

NOTICE: This is an English translation of the guidance on Whistleblowing Hotlines issued by the regional German data protection authorities' Ad-hoc Working Group on Employee Data Protection, referred to as the "Düsseldorfer Kreis," at its meeting in Hamburg on April 19-20, 2007. The original German is posted on the Hamburg data protection authority site at: <http://fhh.hamburg.de/stadt/Aktuell/weitere-einrichtungen/datenschutzbeauftragter/informationsmaterial/wirtschaft/whistleblowing.html>

This translation is an unofficial one of the World Law Group - Privacy Matters (www.theworldlawgroup.com), Co-Chaired by Mark E. Schreiber, Edwards Angell Palmer & Dodge LLP, Boston (mschreiber@eapdlaw.com) and Christian M. Runte, CMS Hasche Sigle, Munich (christian.runte@cms-hs.com), and was prepared by CMS Hasche Sigle. It is provided for informational purposes only and should not be relied upon as an official translation or as authoritative. Closed brackets [] are used to signify inserted material to clarify the text.

Whistleblowing – Hotlines: Internal Warning Systems and Employee Data Protection

Report of the Ad-hoc Working Group on "Employee Data Protection" of the Düsseldorfer Kreis

A. Introduction

Whistleblowing hotlines are options offered by companies to their employees to report misconduct of other employees to the company. Reporting such misconduct implies the collection, transfer and storing of personal data. If such data are to be processed in automated or non-automated files, the provisions of the data protection laws must be complied with. The whistleblowers and the incriminated persons are the main groups involved. The Article 29 Data Protection Working Party (national data protection authorities for the EU Member States) summarized the data protection law objectives and rules arising from the EC Data Protection Directive in an Opinion adopted on 1 February 2006 on whistleblowing schemes (in the following: Opinion WP 117).¹

The report of the "Employee Data Protection" Working Group of the Düsseldorfer Kreis is limited to the assessment of the admissibility under data protection law of the automated collection, processing and use of personal data in reporting procedures using whistleblowing hotlines in accordance with the provisions of the German Data Protection Act (Bundesdatenschutzgesetz - BDSG). The transfer of personal data to third countries [outside the EU] - for example on the basis of the Sarbanes-Oxley Act (SOX) - is not subject to assessment under data protection law of this report.

B. Breaches of company codes of conduct

As a rule, internal procedures to report misconduct (whistleblowing) are established as a result of the need to introduce reliable management principles for the daily operation of the company. Whistleblowing procedures to report misconduct are intended as an additional mechanism for employees to report misconduct internally through a specific channel. They complement the regular information and reporting channels of the establishment, such as employee representative bodies, line management, quality assurance personnel or internal auditors who are appointed for the sole purpose of reporting such misconduct. Whistleblowing is

¹ Opinion 1/2006 from Article 29 Data Protection Working Party, can be downloaded from Internet at: www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_en.pdf

only an addition to internal management and not a replacement thereof.² When introducing codes of conduct, employment law requirements must also be taken into consideration and co-determination rights of the works council must be complied with.

The following qualify as breaches of codes of conduct:

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),³
2. conduct breaching human rights (e.g., exploitation of favorable production conditions abroad in the form of child labor) or environmental interests,
3. conduct which adversely affects company ethics (see the Wal-Mart case).⁴

C. Data flow in the case of whistleblowing

When breaches against codes of conduct are reported, personal data relating to individuals are collected, processed and stored. The data collected include data relating to the person incriminated, the (alleged) breaches of conduct and the details relating thereto. If the reporting procedure states that reports may be anonymous, no personal data are recorded about the whistleblowers, unless the whistleblowers themselves state otherwise. Otherwise the personal information which may be recorded could include the name of the whistleblower, his/her position in the company and, where appropriate, the circumstances under which he/she made his/her observations. Depending on the structure of the reporting procedure, this data may be used internally by the relevant department (e.g., auditing, compliance); in the case of affiliated companies it may also be the case that the personal data is transmitted to the parent company or to other companies in the group.

D. Legal principles

If personal data is processed in automated or non-automated files, the collection, processing and use of the personal data are only legitimate in cases in which the German Data Protection Act or another legal provision permits or requires this or the parties involved have given their consent thereto (§ 4 (1) of the German Data Protection Act).

1. Contractual relationship pursuant to § 28 (1) sentence 1 no. 1 of the German Data Protection Act

The prevailing opinion is that § 28 (1) sentence 1 no.1 of the German Data Protection Act does not apply because the employment relationship is not directly affected by the data collection organized or attributed to the management. What does apply is § 28 (1) sentence 1 no. 2 of the German Data Protection Act.

² Opinion WP 117, III. -p. 6-.

³ Opinion WP 117, IV. No.1 ii) -p. 9-.

⁴ Decision of the Düsseldorf Regional Employment Court dated 14 November 2005 - 10 TaBV 46/05 – (Wal-Mart); see also provisions regarding anti discrimination in the General Equal Treatment Act dated 14 August 2006 (BGBl. I p. 1897).

2. Consideration of interests pursuant to § 28 (1) sentence 1 no. 2 of the German Data Protection Act

2.1 Requirement to safeguard legitimate interests of company

The establishment of whistleblowing reporting procedures may be considered necessary to realize a legitimate interest pursued by the data controller or the third party to whom the data is disclosed. The goal of ensuring financial security in international financial markets and in particular the prevention of fraud and misconduct with respect to accounting, internal accounting controls, auditing matters, as well as the fight against bribery, banking and financial crime or insider trading, appears to be a legitimate interest of the employer that justifies the processing of personal data by means of whistleblowing systems in these areas.⁵ However, such data processing would only be permissible if the legitimate interests of the data subjects in [having the company] refrain from the data processing do not prevail.

2.2 Legitimate interest of the data subjects

In a whistleblowing case there is a risk of victimization and stigmatization of the incriminated person.⁶ A review of the legitimate interests of this person will have to be made especially carefully, [particularly] in the case of specific events leading to the suspicion that relevant misconduct has taken place. The processing of personal data connected with the uncovering of breaches as set out in sections B.1. and B.2. above ("objective criteria") may be regarded as legitimate. As a rule, the interests are weighed in favor of the legitimate interest of the company as the reporting of such breaches helps to avoid legal consequences in the form, for example, of prosecution, compensation claims and defamation if the procedure is structured so as to comply with data protection provisions (section E).

In the case of conduct which falls under section B.3. above ("soft criteria") the legitimate nature can only be appraised on a case by case basis. It should be noted in this respect that certain conduct may not qualify from the outset for an appraisal or consideration of interest.⁷

For this group [section B.3.] it is assumed that the legitimate interests of the data subjects involved are compelling. Employment law principles must also be complied with. The soft criteria of the internal codes of conduct (e.g., "to be friendly when dealing with customers") are generally not clearly defined, so that it is difficult to identify a breach. Moreover, a connection between the breach and considerable loss for the company (comparable with the categories described in sections B.1. and B.2. above) cannot be identified so that at this point doubt arises as to the legitimate interest of the data controller. Therefore in such cases it can be assumed in principle that there is a compelling legitimate interest of the data subjects involved, and the processing or use of the personal data is not legitimate in this respect.

3. Special legal provision pursuant to § 4 (1) of the German Data Protection Act

A works agreement that contains rules of conduct can only be considered as a special provision of law if the collection, processing and use of the data is adequately and precisely regu-

⁵ Opinion WP 117, IV, No. I ii) -p. 9-.

⁶ Opinion WP 117, III. -p. 7-.

⁷ Decision of the Düsseldorf Regional Employment Court dated 14 November 2005, NZA 2006,63. The court's view is that the issue "Private relationships / love affairs" is in breach of Art. 1 and 2 of the German Constitution and therefore invalid.

lated – within the permitted scope of the German Data Protection Act - and if it does not fall short of the level of protection set by the German Data Protection Act.⁸ The mere description of a function does not suffice even if personal data has to be processed to accomplish it. However, in such cases it may be used to weigh the legitimate interests of the controller against the legitimate interest of the data subject concerned in having the data not being processed or used.

4. Consent of parties involved pursuant to § 4a of the German Data Protection Act

The validity of consent to commence such procedure would have to be linked, among other things, to the requirements of its voluntary nature and of informing [the data subject] of the collection, processing and use of the data. It is doubtful as to whether consent can be granted voluntarily in an employment relationship. In an employment relationship, one cannot regularly assume that consent has been given freely due to the hierarchical relationship between the company and its employee.⁹

E. Data protection structure of a reporting system using hotlines

1. Principles

Personal data must be collected for fixed, clear purposes and may not be further processed or used in a manner not already agreed (§ 28 (1) sentence 2 of the German Data Protection Act). The data processed must also correspond to the purposes for which it is collected and/or processed, be necessary and may not exceed requirements. The structure and selection of data processing systems must be geared towards collecting, processing or using as little personal data as possible. In particular, the information must be recorded anonymously or pseudonymously in as far as possible and the time spent must be in due proportion to the intended purpose (§ 3a of the German Data Protection Act). The controller must ensure that inappropriate or incomplete data are erased or rectified. Clear, unambiguous information must be provided relating to the purposes pursued by a whistleblowing hotline. To avoid misunderstandings, not every irregularity, including slight or presumed irregularities, should be reported. It must be clear that there is no value in [having] unspecified incriminating reports.

2. Persons concerned

In accordance with the principles of minimal personal data collection and avoidance [of unnecessary data collection], the data controller will review the extent to which the group of people to whom irregularities are reported can be confined and specified for a whistleblowing hotline. The company which introduces a whistleblowing procedure will also carefully review whether it would be appropriate to restrict the number of persons to whom irregularities can be reported, in particular given the severity of the alleged breaches reported.¹⁰ However, the circumstances in each individual case will be determinative.

3. Anonymous or personal reference

The Article 29 Data Protection Group recommends accepting anonymous reports (i.e., also information) only in exceptional cases. Anonymity contradicts the principle of transparency, and - compared with identifying names - promotes misuse and denunciations. A person who

⁸ Bergmann/Möhrle/Herb, § 4, para. 24; Simitis, German Data Protection Act, Commentary, 6th ed., § 4, para. 16, 17.

⁹ Opinion WP 114, Chap. 2.1 -p.13-.

¹⁰ Opinion WP 117, IV. No. 2i) - p. 11-.

is the subject of anonymous whistleblowing is not able to defend himself/herself against defamation in formal and constitutional proceedings. On the other hand, a system based on the collection of personal data from [only identified reporters] has the disadvantage [that some reports] are deterred, even though the desired information is obtained. This should be weighed against anonymous information, especially as anonymous information can be given at any time without a whistleblowing hotline. Special emphasis should be placed upon appropriate guarantees for the protection of the whistleblowers from discriminatory or disciplinary measures.¹¹

When weighing the said interests, the following procedure is to be recommended: whistleblowing procedures should ensure that the identity of the whistleblower is kept confidential. A person who would like to make a report under such a whistleblowing scheme should know that he/she will not be adversely affected by making this report. This is why the whistleblower must be informed on the first contact with the system that his/her identity will be treated confidentially during all stages of the procedure.

4. Notification and information duties

If personal data is collected from the data subject, the responsible body must state the particular purpose of the collection, processing or use of personal data provided the data has not been obtained elsewhere (§ 4 (3) of the German Data Protection Act). If works agreements have been concluded relating to whistleblowing procedures with provisions relating to the processing of personal data, the company shall interpret this to mean that all employees, even the newly hired ones, are able to become familiar with the content without great difficulty (§ 77 (2) of the Works Council Constitution Act (Betriebsverfassungsgesetz - BetrVG).¹²

4.1 Information about the incriminated person (§ 33 of the German Data Protection Act)

If the personal data is first recorded for [the company's] own purpose without the knowledge of the data subject concerned, the latter will be informed that the data has been stored, of the type of data, the specific purpose of collection, processing or use and the identity of the responsible body (§ 33 (1) of the German Data Protection Act). There is no duty to inform if the data has to be kept confidential in accordance with a legal provision or its nature, i.e., owing to the compelling legal interest of a third party (§ 33 (2) sentence 1 no. 3 of the German Data Protection Act).¹³ In cases where there is a high risk that such information could jeopardize the ability of the company to effectively investigate the accusation or to collect the evidence required, the incriminated person need not be informed until this risk no longer exists.¹⁴ In view of the possible adverse effects on the personal rights of the incriminated person and his/her defense rights, long-term non-disclosure [to the incriminated person] may not be assumed.

4.2 Information (§ 34 of the German Data Protection Act)

Under § 34 (1) of the German Data Protection Act the person involved, both the whistleblower and the incriminated person, is entitled to information relating to the data stored

¹¹ Opinion WP 117, IV. No. 1 ii) -p. 9- ; Federal Constitutional Court, decision dated 02 July 2001 – 1 BvR 2049/00 (www.bundesverfassungsgericht.de/Entscheidungen.html); see also: Müller, Whistleblowing - ein Kündigungsgrund? [a dismissal reason?] NZA 2002, 424; Breinlinger, Krader, Chancen und Risiken bei der Umsetzung von anonym nutzbaren Hinweisgebersystemen im Rahmen des Compliance-Managements von Unternehmen [Chances and risks when implementing anonymously usable whistleblowing schemes as part of internal compliance management], RDV 2006, 60; Sauer, Whistleblowing – notwendiger Bestandteil moderner Personalpolitik [Necessary part of modern HR policy], DÖD 2005, 121.

¹² Fitting, para. 25 on § 77 Works Council Constitution Act

¹³ Schaffland/Wiltfang, paras. 63 et seqq., Bergmann/Möhrle/Herb paras. 89 et. seqq. on § 33 German Data Protection Act.

¹⁴ Opinion WP 117, IV. No. 4 i) -p. 15-.

about himself or herself, including the origin and recipient of the information. The incriminated person's right to information conflicts in principle with an anonymous report provided for the whistleblowing system (see section E.3.). However, under § 34 (4) of the German Data Protection Act in cases concerning § 33 (2) sentence 1 no. 3 of the German Data Protection Act, there is no obligation to reveal the information. Therefore the essential elements for operating whistleblower hotlines - the confidentiality of the reports and thus the identity of the whistleblower - can be ensured. However, in each case the responsible body must review the details and decide under which conditions the identity of the whistleblower is revealed to the incriminated person.

5. Transfer information to third parties

In principle it is not legitimate to transfer personal data of either the whistleblower or the incriminated person to third parties. However, it must be made clear to the whistleblower that his/her identity may be disclosed to persons involved in further investigations or ensuing court proceedings commenced after inquiry.¹⁵ Rights to inspection of records in any criminal proceedings remain unaffected. Personal data of incriminated persons may be forwarded for prosecution purposes pursuant to § 28 (3) sentence 1 no. 2 of the German Data Protection Act.

6. Blocking and rectification (§ 35 of the German Data Protection Act)

Pursuant to § 35 (4) of the German Data Protection Act, the accuracy of personal data may be disputed by the data subjects concerned, and when neither the accuracy nor inaccuracy can be determined, the personal data is to be blocked. Personal data may not be collected, processed or used for automatic processing or processing in non-automatic files if the data subject concerned objects to the controller and a review reveals that the legitimate interest of the data subject – due to a special personal situation of the data subject – outweighs the interest of the controller in the collection, processing or use of the data. This does not apply if a legal provision obliges the collection, processing or use of such data (§ 35 (5) of the German Data Protection Act). Personal data shall be rectified if it is incorrect (§ 35 (1) of the German Data Protection Act).

7. Destruction of data (§ 35 of the German Data Protection Act)

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 (§ 35 (2) no. 3 of the German Data Protection Act). Generally, data should be destroyed within two months after conclusion of the investigation. Storing the data for a longer period may only be legitimate until further legal measures such as disciplinary proceedings or the commencement of criminal proceedings have been clarified. Personal data in connection with whistleblowing which are regarded as without substance by the entity responsible for handling the report have to be deleted without undue delay.¹⁶

8. Involvement of the company data protection officers

In as far as automated processing may constitute risks to the rights and freedoms of the data subjects, such processing is subject to review before processing is commenced pursuant to § 4d (5) of the German Data Protection Act (prior review). As there is no exception to the prior review obligation other than where the processing of data is obligatory by law, an auto-

¹⁵ Opinion WP 117, IV. No. 2 iii) -p. 12- .

¹⁶ Opinion WP 117, IV. No. 2 v) -p. 13/14- .

matic whistleblowing procedure must be reviewed by the company's data protection officer.

9. Instruction of outside bodies (§ 11 of the German Data Protection Act)

Data processing by third parties pursuant to § 11 of the German Data Protection Act is only possible if the agent only carries out the technical process of processing the personal data on the basis of precise instructions from the employer. Otherwise any instruction issued to outside bodies would constitute a transfer of data, the legitimacy of which is to be decided pursuant to § 28 (1) no. 2 of the German Data Protection Act. Depending on the structure of the whistleblowing system, the legitimate interest of the responsible body and the legitimate interest of data subjects involved must be weighed against one another. The legitimacy of forwarding information to outside bodies must be the subject of prior review. As a rule, if the external body is to carry out part of the investigation [following a complaint], such external body cannot be considered a data processor [in terms of § 11 German Data Protection Act]. The appointment of an external body outside the company organization (group) may be prove to be advantageous (also taking into account the data protection law provisions) because such external involvement may inhibit the risk of abusing the system.

10. Technical and organizational measures (§ 9 of the German Data Protection Act)

In order to fulfill the requirements of the annex to § 9 of the German Data Protection Act, suitable technical and organizational measures shall be taken. This applies in particular to the required confidentiality and destruction obligations. For internal data processing, it is recommended that the whistleblowing hotline should not be organized or operated within [the company's] human resources administration.¹⁷ An authorization system, password mechanism and encryption with respect to the sensitive nature of the data should be considered, as these measures would help to ensure that unauthorized persons do not have access to the relevant data processing systems.¹⁸ The measures should include recording entry of data and routines to erase data.

F. Conclusion

A reporting procedure using a whistleblowing hotline can be structured and operated in compliance with data protection laws, taking into account the purpose pursued by the company and the modalities in setting up such hotline. We recommend that those companies which intend to establish such warning systems discuss the matter at appropriate times with all parties involved (e.g., internal auditing, management officers, data protection officers, workers representative bodies). The data protection authorities can also be contacted to clarify any issues.

¹⁷ Opinion WP 117, IV. No. 6 i) -p. 17-.

¹⁸ BSI-IT- Basic Protection Manual