelve new staff posts to cope with the additional tasks resulting from unification, including a section primarily concerned with State Security issues.

New Federal Data Protection Act

On June 1 1991, the new Federal *Data Protection Act* entered into force. (The official English translation has been distributed to subscribers with this newsletter). For the public sector, it represents major progress. It draws the appropriate conclusions from the 1983 decision of the Federal Constitutional Court on the national census and is closer than the previous Act to the principles of the *Council of Europe Data Protection Convention,* including for the first time in Germany coverage of the *use of data.*

The most important changes are as follows:

1. extension of the Federal *Data Protection Act's* scope in the public sector (section 12); to include *inter alia* personal data in the form of images and sound recordings (section 3 (3); (this broader definition of personal data is not explicitly extended to the private sector) and provisions governing data collection (section 13);
2. the enabling of claims for compensation to be made against public bodies, regardless of fault (section 7);
3. definition of conditions for the establishment of automated retrieval procedures (section 10);
4. improvement of citizens' rights to obtain information, such as an exemption from fees in many cases and inclusion of the sources and recipients of data (section 19);
5. election of the Federal Data Protection Commissioner by the Bundestag (section 22).
6. only very limited sections of the Act, covering mainly confidentiality and data security, apply to *manual records* when personal data is not intended for communication to third parties (section 1 (3) 2).
7. press/film/broadcasting companies using personal data exclusively for their own editorial use have an exemption so that they need to implement only the confidentiality and security sections (sections 5 and 9) of the Act (section 41). If such companies publish directories, they may retain this exemption only if "a journalistic-editorial activity is connected with such a publication."

Few Changes for the Private Sector

In the private sector, a similar development of data protection law has, apart from a few exceptions, not yet taken place. Therefore, the requirement in future will be for legislation geared more specifically to individual sectors so as to ensure adequate data protection in sensitive sectors such as labour, the insurance and banking industries and the activities of personal information bureaus, such as head hunting and introduction agencies.

Legislation on the Intelligence Services

On December 30 1990 new laws governing the intelligence services entered into force. The Federal Intelligence Service (BND) - concerned

with foreign intelligence - and the Federal Armed Forces Counterintelligence Office (MAD), have for the first time been provided with a legal basis. The *Protection of the Constitution Act* has been thoroughly revised. Parliament has improved data protection on important points, for example:

- more precise allocation of tasks to each enforcement agency, for example by providing an exact definition of the "efforts aimed at subverting the free democratic basic order."
- provisions governing the special forms of data collection, for example, by technical means for covert image and sound recordings in homes, with these being subject to very tight restrictions;
- special provisions for the protection of minors;
- inclusion of all types of collected information, not only data files;
- an obligation to adopt, with the participation of the Federal Commissioner, a set of data file rules for every automated data file;
- regular inspection of the stored data every five years, and regular erasure after ten years.

The data subject has a right to obtain information if he/she refers to specific facts of the case, asserts a special interest, and if there is no overriding requirement for maintaining the secrecy of the information. It is still to be seen whether, in practice, this policy will be responsive to citizens' concerns.

Current Legislation

Protection of Employee Data

For a long time, there have been demands to establish special legal provisions for the collection and processing of employee data.

The Federal Government, in the last legislative session, submitted to the legislature a bill to revise employment regulations and has once more introduced it in the current session. This bill is largely modelled on the *Council of Europe's Data Protection Recommendation on Employee Data.*

The bill concerns only the public sector. However, the Bundestag has invited the Federal Government to submit bills covering the entire field of data protection for employees and this work is still in progress.

Court Debtor Lists

Courts which make orders for the payment of debts by seizing debtors' property keep Debtor Lists. Individuals who have been the subject of unsuccessful claims against their property make a statutory declaration on the inventory of their assets, a so-called oath of disclosure. These people are then added to the Debtor Lists for a period of about three years. Under the provisions of the current version of the *Code of Civil Procedure,* anyone must, upon request, be given information on the existence or non-existence of a specific entry in the Debtor List or be granted an opportunity to inspect the List. Also, extracts copied from the Debtor Lists will be provided, for instance, to Chambers of Industry and Commerce which, in turn, will supply their members with copies.

The need-to-know principle

The Federal Government has introduced a bill under which provision of information from a Debtors' List will be subject to the need-to-know principle and which, in principle, requires the existence of a legitimate interest as a prerequisite for the passing on of copies and lists. Also, it is mandatory to keep confidential the processing of the data contained in copies, lists and data files. As the Federal Data Protection Commissioner sees it, the requirement is for the recipients of data to be sufficiently checked so that, in particular, the prescribed time limits for erasure will actually be observed.

Whose interest prevails?

Germany's new Federal Data Protection Act, like the European Community data protection draft directive, is based on a strong human rights platform.

1. Purpose

The new law's *purpose* is stated clearly in Part 1 Section 1 Article 1:

"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. Inalienable rights

This theme is continued in a series of strongly worded sections, for example, section 6 on the *inalienable rights of the data subject:*

"The data subject's right to information (sections 19, 34) and to correction, erasure or blocking (sections 20, 35) may not be excluded or restricted by a legal transaction."

3. Compensation

Section 8 on "*compensation by private bodies.*"

"If a data subject asserts a claim against a private body for compensation because of automated data processing that is inadmissable or incorrect under this Act or other data protection provisions and if it is disputed whether the controller of the data file is responsible, the burden of proof shall rest with the controller of the data file."

4. Marketing and Research

Section 28 (3) on *marketing and research*:

"If the data subject objects vis-à-vis the controller of the data file to the use or communication of his data for purposes of advertising or of market or opinion research, use or communication for such purposes shall be inadmissable. Where the data subject objects, ... the recipient shall block the data for such purposes." (Blocking means labelling stored personal data so as to restrict their further processing or use). These clauses strengthen the existing voluntary Robinson list organized by Germany's direct marketing industry which gives individuals an opportunity to indicate that they do not wish to receive direct marketing communications.

5. Communication of data

Communication of data (section 28 (2)) is admissable in certain circumstances,such as to safeguard justified interests of a third party, or if the data concerns members of a group of persons and are restricted to:

- the data subject's membership of this group of persons
- occupation or type of business
- name
- title
- academic degrees
- address
- year of birth

"and if there is no reason to assume that the data subject has a legitimate interest in his data being excluded from communication."

In the past, German Data Protection Authorities have not regarded any such groups used by industry as being too specific. Therefore, German experts cannot understand the direct marketing industry outside Germany criticizing the German law for effectively preventing targetting of prospects.

As telephone and fax numbers are excluded from this list, the transfer of these numbers would *not* be permitted unless the individuals had given their consent.

Data subjects' interests also prevail in requiring consent for the communication of data on:

- health matters
- criminal offences
- administrative offences
- religious or political views and
- when communicated by an employer under labour law.

If the personal data does not come under one of the above sensitive categories, then the data subjects' legitimate interests may or may not prevail if a case goes before a court. However, the interpretation of the law given by some experts in the Interior Ministry is that in such cases, the data subjects' interests do *not* prevail. However, there have not yet been any court decisions on this point.

6. Storage or Modification of Data

Storage or modification of data for the purpose of communication is admissable if the data subject's "legitimate interests" are not harmed (section 29 (1)).

7. Use of Data for a Limited Purpose

The *recipient of personal data* must use or process it "only for the purpose for which he has received" the data (section 39 (1)). The recipient may use or process the data for another purpose only if the change of purpose is "permitted by special legislation" (section 39 (2)).

8. Duty to Inform the Data Subject

The organization communicating the data must *inform the data subject* when the data is transferred for the first time, unless it can be assumed that the data subject knows of the data storage another way (section 16 (3)).

Federal Data Commissioner's Role

Unlike other European data protection laws, the Federal Data Protection Commissioner has responsibility for the public sector but no supervisory powers over the private sector. However, he must report to the Bundestag (Parliament) every two years on developments in both sectors (section 26 (1)) and *make recommendations* to the Federal Government and Parliament on improving data protection (section 26 (3)). His duty to report to the government on the private sector is stated explicitly for the first time.

If you are interested in a workshop on Germany's new Data Protection Act, please inform the *Privacy Laws & Business* office.