are quoted by reference to names of the parties involved.

In addition to the above cases, processing of judicial data is allowed if it is necessary:

- for execution of a *legal obligation*;
- for execution of an *obligation imposed by a law of a country party to the Council of Europe Convention* on Protection of Personal Data 1981 which ensures an equivalent level of protection;
- to take a *decision at the request of a data subject*;
- to provide a *service in favour and on request of a data subject*;
- for execution of an *obligation imposed by international public law*.

In these particular cases, a data controller has to ensure that the data subject is notified in writing of processing of such data at least one month before the start of processing.

Finally, judicial and other related data can always be legitimately processed where the data subject has consented to it in writing.

Safeguard measures

Where the processing of judicial data and other related data is legitimately carried out in one of the above situations, data controllers still have a duty to take adequate safeguard measures. The Decree mentions the same type of measures as envisaged in the Sensitive Data Decree (see above). In addition, there is a special provision regarding international police co-operation, requiring the data controller to keep a record of all communications of judicial data abroad in the previous six months.

Registration fees

The registration fees range from 1,500 Belgian francs (£33) to 10,000 Belgian francs (£217), depending on the purposes of processing and the form in which the declaration is made. Generally, fees for a declaration presented by automated means are lower than for the cases where declaration is made by filling in the paper forms.

This report was written by Bojana Bellamy, a *Privacy Laws & Business* consultant.

A German DP Commissioner's view on the role of a company data protection officer

Dr. Astrid Breinlinger, Data Protection Commissioner for the land of Hesse, discusses the role of the data protection officer as provided for in Chapter III of the German Data Protection Act (BDSG). This report is based on her article in the German journal *Recht der Datenverarbeitung* [1].

The legal base for the German model

According to Section 36 of the BDSG, private bodies engaged in the automated processing of personal data and regularly employing at least five employees for this purpose need to appoint an internal data protection officer. The main responsibility of the data protection officer is to enforce and audit data protection compliance within the organisation.

The underlying rationale of the German approach is self-regulation, since in the exercise of their duties, data protection officers work in close co-operation with those involved in the processing of personal data and *"with particular reference to the situation prevailing in this area and the special data protection requirements arising therefrom"* [Section 37(1)2].

The Act also makes legal provisions for a relationship between the company data protection officer and the relevant land data protection authority for the private sector. According to Section 37(1), data protection officers may in the exercise of their duties *"apply to the supervisory authority in cases of doubt,"* in order to get an official point of view in controversial matters. On the other hand, the company data protection officer is present when the supervisory authority monitors and checks in specific cases the application of the BDSG and other data protection provisions as stipulated by Section 38(1) and (2).

The duties of the data protection controller - in law and in practice

The duties of the data protection officer as laid down in Section 37 of the BDSG are to ensure the observance of data protection law and other relevant provisions. In three subsections the

legislator has emphasised the following specific tasks as particularly relevant:

- monitoring the proper use of data processing programs with which personal data are to be processed [Section 37(1)1];
- raising staff awareness of data protection issues and regulations [Section 37(1)2];
- providing assistance and advice in the selection of persons to be employed in personal data processing [Section 37(1)3].

Dr. Breinlinger particularly examines the first task of a data protection officer. She believes that for the effective exercise of the duty conferred by Section 37(1)1, a broad interpretation needs to be given to the content of that duty. To monitor the proper use of a data processing program implies comparing processing procedures as conceived by the program with what happens in reality. However, constant monitoring would be far too time consuming and in view of the fact that most data protection officers fulfil this function only on a part-time basis, monitoring would have to take the form of merely occasional controls. Dr. Breinlinger therefore suggests widening the scope of the monitoring duty going beyond the BDSG provisions on processing, collection and use of personal data in the private sector and the observance of other measures such as stipulated in Section 9 of the BDSG. Monitoring should also be undertaken in relation to the observance of data protection provisions found in other pieces of legislation or regulation. Examples in the German context are the *Sicherheitsüberprüfungsgesetz* (Law on Safety Checks), or provisions relating to data protection in Employment Agreements.

The tasks of the data protection officer should not be seen as merely monitoring and evaluation of a given situation. According to Section 37(1)1, the officer should be *"informed in good time of projects for automatic processing of personal data"*. This provides the officer with pro-active powers during the planning stages, and thus allows for a data protection input prior to a management decision on how to implement a particular data processing project.

The duties of the data protection officer - as seen by the supervisory authorities

According to Dr. Breinlinger, German supervisory authorities have recognised such a wide interpretation of the internal data protection officer's tasks as essential. For example, the supervisory authority of the state of Baden-Würtemberg has listed as the first two tasks for officers to:

- provide advice on issues of data protection and data security to the company management and to individual organisational units within the company;
- participate in the development and implementation of data processing programs/systems, as well as provide input for the technical and organisational measures necessary for the implementation of data protection provisions.

Monitoring the proper use of data processing programs [Section 37(1)1] is only mentioned as a third point.

The relationship with the supervisory authority

Besides the activities of the internal data protection officer, data protection compliance is further controlled by the supervisory authority who, according to Section 38(2) *"shall monitor observance of [the BDSG] and other data protection provisions."* Although not laid down by law, it is usual for the internal data protection officer to be present during such an investigation. Any absences would appear to the authority as though the officer is either not taking his/her task seriously or something is being covered up.

When exercising its monitoring powers under Section 38(2), the supervisory authority usually addresses the tasks and effectiveness of the company's data protection officer. In doing so, the following issues are normally discussed:

- the date and manner by which the officer was recruited;
- professional training and experience of the officer;
- further training in view of the responsibilities as internal data protection officer;
- if the officer fulfils this function on a part-time basis, attention will have to be paid to his/her main activities and the time spent on them;
- data protection related actions taken by the officer so far, such as monitoring and control,

training and awareness raising of employees, participation in company planning related to data protection, participation in resolving data protection incidences, participating in the choice of employees.

In this type of process it is important that officers are able to provide the supervisory authority with evidence of their activities, so that any doubts the authority may have in relation to their effectiveness and reliability may be reduced.

Speaking from a supervisory authority's point of view, Dr. Breinlinger believes that auditing and monitoring the activities of the internal data protection controller is an essential task for the authority. Effective data protection control from within a company is, at present, the most important pre-requisite for proper implementation of data protection law. The external control exercised by the supervisory authority cannot do without efficient internal control.

The main weaknesses in German data protection

In practice, the relationship between an internal data protection officer and the supervisory authority differs from case to case and it is thus difficult to draw general conclusions on how well officers fulfil their tasks. In addition, only businesses processing data for the purpose of communication to third parties are under a legal obligation to supply the name of their data protection officer to the authority [see Section 32(2)5]. In other words, in most cases the supervisory authority is unaware of whether the internal officer is fulfilling his/her duties or even whether such an officer has been recruited at all.

In the annual report of the supervisory authority for the land of Hesse, both the failure to recruit officers and their lack of expertise in data protection matters are mentioned as the main data protection weaknesses. The issue of inadequate data security implementation only comes in third place. Reports from authorities in other lands confirm these findings.

It appears that these weaknesses are related to the size of the business. Smaller enterprises such as small and medium enterprises (SMEs), law firms or medical practices often fail to recruit data protection officers. Although larger organisations usually employ internal data protection officers, they are often allowed insufficient time to carry out their tasks properly. Frequently, the function of data protection officers is fulfilled by the company lawyers which is often unsatisfactory since they tend to have insufficient knowledge of technical matters and of the company's internal organisation. Only large businesses tend to pay enough attention to the implementation of data protection law and provisions.

Setting an example for other countries?

Dr. Breinlinger notes that the general weaknesses of internal data protection compliance are particularly striking if measured against the high requirements laid down by the German Data Protection Act. This does not mean, however, that the Act is too demanding. Dr. Breinlinger believes that too much freedom is being given to individual businesses on how to organise the work of the internal data protection officer, in particular in relation to the actual time spent by the officer on the delegated tasks. Sufficient time and necessary independence of data protection officers are prime pre-requisites for efficient and effective internal data protection control.

The self-regulation model is unique as laid down in the federal data protection law. However, it should be of interest to organisations outside Germany, since it addresses the vital question of effective data protection compliance in the private sector.

The regulation of data protection should not be limited to the enactment of legislation, but must be made more effective by adopting other measures complementing general data protection legislation. The combination of legislation setting out the fundamental legal principles together with more specific self-regulatory tools allows for a hierarchy of measures and a comprehensive data protection approach. From that point of view alone it is interesting to examine the German model and consider how it works in practice.

[1] Breinlinger A. *Kontrolle des Datenschutz-beauftragten aus Sicht der Aufsichtsbehörden* Recht der Datenverarbeitung, 1/1995 pp. 7-10, Staatsanzeiger für Baden-Würtemberg Nr. 1/2 of 09.01.1993.

This report was written by Caroline Laske, M.A., LL.M., Legal Consultant, Free University of Brussels, Belgium.