Gesellschaft für Datenschutz
und Datensicherheit e. V.

German Association for Data Protection
and Data Security

CONTRIBUTION TO

CONSULTATION ON THE COMMISSION´S

COMPREHENSIVE APPROACH ON PERSONAL DATA PROTECTION

IN THE EUROPEAN UNION

COM(2010) 609 final

I. INTRODUCTION

The German Association for Data Protection and Data Security (GDD) was founded in 1977 and stands as a non-profit organization for practicable and effective data protection. With more than 2200 – mostly company – members the GDD is Germany`s leading privacy association. Besides offering various member services such as education, training and certification of Data Protection Officers, guides for practitioners and networking opportunities for data protection professionals all across Germany, the GDD also represents member positions at a national and European level, especially as far as new privacy legislation is concerned.

In addition to the contributions already made (Stakeholders' Conference 2009, Public Consultation 2009, Stakeholders' Consultation 2010), the GDD welcomes the opportunity to make some additional remarks on the Communication from the Commission - COM(2010) 609 final.

II. REDUCING THE ADMINISTRATIVE BURDEN

The GDD welcomes the Commission`s intention to reduce administrative burdens, especially with regard to the current notification system. At the same time, the GDD shares the Commission`s view according to which administrative simplification should not lead to an overall reduction of the data controllers' responsibility in ensuring effective data protection.

In previous contributions the GDD already pointed out the necessity to improve internal control mechanisms and welcomes the Commission`s intention to spell out appropriate obligations in more detail.

From a GDD point of view, the reduction of administrative burdens can be balanced by strengthening the role of the Data Protection Officer. Appointing a Data Protection Officer is not an additional burden for controllers. Companies in Member States have to comply with data protection law anyway and "somebody has to do the job".

III. STRENGTHENING THE ROLE OF THE DATA PROTECTION OFFICER (DPO)

1. Perspective of the Commission

According to Communication COM(2010) 609 final, the Commission will consider to enhance data controllers' responsibility by

- *making the appointment of an independent Data Protection Officer mandatory, while reflecting on the appropriate threshold to avoid undue administrative burdens, particularly on small and micro-enterprises;*

- *harmonising the rules related to the Data Protection Officer`s tasks and competences.*

2. Mandatory Data Protection Officer

a) Growing acceptance of the DPO around the world

As expressed in previous GDD contributions, Germany has made good experiences with the Data Protection Officer within the past 30 years and DPOs are becoming increasingly accepted by Member States and by companies around the world.

On the occasion of the 31st International Conference on Data Protection and Privacy data protection authorities from over 50 countries approved the "Madrid Resolution" on international privacy standards. One of the most relevant chapters of the document is the one that refers to proactive measures. It includes the recommendation to appointment Data Protection or Privacy Officers, with adequate qualifications, resources and powers for exercising their supervisory functions adequately.

b) Appropriate threshold

Making the DPO mandatory at EU level could help to achieve the goal of improving internal control mechanisms. The GDD agrees with the Commission on the necessity of avoiding undue administrative burdens, particularly on small and micro-enterprises. However, the ***number of persons employed*** for the purpose of processing personal data is only one of several

factors that should be taken into account. After all, the risks to the rights and freedoms of the data subjects depend on the circumstances of the individual case.

With regard to a possible obligation to appoint a Data Protection Officer, the GDD suggests to also take into account the following criteria:

- ***Amount of personal data being processed***

Companies processing large amounts of personal data are more likely to put the rights and freedoms of the data subjects at risk than companies only dealing with a minimum of personal data. Generally, companies where the processing of personal data is a major part of the overall business purpose (e.g. internet or telecommunication service providers) have a higher risk potential, because of the large amounts of personal data being processed.

The same applies to companies processing personal data on behalf of their clients. The GDD agrees with the Commission that internal control mechanisms are especially important *"in those increasingly common cases where data controllers delegate data processing to other entities (e.g. processors)."* Even if the controller remains responsible in such cases, it is essential to have a knowledgeable contact person within the processor.

- ***Purpose of processing operations***

A higher risk potential could also be attributed to companies which commercially carry out automated processing of personal data for the purpose of transferring them to other parties (e. g. companies trading mailing lists). The same applies to organizations processing personal data for market or opinion research purposes.

Generally, the profiling of personal data – e.g. by credit agencies – involves specific risks for the rights and freedoms of the data subjects.

- ***Sensitivity of data***

According to the German Federal Data Protection Act (BDSG), the obligation to appoint a DPO applies in all cases where prior checking is required. That may include the processing of sensitive data according to Article 8 (1) of EU Directive (95/46/EC). Health data, for example, are being processed not only by hospitals but also by insurance companies. Also the financial sector highly depends on a confidential handling of personal data (e. g. with regards to bank or credit card information).

c) Alternative: The DPO as an option

In case the Commission decides not in favor of a mandatory DPO, the GDD recommends the following:

Also with regard to harmonization, the function of DPO should be reflected in the laws of each Member State, at least as an option. This view is also shared by the French organization AFCDP (Association Française des Correspondants à la Protection des Données). In France, since the data protection law has made this function optional to data controllers, the number of DPOs but also of other data protection professionals has grown, to the benefit of the protection of personal data and the spreading of a culture of privacy in the country.

Companies making use of the option to appoint a DPO should benefit from real incentives, since the DPO will ensure more effective data protection, thus unburden the DPA.

2. Harmonizing / specifying the role of the DPO

The Directive 95/46/EC is not very specific with regard to the role of DPOs, their appointment, their tasks, their independent status and their qualifications. German law includes much more detailed information on the role of the DPO which may serve the Commission as a source of information (for an overview see article by *Christoph Klug*, Improving self-regulation through - law-based - Corporate Data Protection Officials; available at http://www.gdd.de/international/english).

In addition, the GDD would like to make the following recommendations:

Appointment: In some Member States there is an obligation to register the appointed DPO with the Data Protection Authority (DPA). Some DPAs keep a list of the appointed DPOs which is publicly available. In favor of harmonization and transparency for DPAs and data subjects an EU wide obligation to register the appointed DPO with the competent DPA could be considered.

Tasks and duties: The GDD once again (see previous contributions) emphasizes the necessity to clarify that generally prior information of the DPO about all processing operations involving personal data and – where necessary – prior checking are legally binding requirements.

The recent revision of the e-Privacy Directive introduced a mandatory personal data breach notification covering, however, only the telecommunications sector. This provision was already transposed in German law. The German legislator even went a step further by amending a general provision on breach notification to the Federal Data Protection Act (Section 42a BDSG) which covers the entire private sector. Given the fact that the Commission will examine the modalities for extending the obligation to notify personal data breaches to other sectors, it should be clarified that the DPO should belong to the prevention and emergency team and that the DPO should become involved in the notification procedure.

Complete independence: In order to enable the DPOs to perform their job effectively they have to be guaranteed the necessary powers, means, premises, facilities, equipment and

resources. Once appointed, the DPOs should be in a position to make their own professional judgement. Regarding their independence, it is essential for DPOs to have the right to directly report to the board of directors, respectively to the company management. According to German law the DPO "shall be directly subordinate to the head of the public or private body".

Generally, the role of the DPO should not be reduced to a mere compliance function. With the growing risks for the rights and freedoms of data subjects the DPO`s role should become more influential and more strategic.

Qualifications: Only qualified DPOs may perform their increasingly important job effectively. Therefore, a future directive should include at least some essential job prerequisites.

The GDD conducted a study on the necessary qualifications.

The results of the study have recently been confirmed by German DPAs http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/24112010-MindestanforderungenAnFachkunde.pdf?

According to the GDD study the DPO should have

- a profound knowledge of data protection law,
- an adequate knowledge of IT standards,
- the ability to establish a proper data protection management, based on an adequate knowledge of business related economics and a specific knowledge of the company`s inner structures and processing operations.

Based on this study, the GDD has developed an educational program for data protection professionals, including a certification program for DPOs (GDDcert).

Since 2009, the German Federal Data Protection Act includes a provision according to which the controller must allow and pay for an adequate education of the DPO.

IV. DATA PROCESSING WITHIN – INTERNATIONAL – BUSINESS GROUPS

The Commission aims to *clarify and simplify the rules for international data transfers*.

In addition to the contributions already made, the GDD would like to mention that the German Government (BT-Drs. 17/4230) shares the view of the Federal Council (Bundesrat - BR-Drs. 535/10) according to which questions arising from the processing of personal data within business groups need further investigation and need to be discussed in connection with the revision of the European Directive (95/46/EC).

Bonn, January 7th 2011