Improving self-regulation through law-based Corporate Data Protection Officers

Report by Christoph Klug

THE RISE OF GLOBALISATION and multinational corporations is creating a pressing need for more effective self-regulation in the data protection sphere. The role of Corporate Data Protection Officer could help to achieve this goal.

The EU Data Protection Directive and national legislation in a growing number of Member States allow for the appointment of corporate data protection officers (DPOs). Since 1977, German law has prescribed that companies of a certain size must appoint a data protection officer. Irrespective of legislative measures, more and more multinational companies throughout the world are now realising the advantages of installing their own privacy chiefs.

The German Model

Germany is one of three EU member States to have enacted the DPO concept in their new law. In the Netherlands and Sweden the appointment of a DPO is optional. After the EU Data Protection Directive was implemented in Germany in May 2001, the German legislature took the opportunity to strengthen the principle of corporate self-monitoring, especially with regard to exemption from notification. Based on past experience, the new federal German data protection law now extends the obligation to appoint a DPO to the public sector. In certain states (Bundesländer), the installation of a DPO in public authorities is optional.

The EU Directive has not only impacted the Member States but also non-EU countries, where companies (for exemptions see *PL&B Int*, Dec 1998, p.4) have to ensure adequate protection for personal data transferred there, according to Article 25 (1) so as to avoid disruptions in transborder data flows. However, ensuring compliance with data protection provisions and a customer-oriented handling of personal data are two sides of one coin. With growing awareness of the need for on and offline data protection and privacy in a global information society, the role of corporate data protection officers becomes increasingly important. Regardless of their legal basis, data protection officers (Germany, Netherlands), personal data representatives (Sweden) and corporate privacy officers (US), have one thing in common: they are specialised guardians of fundamental privacy rights and thus contribute to customer and employee satisfaction.

Origins of the corporate DPO concept

As a result of globalisation, the number of companies with multinational activities is growing. Consequently, more personal data is being transferred from one country to another. Multinationals may wish to harmonise the level of protection on a worldwide basis and thus facilitate transborder data flows. This can be done effectively by self-regulatory means (global codes of conduct, global privacy policies).

Self-regulation has already played a role in Germany since the DPO concept was established for the pri-vate sector via the 1977 Data Protection Act (BDSG). The underlying rationale was to strengthen effective self-monitoring so as to make state supervision and controls unnecessary as far as possible and thus reduce administrative bureaucracy. In accordance with the European Directive, the German law prescribes independent supervisory authorities. Once companies have installed a corporate compliance institution, authorities intervene only when a breach is suggested and after the DPO has first checked the legality of an operation.

The corporate DPO plays a key role vis-à-vis the controller as he is in charge of the many different legal, technical and organisational problems linked to processing personal data. He closely interacts with the management and other staff and, if necessary, with data protection authorities. The past 25 years have proven the self-regulatory approach to be useful in guaranteeing both effective data protection and reasonable economic freedom (see note 2).

The EU Directive

In 1994, the German EU delegation in Brussels convinced the European Commission to give Member States the opportunity to adopt the German model. In fact, the Directive virtually promotes the principle of corporate

self-monitoring by allowing for exemptions from notification and new tasks of the DPO. According to Article 18 (2), Member States may provide for the simplification of, or exemption from, notification where the controller, in compliance with the national law, appoints a personal data protection officer, responsible in particular for:

• ensuring in an independent manner the internal application of the national provisions taken pursuant to the Directive

• keeping a register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2).

Article 20 (2) of the Directive enables the Member States to charge the corporate DPO with the new obligation of prior checking. Prior checks are required when processing operations are likely to present specific risks to the rights and freedoms of data subjects. By enacting these provisions with the Directive, the European Union has expressed confidence in decentralised data protection controls and has also emphasised the necessity of avoiding unsuitable administrative formalities.

Formal Appointment

In principle, all bodies that collect, process or use personal data by automated means have to appoint a DPO with a written job specification. Non-public bodies, however, are only bound to do so if they employ more than four people on such activities.

Companies where personal data is collected, processed or used by non-automated means, and where at least 20 people are employed for that purpose on a regular basis must also install a DPO. Non-public bodies which perform automated processing subject to prior checking or collect, process or use personal data in the course of business for the purpose of disclosure or anonymous disclosure (such as list brokers, inquiry offices or market researchers) are required to appoint a DPO irrespective of staff numbers.

Smaller businesses not legally bound to appoint a DPO often do so anyway, relying on an employee who holds another job in the firm. The companies thus benefit from the exemption from notification to the supervisory authority. Violations of the obligation to appoint a DPO are punishable by a fine of up to 25,000 Euro.

Tasks and Duties – Supervision and Compliance

The DPO's main task is to carry out an independent inspection of the processing operations involving personal data such as customer and employee data. As a compliance institution, he is supposed to ensure that personal data is handled in accordance with all relevant data protection provi-sions covering on and offline processing operations.

Prior checks by the DPO are required when processing operations are likely to present specific risks to the rights and freedoms of data subjects. In these cases, automated processing operations may take place, only when the DPO – if necessary, in cooperation with the data protection authority - has confirmed the lawfulness in advance. Furthermore, he has to keep an eye on the technical and organisational measures necessary to ensure the implementation of the data protection provisions. Where proc-essing is carried out on behalf of a controller, the DPO of the controller has to supervise the processor, especially with regards to security measures.

Lawful Processing

Personal data may not be collected, processed or used for automated processing or processing in non-automated filing systems if the data subject objects and inquiry reveals that their legitimate personal interests outweigh the data controller's interest in collection, processing or use. Also, if data subjects object vis-à-vis the data controller to the use of their data for marketing purposes, the objection has to be heeded.

Data subjects are becoming more and more aware of their privacy rights, in part due to modern technologies that enable data controllers to generate detailed personality profiles, sometimes used for business and marketing purposes.

Corporate Privacy Provisions

If the DPO is also appointed by affiliated organisations, they have to supervise their processing operations also. Of course, the affiliates have to provide the necessary staff to support them in performing their duties. In larger multinational organisations where a DPO is in charge for the entire group of companies, they can be involved in drawing up a code of conduct which the group may wish to adopt to establish the same level of protection in all affiliated companies or to facilitate transborder data flows. In such cases, he usually has to ensure compliance with internal provisions as well. Furthermore, the DPO can be asked to review data protection contracts.

Transparency and Data Subject Rights

According to Article 21 (2) of the EU Directive, companies have to provide a register of certain processing operations that may be inspected by any person (Principle of Transparency). DPOs receive notification of processing operations that would otherwise go to the supervisory authority. Upon request, the DPO has to make this information available to the data subject. The data subject may also actively request specific information about data concerning him from the controller. The DPO is in charge of providing this information as well.

If approached for marketing purposes, market research or opinion polling, the data subject must be informed of the identity of the data controller and of their right to object. This right also applies when the data is held by a body unknown to the data subject, for example, a list broker. The data subject must be able to find out the origin of the data.

Employees are not always aware of the employer's rules or guidelines concerning the use of modern technologies and their ability to monitor certain actions. In this context, the principle of fair informa-tion practices becomes relevant. Only if employees are informed that certain workplace activities are monitored (Internet surfing, e-mailing, etc.), may they act appropriately.

Employee information and training

People employed in data processing may not collect, process or use personal data without authorisation and one of the DPOs tasks is to ensure all relevant employees are committed to maintaining confidentiality. The DPO also has to take steps to familiarise staff with data protection provisions and with particular data protection requirements relevant to each case, including information about administrative or criminal offences.

Qualifications

DPO qualifications requirements are vague at best. The job is restricted to those who possess the expertise and reliability necessary for the duties in question. A GDD (German Association for Data Protection and Data Security) study has revealed the following prerequisites:

- adequate knowledge of data protection law
- adequate knowledge of technical standards
- basic knowledge of business-related economics
- specific knowledge of company structures and processing operations

Independent Status

According to the EU Directive, the DPO must be in a position to exercise his function in complete independence. The data controller must enable him to do so by granting him the necessary powers and means, staff, premises, facilities, equipment and resources. The DPO has the right to demand information and may inspect data and documents.

Once appointed, the DPO makes his own professional judgements in the area of data protection. His career opportunities within the company may not be damaged when he does what the law requires. The necessity of this kind of protection becomes evident with regard to his task of prior checking. According to Section 4d paragraph (6) of the new German Data Protection Act, the DPO has to refer to the supervisory authority when he is uncertain about the lawfulness of the processing, for example, of sensitive personal data.

Generally, both the company and the DPO can be held liable for non-compliance with privacy provisions. However, in Germany, the DPOs liability is limited to intentional violations and severe negligence. He is not liable in cases where he has accurately informed the company's decision makers about existing grievances, which they then ignore.

Conclusions

Self-regulation in the field of data protection has major advantages. Data protection controls, for example, can be improved. After all, with the appointment of a corporate DPO an additional compliance institution, directly involved in processing operations and closely connected to senior officers, is established. The DPO is a knowledgeable contact person for the supervisory authorities, the management and the data subject. The appointment of a corporate DPO who is granted the necessary independence, and who has good qualifications and professional ethics, contributes to customer confidence.

As part of a global privacy strategy, the presence of a knowledgeable contact person within the data exporter as well as the data importer is essential in order to ensure lawful transfers of personal data from one country to another. Multinationals with an internal compliance department in charge of global privacy management can improve and harmonise the level of protection on a worldwide basis, thus facilitating transborder data flows.

Christoph Klug is an attorney at law for the German Association for Data Protection and Data Security (GDD). He can can be contacted by e-mail at: klug@GDD.de. Visit the website at: www.GDD.de

Notes:

1. Hans Juergen Kranz, New Tasks for the Corporate Data Protection Officer under German Privacy Law - Compliance Institution within the Global Information Society, DuD 1999, 463; for the English translation, contact hans-juergen.kranz@dlh.de

2. Suggestions (including a summary in English) on how to develop self-regulation and the role of the DPO, are available at: www.datenschutz-berlin.de

An unofficial English translation of the German BDSG-Act (2001) is available at: www.datenschutz-berlin.de

An English version of the Dutch Personal Data Protection Act (unofficial translation) can be found at: www.cbpweb.nl

For information on the International Association of Privacy Officers (IAPO) see: http://privacyassociation.org

Information on the European Privacy Officers' Network can be found at: www.privacylaws.com, or E-mail: sandra@privacylaws.com