

Whistleblowing hotline guidelines for Germany

By Dr. Alexander Niethammer, Associate, Heisse Kursawe Eversheds, www.heisse-kursawe.com

Unlike other countries in Europe (e.g., France), Germany has no official binding rules on the admissibility of whistleblowing hotlines. However, the ad hoc working group on "Employee Data Protection" of the Düsseldorfer Kreis ("Working Group") has recently issued a report on whistleblowing hotlines and data protection. Although the recommendations in this report have no binding character, they will materially influence the embodiment of whistleblowing hotlines, because the various data protection authorities in Germany normally adopt these recommendations.

The Working Group which exists of representatives of the data protection authorities of the private sector in Germany generally accepts the establishment of such hotlines to report misconduct as an addition to internal management. For the application of the general legal principles on whistleblowing hotlines, the Working Group qualified the following groups as breaches of codes of conduct:

- Group 1: Conduct which constitutes a criminal offence against the interests of the company (in particular fraud and misconduct relating to accounting and internal accounting controls, auditing matters, corruption, banking and financial crime and prohibited insider trading);
- Group 2: Conduct breaching human rights (e.g., exploitation of favourable production conditions abroad in the form of child labour) or environmental interests;
- Group 3: Conduct which adversely affects company ethics (e.g., *Wal-Mart Case* – Decision of the Düsseldorf Regional Employment Court of 14 November 2004).

The Working Group concluded that the admissibility of whistleblowing hotlines under German data protection law requires the balancing of the interests of the company against the interests of the data subjects. The Group further determined that in the case of processing of personal data being connected with the uncovering of breaches of Group 1 and 2 conducts above ("hard factors"), it might be regarded as lawful. The reason for this is that the interests are generally weighed in favour of the legitimate interests of

the company as the reporting of such breaches helps to avoid legal consequences in the form of, for example, prosecution, compensation claims and defamation. In contrast, in the case of conduct that falls under Group 3 above ("soft factors"), it is assumed that the interests of the data subjects prevail and the processing of such data is unlawful.

As a consequence, internal company guidelines on whistleblowing schemes should mirror this distinction between Group 1 and 2 and Group 3 conducts when defining the purposes of the reporting system. Unless a case-by-case analysis provides otherwise, the Working Group suggests that personal data with regard to Group 3 conduct should not be collected in the framework of whistleblowing systems.

It is also important to mention that the Working Group seriously questions the general validity of individual consent given by the data subjects in an employment relationship. In this regard the Working Group adopts the findings of the E.U. Article 29 Data Protection Working Group and has the opinion that consent cannot be given freely due to the hierarchical relationship between the company and its employee.

The Working Group recommends anonymous reports only in exceptional cases, because it promotes misuse and denunciations. As a consequence, the Group suggests procedures that ensure that the identity of the whistleblower is kept confidential during all stages of the investigation. Further, the whistleblower should be informed on the first contact with the system that his/her identity will be treated confidentially.

German law provides that if personal data is processed for the company's own purposes, such data shall be erased as soon as the knowledge thereof is no longer required. The Working Group clarified this rule with regard to data received in the framework of a whistleblowing system and recommended that such data should be destroyed within two months after conclusion of the investigation. Storing the data for a longer period of time may only be legitimate until further legal measures, such as disciplinary proceedings or the enforcement of criminal proceedings, have been clarified. Personal data which can be regarded without substance has to be deleted without undue delay.