

## HOW GERMANY'S DATA PROTECTION LAW IS ENFORCED BY A LAND DPA

*Privacy Laws & Business is frequently asked about how the Data Protection Act is enforced in Germany. Here, Dr Hans-Hermann Schrader, Hamburg's DPA, explains how the system works.*

### Status of the DPA

The Free and Hanseatic City of Hamburg is a City State and one of the German Federal States. It has a population of nearly two million. I was elected to the post of Hamburg Data Protection Commissioner by the Parliament of this city on the proposal of the Land government for a period of six years. I operate independently and am subject only to the law.

### Reviewing and monitoring the public and private sectors

The Hamburg Data Protection Commissioner is responsible for data protection in the public sector and also acts as supervisory body for data security in the private sector. The Hamburg Data Protection Authority reviews the activities of the administration in respect of the Hamburg law on data protection. This task is similar to that performed in the other German federal states; it also monitors observance of the federal data protection law by private bodies, especially by commerce and industry.

As a result, the control of data processing in the public and private sectors is concentrated in a single body - this is in contrast to the situation in most of the other German federal states, where supervision over commerce and industry is performed by the state ministries of the interior. The Hamburg Data Protection Authority has a staff of nearly twenty.

### Investigation of submissions by citizens

Each citizen may directly consult the Hamburg Data Protection Commissioner. Nobody need be disadvantaged on this account. Members of the administrative staff do not need to observe bureaucratic hierarchies by approaching the DPC via their head of departments.

Numerous citizens report daily to the Data Protection Authority with written submissions, queries by telephone and personal calls. In 1992, we received over 300 written submissions from both public and private sectors.

• <b>Public sector</b>	
security data	51
health & social welfare area	47
other areas	71
<b>Total</b>	<b>169</b>
• <b>Private sector</b>	
mail order business	4
insurance sector	15
credit business	8
advertising	5
employee data protection	10
credit enquiry agencies	22
health sector	23
other	52
<b>Total</b>	<b>139</b>

The submissions, queries and personal visits of citizens provide a basis for the Data Protection Authority conducting an inspection of the government authority or the private organisation in individual cases.

### Inspection Visits

An inspection, which may also originate in anonymous tip-offs or press reports, usually opens with a letter from the Data Protection Authority to the data processing body concerned asking for questions to be answered and for a statement on the matter. If the written reply gives rise to the need for clarification, an inspection is held on the

premises. As a rule, the Data Protection Authority gives notice of this to the body concerned, though usually without specifying the concrete object of concern. In some cases - when there are special reasons - the on-the-spot inspection is conducted without warning. The organisations conducting data processing are legally obliged to grant entry, provide information and present their documents and data-processing programmes. If a private organisation refuses, this infringement is punished with a fine of up to 50,000 DM.

The Data Protection Authority notifies the complainant of the result of the investigation together with an assessment of the situation in data protection law. If this seems appropriate, he also notifies others who are concerned and calls for rectification of the shortcomings.

### **The power of publicity**

In the public sector, violations can be reported formally to the relevant Senator and, in the event of a further complaint, to the Senate, which constitutes the state government. At this stage, the media, too, is informed as a rule. This procedure is just as effective as a directive, which the data protection authority is not empowered to issue to public bodies.

### **Dismissal of a data protection officer and other extreme measures**

In addition, the supervisory authority has powers to issue orders or prohibitions in the private sector if defects have been found in the technical or organisational areas of a private data processing company. In more serious cases, this may lead to the supervisory authority demanding the dismissal of the company data protection officer on the grounds of lack of expertise or unreliability.

In extreme cases, the deployment of individual data-processing methods can be forbidden if serious technical and organisational defects particularly endanger the right to privacy, for example, in the case of the insecure storage of health data.

Otherwise, it is up to the complainants whether they wish to take further steps on the

basis of the notification they have received from the Data Protection Authority. The Data Protection Authority makes assistance available for complainants to implement their rights to information, correction, blocking or deletion of data by calling on the company concerned to act accordingly on behalf of the complainants. If those involved continue their dispute, the decision is reserved for the courts. This applies, in particular, to cases where the complainants propose prosecution.

### **Ongoing supervision and counselling**

Alongside these investigations into individual cases, the public sector and certain private bodies are subject to regular examination by the Data Protection Supervisory authority. In the private sector, this affects primarily:

- credit information agencies,
- address agencies,
- market research and opinion poll institutes, and
- companies in the service sector that process data on a contract basis.

The Hamburg Supervisory Authority knows currently of approximately 200 such companies. In the majority of these cases, the data processors are working on a contract basis.

The Data Protection Authority does not investigate companies every year, but several are targeted each year in an inspection plan. In 1993, the Hamburg Authority investigated a total of about 40 companies under the ongoing data protection supervision scheme, almost one company a week.

### **Inspection procedures**

Such inspections are announced and prepared by the data protection authority. In the opening letter, the date of the inspection is specified. The private organisations are informed of their right to refuse to answer questions if they would thereby incriminate themselves. Apart from being otherwise generally obliged to provide information, the

organisation being inspected has to submit to the activity of the Data Protection Authority inspector - for example, his or her scrutiny and viewing of its business activities. In the case of private companies, the inspector must observe their business hours. In other respects, inspection procedures are similar to those used in the public sector as described above.

### **Advisory Role**

The role of the data protection authority as an advisory body is also important. The aim here is to sharpen consciousness of data protection in public and private organisations and to achieve a lasting improvement in data security. In Hamburg, such advisory work is conducted largely over the telephone, but may also be in writing or take the form of discussions on the premises, in particular, with the company data protection officers.

### **Cooperation with other organisations**

The data protection authorities of the Federal and the State governments are engaged in a continuous exchange of opinion, keeping each other informed in writing and verbally of all important matters. In this regard, the Hamburg Data Protection Commissioner is responsible in Germany for coordinating data protection in the sphere of domestic security and for data protection in the insurance industry, with whose federal association two or three conferences are held annually.

Within Hamburg there is an ongoing exchange in writing and in the form of consultation with the administration and private organisations, for example, with the working groups of the company data protection officers.

In addition, we present our experience annually in the form of an activity report of about 200 pages that is simultaneously presented to the state government, the state parliament and the public. There are also public meetings for disseminating information through talks and discussions.

### **Impact of EC data protection directive**

Whereas until now binding directives could only be issued in exceptional cases by the supervisory authority, the EC directive will lead to a clear extension of powers in the private sector. According to Article 30 of the draft directive, it is intended that the inspection authority should receive "effective powers of intervention such as ordering the blocking or erasure of data, a temporary or definitive ban on processing, the destruction of data material, or warning to the controller."

It is also intended to explore the possibility, provided for in Article 28, of establishing joint "codes of conduct" between the supervisory authority and industry, for example, in the insurance sector. Until now there has not been any such express regulation in the federal law on data protection. In practice, however, many controversial questions, for example about warning files in the insurance sector - have been documented by joint written statements.

**Dr Hans-Hermann Schrader, The Data Protection Commissioner for the Hanseatic City of Hamburg spoke at the *Privacy Laws & Business* Conference in Manchester, in September 1993.**