ReedSmith

German Data Protection Authorities Set Minimum Competency and Independence Requirements for Company Data Protection Officers

Author: Moritz N. Wagner, LL.M. Associate, Munich
Author: Nick Tyler, Associate, London
Author: Katharina A. Weimer, LL.M. Associate, Munich

Publication Date: December 23, 2010

By joint resolution of 24/25 November 2010, the German data protection authorities ("DPAs") have set minimum requirements for the competency and independence of company data protection officers ("DPOs"). The initiative follows inspections carried out within companies that revealed a generally insufficient level of competency among DPOs, and of data controllers' organizational framework and resources for data protection compliance, given the increasing complexity of automated processing of personal data and the requirements of the Federal Data Protection Act.

The DPAs emphasize that a DPO's workload and responsibilities depend in particular on the size of the data controller, the number of data controllers supervised by the individual DPO, particularities of industry-specific data processing, and the level of protection required for the types of personal data being processed.

The resolution sets out the following minimum requirements with respect to competency and independence of DPOs, as well as to the data controllers' organizational framework and resources for data protection compliance:

DPO - Competency Requirements

The Federal Data Protection Act generally requires that individuals must have the necessary knowledge and expertise in order to be appointed DPO. Given the increased requirements for the DPO position, DPOs must have the following minimum knowledge of data protection law, as well as technical and organizational know-how:

General data protection law - regardless of industry sector and size of the data controller

- Basic knowledge of the constitutionally guaranteed personal data privacy rights of data subjects and employees of the data controller.
- Comprehensive knowledge of the Federal Data Protection Act as applicable to the data controller, including technical and organizational know-how.
- Knowledge of the application of relevant data protection and technical provisions, in particular of the data security principles and requirements set forth in the Federal Data Protection Act.

Industry-specific - depending on industry sector, the data controller's IT infrastructure and size, and the sensitivity of the personal data being processed

- Comprehensive knowledge of special statutory provisions relevant to the company.
- Working knowledge of information and telecommunication technology, as well as data security (e.g., physical security, cryptography, network security, malicious software, and security measures).
- Basic business knowledge (e.g., human resources, controlling, accounting, sales, management, marketing).
- Knowledge of the data controller's technical and organizational structure, as well as their interdependencies, including company policies and procedures.
- Expertise in the practical aspects of data protection management (e.g., conducting audits, strategy and policy development, drafting documentation, compiling inventories, conducting log-file analysis, risk management consultancy, analysis of security concepts, advising on the use of CCTV, and cooperation with works councils, including advice on works-council agreements).

As a rule, a DPO should possess the necessary minimum legal, technical and organizational knowledge **at the time of his appointment as DPO**. The DPAs stress that such knowledge may in particular be developed and kept up to date during the DPO's tenure through appropriate training, professional development seminars and exams.

ReedSmith

DPO - Independence Requirements

The Federal Data Protection Act provides that DPOs must be independent in the exercise of their functions as far as data protection is concerned. In order to guarantee the DPO's independence, the following needs to be ensured:

- The DPO must be directly accountable to the data controller's executive board, and he must be able to exercise his functions without any conflict of interest.
- The DPO may not have any disadvantage with respect to his other employment because of the exercise of his functions as DPO, including cases where the appointment as DPO has been withdrawn. If an external DPO is appointed, the service contract must provide for such notice periods, payment terms, indemnifications, and documentation obligations as are necessary in order to ensure the DPO's independence.
- The DPO is bound by confidentiality with respect to data subjects and any circumstances that may reveal their identity, unless otherwise specifically authorized by the data subject concerned.

Data Controller - Organizational Framework and Resources for Data Protection Compliance

- The DPO must have full access and inspection rights in all company areas.
- The DPO must be involved in all relevant business planning and decision-making processes relating to personal data processing.
- In maintaining the data processing inventory, the DPO must be provided with all necessary documentation and information.
- In order to maintain the appropriate competencies, the company must enable the DPO to participate in professional educational seminars and events, and cover the costs associated with such training and professional development.

— In conducting his data protection functions, an internal DPO must be guaranteed sufficient workload capacity to enable him to discharge that role effectively in light of his other functions and duties.

— Data controllers must provide appropriate support and resources to the DPO, in particular by providing personnel, office space, equipment, technology and other means of discharging their duties.

The resolution should be read as a warning from the DPAs that companies must not view the appointment of a DPO as a simple formality, but must ensure that the DPO has sufficient competency and independence and is provided with the necessary support and resources to do their job effectively. The resolution also shows that DPAs will increasingly monitor compliance with these requirements.

Non-compliance with DPO requirements may lead to administrative fines of up to € 50,000 - not only if a company fails to appoint, where legally required to do so, any DPO at all, but also if the appointed DPO does not have the necessary competencies and independence.

About Reed Smith

Reed Smith is a global relationship law firm with more than 1,600 lawyers in 23 offices throughout the United States, Europe, Asia and the Middle East.

This Client Alert was compiled up to and including December 2010.