

Appointment of a Data Protection Official (DPO)

Compliance with German Data Protection Law

Protection of Personal Data

Everyone has the right to the protection of personal data concerning him or her.

Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

Compliance with these rules shall be subject to control by an independent authority.

- Article 8 Charter of Fundamental Rights of the European Union -

German legislation has established two control instances for data privacy compliance. All companies processing personal data, except for small businesses, have to assign a data protection official (DPO). In addition, each state of the federation has installed a data protection authority (DPA) as supervising entity.

Data Protection Official

Every German company that processes personal data may have to appoint a DPO. As a general rule, the appointment of a DPO is required and only very small business may be exempted from such obligation. In this context, the term 'data processing' stands, in particular, for the collection, storage, modification and transfer of personal data (e.g. name, address, telephone number, email, bank account, photos, performance reports etc.). Resulting from this broad definition the processing of personal data forms an integral part of most businesses.

The obligation to appoint a DPO applies in particular if,

- the processing company commercially transfers personal data (address trade, marketing database), i.e. commercially carries out automated data processing of personal data for the purpose of transfer, transfer in anonymous form or for purposes of market or opinion research;
- 10 or more employees of the processing company constantly handle automatic processing of personal data;
- 20 or more employees of the processing company regularly handle non-automatic processing of personal data.

Even if only one part of the employee's work consists of data processing, this work is considered to constitute handling of data processing as stated above.

Where a company's automated processing operations present special risks to privacy

For further information on German data protection law, please contact us:

Bryan Cave LLP

Hanseatic Trade Center
Am Sandtorkai 77
20457 Hamburg
Tel: +49 (0) 40 30 33 160
or through the direct link to
our website bryancave.com

Your personal contact:

Jana Fuchs

jana.fuchs@bryancave.com
+49 (0) 40 30 33 160

rights a DPO has to be assigned irrespective of the number of employees concerned.

Such special risks could result e.g. from the processing of special categories of personal data (sensitive data) or if the processing of personal data is intended to assess the data subject's personality, abilities, performance or behavior.

Appointment of the DPO

The DPO needs to be assigned in writing within one month after the beginning of business operations.

Qualification as DPO

The assigned DPO has to be an adequately qualified and reliable person. The requirements for the DPO's qualification are extensive and vary for every individual case as it depends very much on the scope of data processing performed by the company and also its business field.

Minimal requirements can, however, be summarized as follows:

General Requirements

- Basic knowledge of constitutional privacy rights
- Comprehensive knowledge of applicable terms of the German Data Protection Act including technical and organizational expertise
- Knowledge of the scope of data protection and technical requirements, data privacy principles and data security requirements according to § 9 of the German Data Protection Act

Branch specific requirements

The branch specific requirements depend on the business branch, the size of the business or its

IT infrastructure and on the sensitivity of the processed data.

- Comprehensive knowledge of data protection provisions applicable to the specific business of the company
- Expertise in information- and telecommunication technology as well as data security (e.g. physical security, cryptography, network security, malware and protection measures)
- Basic competence in business economics (HR-Management, Controlling, Finance, Sales, Management, Marketing, etc.)
- Knowledge of the technical and organizational structures of the assigning company
- Expertise in practical data protection management (e.g. experience with control measures, consulting, strategy development, analysis of security concepts, shop agreements, cooperation with works council, etc.)

In general, the above qualifications have to be fulfilled at the time the DPO begins his or her assignment. It is therefore recommended to organize sufficient education programs for the future DPO in order to ensure initial qualification as well as appropriate trainings during the time of the assignment.

Independence of DPO

German data protection law requires that the DPO acts independently, i.e. he or she is not bound by management instructions. In order to ensure such independence the processing company has to install specific structures. For example:

- DPO shall report directly to the management of the company

- DPO shall not be discriminated as a result of the engagement as DPO
- DPO shall not disclose personal information to the management of the company without the concerned person's consent

Organization of the company

In order to ensure that the DPO is able to perform his or her duties the company is obliged to provide an appropriate structure. For example:

- DPO shall have access to all business departments and premises as far as such access is necessary for the performance of the DPO tasks
- DPO shall be included in all relevant management decisions.
- DPO is obliged to create and update the register of processing information and shall be given all information required for this task
- Company shall provide and pay sufficient training and education programs
- Company must grant appropriate working hours to the DPO for the performance of the DPO tasks and for educational purposes. For example if the DPO is also a regular employee the company has to reduce prior working hours.

Protection for the DPO

German law grants the DPO the privilege that during the time of the assignment ordinary termination of the employment is prohibited. Termination may only be served for severe cause. Even if the DPO appointment is revoked the concerned employee is exempt from ordinary termination for one subsequent year.

In-House DPO / Outsourcing

With regard to the extensive requirements outlined above, many companies find it difficult to find a qualified

in-house person to act as DPO for them. Smaller businesses often try to assign the additional tasks to an existing employee, who is often not adequately qualified. Irrespective of the size of a company adequately qualified employees, who could in principle do the job are often needed for less administrative positions. Companies have to consider that depending on the effort needed to perform the DPO duties the concerned employee is not available for other business needs. No conflicts to the DPO duties may arise, should the DPO also serve as employee in another position.

Another option is to employ a DPO solely for this position either full or part time. Given the termination protection and the costs of such new employment companies often hesitate to take such a step.

DPO obligations may also be outsourced allowing an external assignee to supervise internal data processing (e.g. certified attorneys or certified DPO service providers). Service agreements with external DPO have to ensure the DPO's independence, e.g. by having fixed-term agreements.

Liability of the DPO

Under strict provisions, the DPO can be personally liable for breaches of compliance. Such personal liability is usually covered by an insurance.

DPA

For small companies which are not required to assign a DPO, the local DPA is the only responsible control instance. In addition, the DPO is entitled to address the DPA in cases of doubt to seek reassurance of his or her evaluation.

Information Duties

To enable the DPA to perform supervision, the companies are generally obliged to notify the DPA about their data processing tools and security measures. Such notification duty does generally not apply if a DPO has been assigned. The precise information duties are extensive and complex and could be set out in further detail upon request. They could e.g. include a duty to notify about breach of data protection regulation.

Consequences of Violation

- Violation of the duty to appoint a DPO could cause different legal consequences, in particular, monetary fines up to EUR 300.000 for regulatory offences and possibly more if the economic benefit of the breach exceeds this amount.
- Personal liability for management executives in case of data security breaches.
- Duty to notify DPA of the company's data processing tools.
- Loss of business opportunities because German business partners may request proof of compliance.

Summary

- Be aware that usage of personal data is generally restricted.
- Determine whether your company is required to assign a DPO.
- Find adequate and reliable DPO.
- Review internal data processing for compliance with your DPO.
- Address local DPA in cases of doubt.
- If your company is not required to assign DPO, find adequate consultancy to ensure compliance.
- Instruct your employees to ensure compliance.
- Install and observe necessary data protection measurements.

Bryan Cave LLP makes available this information letter for informational purposes only. The information is general in nature and does not constitute individual legal advice. Further, the use of the information provided herewith does not create any attorney-client relationship between us.

About Bryan Cave

Bryan Cave LLP (www.bryancave.com) has a diversified international legal practice. The firm represents a wide variety of business, financial, institutional and individual clients, including publicly held multinational corporations, large and mid-sized privately held companies, partnerships and emerging companies. Aided by extensive investments in technology, Bryan Cave's more than 1,000 attorneys across the United States, the United Kingdom, Continental Europe and Asia serve clients' needs in the world's key business and financial markets.

Bryan Cave LLP makes available this information letter for informational purposes only. The information is general in nature and does not constitute individual legal advice. Further, the use of the information provided herewith does not create any attorney-client relationship between us.