

# ***Improving self-regulation through (law-based) Corporate Data Protection Officials\****

Article by Christoph Klug\*\*

***The rise of globalization and multinational corporations is creating a pressing need for more effective self-regulation in the data protection sphere. The role of corporate data protection officials could help to achieve this goal. The EU Data Protection Directive (95/46/EG) and national legislation in a growing number of Member States allow for the appointment of corporate data protection officials. Since 1977, German law has prescribed that companies of a certain size must appoint a data protection officer (DPO). Irrespective of legislative measures, more and more multinational companies throughout the world are now realizing the advantages of installing their own privacy chiefs.***

## **I. Origins of the Corporate DPO Concept**

Data protection and privacy have become global issues. As a result of globalization, the number of companies with international activities is growing and modern technologies simplify transborder data flows. As opposed to national privacy legislation, the global networking of economic processes has no geographical borders. A self-regulatory approach in the data protection sphere may help to bridge the gap. Self-regulation has already played a role in Germany since the DPO concept was established for the private 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. However, with a corporate compliance institution in charge, interventions of the authorities can be reduced considerably. The corporate DPO plays a key role as he is in charge of the many different legal, technical and organizational problems linked to processing personal data. He reports directly to the head of the data controller, closely interacts with the staff and is the contact person for the data protection authorities and data subjects. The past 30 years have proven the German approach to be useful in guaranteeing both effective data protection and reasonable economic freedom.

---

\* Revised version of publication in *PRIVACYLAWS & BUSINESS INTERNATIONAL NEWSLETTER*, ISSUE NO 63, June 2002, p. 28.

\*\* Attorney at Law (Germany); Deputy Executive Director of the German Association for Data Protection and Data Security (GDD).

## II. The EU Directive

In 1994, the German EU delegation in Brussels helped to convince 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 official, 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), thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

Article 20 (2) of the Directive enables the Member States to charge the corporate DPO with the 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 decentralized data protection controls and has also emphasized the necessity of avoiding unsuitable administrative formalities.

The Directive has not only impacted the Member States but also non-EU countries, where companies have to ensure adequate protection for personal data transferred there, according to Article 25 (1) so as to avoid disruptions in transborder data flows. 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 officials becomes increasingly important. Regardless of their legal basis, data protection officers (France<sup>1</sup>, Germany<sup>2</sup>, Hungary<sup>3</sup>, Luxemburg<sup>4</sup>, Netherlands<sup>5</sup>), data protection officials (Slovakia<sup>6</sup>), personal data representatives (Malta<sup>7</sup>, Sweden<sup>8</sup>), persons responsible for the protection of personal data (Estonia<sup>9</sup>) and corporate privacy officers (US<sup>10</sup>) have one thing in common: they are specialized guardians of fundamental privacy rights and thus contribute to customer and employee satisfaction. Meanwhile, the European Commission<sup>11</sup> and the Art. 29 Working Party<sup>12</sup> recommend the

---

<sup>1</sup> Data Protection Act and Decree in English <http://www.cnil.fr/english/official-texts>; see also <http://www.afcdp.net>

<sup>2</sup> English translation of the German BDSG-Act at <http://www.bfdi.bund.de>

<sup>3</sup> English version of Act LXIII of 1992 on the Protection of Personal Data and Public Access to Data of Public Interest at <http://www.obh.hu>

<sup>4</sup> English translation at <http://www.cnpd.lu>

<sup>5</sup> English version of the Dutch Personal Data Protection Act at <http://www.cbpweb.nl>

<sup>6</sup> English text at <http://www.dataprotection.gov.sk>

<sup>7</sup> Data Protection Act at <http://www.dataprotection.gov.mt>

<sup>8</sup> English version of the Swedish Personal Data Act (1998) at <http://www.datainspektionen.se>

<sup>9</sup> English translation of the Personal Data Protection Act at <http://www.aki.ee/eng>

<sup>10</sup> Information about the International Association of Privacy Professionals (IAPP) is available at <http://privacyassociation.org>

<sup>11</sup> COM(2003) 265 final – Report, p. 18 and 24

appointment of DPOs. For good reasons the Working Party has stated the following: “When considering the opportunity of generalising data protection officials, that is, shifting from administrative to internal supervision, appropriate attention should be made both to the experience gathered by the Member States with the application of the law and to the local legal culture.” In this context the working Party relates to the positive findings reported by the Member States in which data protection officials have been already introduced or have existed traditionally.

### **III. The German Model**

It has already been pointed out that experiences with the DPO in Germany are positive and this supported an implementation of the DPO concept in the EU Directive. Today, Germany is only one of several EU member states to have enacted the DPO in their data protection law. In Estonia, France, Luxemburg, Malta, 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 and the task of prior checking. Based on past experience, the German Federal Data Protection Act has extended 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 following prerequisites characterize the principle of corporate self-monitoring according to the revised German Federal Data Protection Act (BDSG):

#### **1. Formal Appointment**

In principle, most bodies that collect, process or use personal data by automated means have to appoint a DPO in written form. Non-public bodies, however, are only bound to do so if they regularly employ more than nine people on such activities. Companies where personal data is collected, processed or used by non-automated means, and where at least twenty 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 may 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.

Also an individual from outside the data controller may be entrusted with the office. For business groups it may be useful to appoint a DPO, who is responsible for the affiliates as well. In these cases the DPO is generally supported by designated assistants from the affiliated businesses, which may also be located in other countries. Public bodies may, with the approval of their supervisory authority, appoint a civil servant from another public

---

<sup>12</sup> WP 106, p.22 and 23

body as DPO.

Violations of the obligation to appoint a DPO are punishable by a fine of up to fifty thousand Euro.

## **2. Tasks and Duties**

In fulfilling his duties, the DPO closely interacts with the various business units/departments and, if necessary, with the head of the controller. A detailed up to date register of all relevant data processing operations should be the basis for his work. In cases of doubt, he may consult with to the supervisory authority.

### ***a. Supervision and Compliance***

#### ***aa. Lawful Processing***

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 provisions 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 organizational measures necessary to ensure the implementation of the data protection provisions. Where processing is carried out on behalf of a controller, the DPO of the controller has to supervise the processor, especially with regards to security measures.

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 the 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 the modern technologies that enable data controllers to generate detailed personality profiles, sometimes used for business and marketing purposes.

#### ***bb. Corporate Privacy Provisions***

If the DPO is also appointed by affiliated organizations, he has to supervise their

processing operations also. Of course, the affiliates have to provide the necessary staff to support him in performing his duties. In larger multinational organizations where a DPO is in charge for the entire group of companies, he can be involved in drawing up Binding Corporate Rules (BCRs) which the group may wish to adopt to establish the same level of protection in all affiliated companies and 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.

### ***b. 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. If personal data are recorded for the first time for one's own purposes without the data subject's knowledge, the data subject shall generally be notified of the recording, the type of data, the purpose of collection, processing or use and the identity of the data controller. It belongs to the DPO's duties to make sure that such notification is granted, unless notification is not required because of certain exemptions. The data subject may also actively request specific information about data concerning him from the controller.

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 information practices becomes relevant. Only if employees are informed that certain workplace activities are monitored (Internet, e-mailing etc.), may they act appropriately.

The DPO has to maintain secrecy regarding the identity of the data subject and any circumstances from which the data subject's identity could be inferred, unless he is released from this obligation.

### ***c. Employee Information and Training***

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

## **3. 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<sup>13</sup> study has revealed the following prerequisites:

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

#### **4. 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. A recent amendment of the German Federal Data Protection Act (BDSG) explicitly mentions the obligation of the data controller to allow and pay for an adequate education of the DPO. He also has the right to demand information and may inspect data and documents. The DPO must be informed before new processing operations are implemented.

Once appointed, the DPO makes his own professional judgement in the area of data protection. He reports directly to the head of the public or non-public body and 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 German Data Protection Act, the DPO must refer to the supervisory authority when he is uncertain about the lawfulness of the processing, for example, of sensitive personal data. If the management, upon report of the DPO, disagrees with him and considers the processing as undoubtedly lawful, it may not wish the intervention of the authority. In such cases the DPO faces no disadvantages because of his legal opinion. An amendment to the German BDSG Act in 2009 has clarified that the DPO is protected against dismissal. An appointment as DPO may only be revoked for important reasons or, alternatively, in the case of non-public bodies, at the request of the supervisory authority.

Generally, both the company and the DPO can be held liable for non compliance with privacy provisions. However, in Germany, the DPO's 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.

---

<sup>13</sup> Gesellschaft für Datenschutz und Datensicherung e.V. (German Association for Data Protection and Data Security); more information about the organization at <http://www.gdd.de>

## **IV. Conclusions**

Self-regulation in the field of data protection has major advantages. By installing a corporate DPO, administrative bureaucracy can be reduced and data protection controls become more efficient. After all, with the appointment of a DPO an internal compliance institution, directly involved in the processing operations and closely connected to senior officers, is established. Furthermore, the DPO is a knowledgeable contact person for the controller, staff, supervisory authorities and the data subject.

As part of a global privacy strategy, the presence of a data protection expert 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 data protection official in charge of global privacy management can improve and harmonize the level of protection on a world wide basis, thus facilitating transborder data flows.

More and more leading companies around the world are realizing the benefits of installing their own privacy chiefs. For many of them data protection has developed from a mere safeguard with respect to individual rights to a competitive edge issue with consumers. In other words “privacy sells”.

The EU Data Protection Directive virtually promotes the principle of corporate self-monitoring. Meanwhile, the European Commission and the Art. 29 Working Party recommend the appointment of DPOs. After all, compliance with data protection provisions can most effectively be granted by coexisting administrative and corporate compliance institutions.

# *Advantages of installing Corporate Data Protection Officers*

## Data protection controls can be improved

*Two compliance institutions instead of one*

DPO (internal)

- familiar with company structures and processing operations
- knowledgeable contact person for controller, staff, supervisory authorities and data subjects

Supervisory authority (external)

## Supervisory authorities can be unburdened

*Corporate privacy management (self-monitoring, compliance)*

*Notification to the DPO (less administrative bureaucracy)*

*Prior checking (corporate initiative with a DPO in charge)*

## Global privacy management

*Facilitating transborder data flows*

- knowledgeable contact person within data exporter and importer  
harmonized level of protection in multinational organizations (BCRs)
- global enforcement

## Privacy as a competitive advantage

*Corporate privacy management (own privacy chief)*

*Customer satisfaction (privacy sells)*