Major changes ahead for data protection in Germany

Ideally, data protection and data security are regarded as values, not as a nuisance but as part of the value of the products that a company offers to the public. Seen from that perspective, data protection managers in Germany are confident about their role. But below the surface, major changes are ahead for Germany's data protection law. Dr. Ulrich Dammann, Germany's Deputy Federal Data Protection Commissioner, explains.

Our main work in our office is to help prepare and execute special sectoral legislation. We already have special legislation in perhaps 20-25 Acts at the federal level and not much less on the state level but there is still a large programme to fulfil. It is a part of our constitutional law that any data processing activity, such as a change of purpose, has to take place on a legal basis and so the legislature has to provide for data protection regulations in a very differentiated way.

We have recently made a review of sectoral regulatory activities which should be implemented in the next few years. It adds up to about 40 items. The most important ones are in the areas of criminal justice, tax, customs, telecommunications and labour.

Internationalisation of data protection

Another very important aspect of our work these days is the internationalisation of data processing and data protection. For a long time, this was the task of one or two specialised staff in our office. Now nearly every subject has important international aspects, for instance, security, immigration, telecommunications, and taxes.

When international information systems, such as Schengen or Europol, are established, it is our aim on an international level to make sure that full and efficient data protection is guaranteed in all states which participate. This is a condition for easier data transfer between the countries. A problem which has occurred repeatedly comes from the fact that not all parties are prepared to include full protection for manual data. In Germany, we regard both automated and manual functions of an information system as a whole, both requiring the same high quality control and protection.

Another cause for concern is the lack of a data protection policy within the institutions of the European Union (EU). We are very happy about the adoption of the Data Protection Directive, but now it is time for the EU to have a regulation for itself. Otherwise, the whole system would not be consistent and the Member States would not exchange data with the European institutions.

Need for a major change of approach

We are becoming more and more aware that the approach that we have taken in the past 20 years will not be sufficient in the future. Some changes in the context of the EU Data Protection Directive are under way. But we must admit that the information highways and the information society require a more fundamental revision of our approach.

Generally, Germans look more sceptically towards the information age than other European countries. This goes along with a high awareness of security and protection. In a digitalised world, data protection authorities no longer have full control of what is going on: the files which are created, the kind of data which is processed and used, and for which purposes. Perhaps this has always been an illusion.

Data Protection Commissioners will have to concentrate on sensitive areas, on broad effects, on infrastructure changes. They will have a stronger role as mediators between information technology and individuals, and between organisations and individuals. They have to inform the public and help the individual to be in a position to act on his own in a changed environment. That will be an even more difficult job but one which is worth doing.

Informed consent and enforced subject access

Another fundamental question is the extent to which we can further rely on the principle of informed consent. Does informed consent always operate as a mechanism for individual self-determination? The federal data protection authority and others have expressed doubt in a couple of cases.

For instance, employers have asked job applicants, and landlords have asked their

prospective tenants to present a copy of the data held on them by the police or by credit reference institutions. The employers or landlords could not gain access to the data directly as a consequence of data protection regulation. So they used the individuals themselves as a key. It is not possible, from a legal point of view, to say that in that case the individual's decision was not free and was therefore not valid. And you would not help the people who are looking for a job or an apartment.

The only way to help is to tell employers and landlords that this is not fair data collection. Unfortunately, in the case of landlords, our Länder authorities could not all agree with that position.

Informed consent in an electronic environment poses problems. Does the individual really know what he is doing? Was the information sufficient? Is it possible to assess the consequences in a highly complex and fast changing electronic world with so many interrelated actors and functions?

But we also have to ask to what extent telecommunications services providers should have any right to collect and process more personal data than is necessary for their functions? Should they do that by regularly asking their clients for consent? Does giving such a consent not mean consumers selling their inalienable rights? One has to take into account:

- the immense amount of data, which will soon cover a large part of an individual's professional and private life
- the growing sensitivity of the data, which is no longer limited to commercial and other transactions as such, but record every step through the electronic world thus revealing individual behaviour, capacities, preferences, and desires in maximum detail and in terms of time, space and money
- the fact that all this data can be stored, interrelated, distributed by many institutions and kept for a long time.

In Germany, since 1983, there has been legislation on Telekom's Btx (on-line) services which allows service providers to process all necessary data in an appropriate way, but at the same time prohibits going beyond these limits by offering contracts or services on condition that the customers give their consent. This is the right approach and it should be broadened to other service providers.

Information infrastructure to require anonymous use

More than in the past, our strategies will have to focus on questions of information infrastructure. For example, there should be the principle that electronic services may be offered to the public only if the service includes ways of anonymous use and anonymous payment. This principle could be the core of the new data protection era. Obviously, it will be difficult to translate that principle into legislation, given the complexity of the market and its international character.

Current issues

The Berlin data scandal

A recent incident has been called the Berlin data scandal. A credit service information company in Berlin was found to operate illegally to a great extent. They had educated their personnel on how to get information from all kinds of public and private institutions by, for example, impersonating a policeman when making a telephone enquiry. They seem to have done that quite successfully. In the meantime, it came out that similar practices had been used by companies in some other German cities. It is now up to the police and law courts to look deeper into these issues and we will see how public opinion will be affected.

"They had educated their personnel on how to get information... by, for example, impersonating a policeman when making a telephone enquiry."

We have had a test of road pricing systems on a highway between Cologne and Bonn. The companies and the authorities are now analysing the results. A clear position has been taken by the Minister of Transport who said that he would not introduce such a system if data protection questions were not solved in a satisfactory way.

Smart cards

The privatised German National Railway has produced a multi-purpose smart card in

co-operation with Citibank. Owners of the card have the right to buy tickets at half price and with this new card they also have a full service credit card. This was not very good news for the existing credit card companies. Of course, this was one of the reasons for vigorous discussion on the data protection implications. The problem was that interested persons had only one form to apply for such a bi-functional card, and there was no option in the form to say "I don't want the credit card." So everybody seemed to be obliged to fill in all his details on his financial status and so on. It shows the kind and quality of problems associated with multi-functional cards.

Electronic signatures

The federal government is beginning to think about electronic signatures. Initial studies have been made but no decisions have been taken so far. To gain approval for electronic signatures in the same way as for written signatures requires legislation and perhaps even the creation of state institutions. The privacy implications are not only for the security sector but also linked to the fact that these authorities will distribute the keys. As a by-product, they would create a kind of population register. The situation is similar to that in the case of centrally issued and numbered identity cards. Until now in Germany, we have not had, and we have always objected to, the creation of a federal register of citizens and this might become a very comprehensive one. These questions will be answered in the next few years.

The Stasi files

The authority which administers the former Stasi archive has been requested by a Land parliamentary committee of investigation to contribute Stasi data to help with their investigation into the Barschel affair. Mr. Uwe Barschel, in his time as Land Prime Minister in the late 1980's, had used extraordinary dirty tricks to influence the elections. Later, he was found dead in a Geneva hotel in mysterious circumstances. Apparently, the opposition party was not quite so ignorant of the affair as they had claimed to the public at the time. So the committee, besides looking into the election affair, also investigated how and when the opposition learned of these facts. The committee made a list of 19 ministers, members of parliament and other leading politicians of the present Social Democratic Government, which was the opposition at that time, and some of their advisors. They asked the Stasi Archive to hand over any information pertaining to these 19 people. The archive sent 700 pages of information, mostly based on the interception of telephone calls which had been carried out at the time by these 19 people in the course of their government and political activities.

When this material was presented to the parliamentary committee, some of its members were shocked and objected to its use. The committee then locked the material away in order to obtain more legal evidence on the case. Some of the individuals concerned went to court. The lower court ruled that it was illegal to look into these papers. The case is now pending before the higher courts.

The Act on the Former Stasi Archive generally allows its use for parliamentary enquiries. The Federal Data Protection Commissioner has pointed to the fact that the Stasi archive has been preserved only for the purpose of giving access to the victims and enabling society to reflect on their political history. For these purposes only was it decided to keep the data, knowing that large parts of it had been collected by means of serious violations of human rights. Consequently, these constitutional limitations have to be observed in this case of parliamentary enquiries in the same way. The Commissioner, therefore, asked the Federal Government to ensure that the papers will be returned. The Federal Government has not yet replied.

It was widely noticed, and by some with astonishment, that the Federal Government recently appointed Dr. Hansjörg Geiger as first director of the Internal Federal Intelligence service. Before his time as administrative director of the authority which administers the former Stasi Archive, he had held a leading position in the Bavarian data protection office for ten years and he is one of the authors of the well known commentary to the Federal Data Protection Act, the BDSG, edited by Simitis et al.

This report is based on a presentation by Dr. Ulrich Dammann, Deputy Federal Data Protection Commissioner, at the *Privacy Laws & Business* 8th Annual Conference, 10th-12th July, 1995 at St. John's College, Cambridge.