Defining the role of the European data protection officer

European businesses are being urged to appoint data protection officers within their organisations, but EU member states differ on how they define the role. **Florence Raynal**, **Fabrice Naftalski** and **Dr Stefanie Hellmich** compare and contrast the approaches taken in two countries - Germany and France.

According to the EU Data Protection Directive, companies appointing a "Personal Data Protection Official" (the data protection officer) should benefit from simplification or exemption from the notification process with national data protection authorities. The data protection officer is defined as being in charge of ensuring in an independent manner the implementation of national data protection laws internally and of keeping a register of data processing carried out by the company.

Despite a growing success within multinational organisations, the function of a data protection officer is not subject to a uniform regime in the European Union (EU). This aspect should be taken into consideration, especially for multinationals thinking of having national data protection officers responsible for compliance in their EU entities.

Germany and France are both interesting illustrations of those differences.

For example, while the German experience, through a well-established and regulated function, makes the data protection officer a mandatory element for most companies, the current French data protection bill seems to provide an optional system, still subject to controversy and whose exact status would need to be further defined by sub-regulations.

This article outlines the current status of data protection officers in Germany and in France, and highlights their similarities and differences.

How is the function of data protection officer regulated?

In Germany - German data protection legislation places particular emphasis on the self-regulatory mechanism within companies. The institution of the 'data protection officer' constitutes an important element within this self-regulatory mechanism and has an established tradition within German data protection and privacy legislation. The 'data protection officer' was introduced into German law with the enactment of the first Federal Data Protection Act in 1977 and has been maintained in the re-enactments of the same law in 1990 and 2001.

Germany - A data protection officer has to be involved if new data processing systems or procedures are introduced, or if company practices impose specific risks for customers or staff.

In France - The data protection officer does not have yet any legal grounds in French law. However, some leading multinational companies have already adopted the practice of appointing a data protection officer for their French branches or subsidiaries. An Administrative Circular enacted in March 1993 also recommended that public sector bodies adopt a similar approach.

The practice of appointing data protection officers will probably be addressed in French law following the bill implementing the EU Data Protection Directive (95/46) which will update the existing data protection law enacted in 1978. The Senate has overcome the reluctance of the French National Assembly to implement such a practice with the following three arguments:

- The appointment of a data protection officer corresponds to the implementation of Article 18 of the EU directive and the recommendations of the OECD.

- Successful examples from European (eg. Germany, the Netherlands, Sweden, and Slovakia), non-European countries (the US and South Korea) and the French public sector, demonstrate the appropriateness of such a practice.

- The identification of illegal databases, through the training of the data protection officer within companies, is preferable to increasing controls by additional administrative bodies. [Please note that such provisions of the bill are still under discussion and would be supplemented by implementing decrees after its adoption.]

What is the function of the data protection officer?

In Germany - As an independent body with investigative and advisory functions, the data protection officer supports the company with regard to data protection and privacy matters and complements the activities of the competent supervisory authority. The officer is the point of contact for the

competent supervisory authority and for employees with regard to queries concerning the data processing activities of the company.

The data protection officer must ensure compliance with the applicable data protection provisions. For this purpose, the officer monitors the proper use of data processing activities that involve personal data, and takes suitable steps to familiarise staff employed in the processing of personal data with the applicable data protection provisions. In cases of doubt, the data protection officer must contact the supervisory authority.

The data protection officer must be supported by the management of the company; in particular, the officer shall be provided with an overview of the details concerning the data processing activities within the company. Such data includes information on the people responsible for data processing, the data categories that are processed, the purposes of use, any transfers to third parties and third countries, and the technical and organisational security measures implemented within the company.

This information - with the exception of the technical and organisational security measures and the persons authorised to access the data - has to be made available to any interested party upon request. Furthermore, a data protection officer has to be involved if new data processing systems or procedures are introduced, or if company practices impose specific risks for customers or staff.

The importance of the data protection officer's role is underlined by the fact that a company may, in principle, be exempt from notifying its data processing activities to the relevant supervisory authority. Notification remains obligatory only for those companies which perform data processing activities with specific risks for the individuals affected.

In France - As required by the French bill, the data protection officer must provide a list of the data processed within his or her company to any party requesting such information.

Other information to be provided upon request includes the type and purpose of the data concerned, the contact details of the data controller, the function of the individual or department responsible for implementing access rights, the categories of personal data processed, the categories of recipients and, where applicable, the data transferred countries outside the European Economic Area (EEA).

The data protection officer is also required to carry out controls in respect of compliance with data protection law.

The bill does not provide for any specific obligations by the data controller towards the data protection officer or for any obligations by the data protection officer towards the French National Data Protection Commission (CNIL).

The appointment of a data protection officer should exempt the data controller from providing information to the CNIL on the data processing activities within his or her company, provided that the data processed is not subject to any authorisation (by the CNIL or other administrative bodies) and that no data is transferred outside the European Union.

Who has to appoint a data protection officer?

In Germany - Public authorities and private companies that collect, process or use personal data are required to appoint a data protection officer. Such appointments must be made within one month of commencing the processing activities. The same applies where personal data is processed by other means (ie. in non-automated files) and at least 20 persons are permanently employed for this purpose. As an exception to this rule, companies with a maximum of four employees collecting, processing, or using personal data do not have to appoint a data protection officer.

Nonetheless, in the case of entities carrying out automated processing operations and processing or using personal data in the course of business for the purpose of a transfer or anonymous transfer to another company or entity, a data protection officer has to be appointed irrespective of the number of employees.

In France - The French data protection bill states that the appointment of a data protection officer will be optional. If a company decides to appoint a data protection officer, the CNIL and the entity's Works Council (Comité d'Entreprise) will have to be informed about the appointment.

France - If a company decides to appoint a data protection officer, the CNIL and the entity's Works Council (Comité d'Entreprise) will have to be informed about the appointment.

It should be noted that, pursuant to the French Labor Code, the Works Council must also be informed or consulted with respect to any technologies used in the recruitment of employees, to any data processing relating to the management of employees, and any surveillance or monitoring used to control employees' activity at work, prior to its implementation.

The above measures will make the data protection officer a preferred point of contact for the CNIL and employees with respect to queries concerning data protection and the data processing activities of the company.

Who may undertake the role of a data protection officer?

In Germany - The duties and functions of a data protection officer may be performed by an employee of the company (an "internal data protection officer") or by a third party engaged for such a purpose (an "external data protection officer"). Also companies may undertake the functions of an external data protection officer.

Only persons possessing the special knowledge and demonstrating the reliability necessary for the performance of the duties concerned may be appointed as data protection officers. They are obliged to extend their knowledge on a

continuing basis. A proliferating number of seminars is offered to the market to respond to this practical need.

In small and medium sized companies, employees are commonly assigned the function of a data protection officer on a part time basis besides their primary responsibility/function in the company. However, the role of the data protection officer must not be incompatible with the other responsibilities of the employee within the company. The head of the IT department, for example, would not be eligible for the role of data protection officer due to potential conflicts of interest.

In France - The French bill only stipulates that the data protection officer should have the professional qualification required for the performance of his or her duties. It does not provide details on how to assess, obtain, or monitor such a professional qualification. The Parliamentary debates stress the important role played by foreign data protection authorities in the training of their domestic data protection officers (eg. telephone hot lines, special websites, conferences and training sessions).

It is likely that the CNIL will also be involved in the training of data protection officers. This is a good way for the supervisory authorities to stay up-to-date with recent practices regarding personal data processing in companies.

In this respect, it should be noted that the CNIL must be informed of any appointment and consulted in cases where data protection officers are dismissed by their employer. The CNIL will also have the right to request the dismissal of a data protection officer. These provisions, in effect, provide the CNIL with powers of control regarding data protection officers.

How is a data protection officer appointed and what is his standing within the company?

Germany - The data protection officer is appointed by a formal act. He may be appointed for a definite or for an indefinite period of time. However, the period must not be too short as to impede any constructive work. Generally, a period of at least two years is considered necessary in order to ensure long term control and consistency of the work. The appointment of the data protection officer itself is not subject to the consultation and approval of the Works Council.

The appointment may only be revoked by the company for an important reason, such as continued non-compliance of duties or a breach of serious obligations. The company may therefore not terminate the appointment by regular notice of termination.

The data protection officer in exercising his functions and responsibilities is directly subordinate to the management of the company and shall be free to use his knowledge. He may not suffer any disadvantage through the performance of his duties. The company shall make available any resources necessary for the performance of his duties. In spite of this legally prescribed standing, in practice, conflicting interests between the data protection officer and the company or simple budget constraints may render it difficult to tackle data protection compliance gaps or to improve compliance to the required level outlined by the data protection officer.

> the French [data protection] bill will grant the data protection officer the right to refer any problems in the performance of his or her duties to the CNIL.

In France - The French bill provides direct and indirect safeguards with regard to the independence of the data protection officer within the company:

- The data protection officer's employer (ie. the data controller) will be prohibited from imposing penalties on them in connection with their data protection duties. This direct protection is limited in practice because data protection officers may be subject to other disadvantages or penalties in connection with their other responsibilities within the company.

- The indirect safeguards are related to the notification of the data protection officer's appointment to the CNIL and the Works Council. The CNIL's advice will also be solicited before any decision by the employer to dismiss a data protection officer. Moreover, the French bill will grant the data protection officer the right to refer any problems in the performance of his or her duties to the CNIL. This will enable the data protection officer to indirectly use the CNIL's powers, which have been reinforced by other provisions of the bill. Data protection officers may be dismissed by their employers following a breach of legal obligation and following prior consultation with the CNIL.

IN CONCLUSION

Although the German and French approaches to data protection officers have some significant differences (in the roles and the direct benefits to the company), there are also significant similarities. The longer history of the German data protection officer provides us with an example and a model on which to build our approaches to implementing the expected requirements of the French law. Multinationals may decide to institutionalise the role of data protection officer throughout their European business units, even though the legal treatment afforded to the role may vary from country to country.

AUTHORS: Florence Raynal (florence.raynal@fr.eylaw.com) is part of the European coordination team and the French data protection practice of EY Law.

Fabrice Naftalski (fabrice.naftalski@fr. eylaw.com) is also involved in EY Law's French data protection practice.

Dr Stefanie Hellmich (stefanie.hellmich @de.eylaw.com) represents EY Law's German data protection practice.