

C/M/S/ Hasche Sigle

Rechtsanwälte Steuerberater

Whistleblowing and Privacy Protection in Europe

**Annual CLE Conference
November 7 – 10, 2007, Philadelphia**

Gerlind Wisskirchen

CMS Hasche Sigle

Theodor-Heuss-Ring 19-21

D-50668 Cologne

Germany

Tel.: +49 (0)221 7716-140

Fax: +49 (0)221 7716-334

gerlind.wisskirchen@cms-hs.com

www.cms-hs.com

A. Legal Background in the EU	4
I. Introduction	4
II. Legal Background of whistleblower channels	5
III. Recommendations of the Article 29 data protection Working Party	5
B. Details of Individual EU-Countries	8
1. France	9
a) Data protection	9
b) Authorisation procedure.....	10
c) Practical procedure	11
d) Labour law and employee participation	11
2. Germany	11
a) Data Protection	11
b) Employee participation	12
c) Practical procedure	13
3. United Kingdom	13
a) Data protection	13
b) Notification	13
c) Employee participation	13
4. Spain	14
a) Notification	14
b) Employee participation	14
5. Netherlands	15
a) Corporate governance law.....	15
b) Notification	15
c) Employee participation	15
6. Austria	16
a) Notification	16
b) Employee participation	16
7. Belgium	16
a) Notification	17
b) Employee participation	17
8. Denmark	17
a) Notification	17
b) Employee participation	17
9. Greece	17
a) Notification	17
b) Employee participation	18

10. Ireland	18
a) Notification	18
b) Employee participation	18
11. Italy	18
a) Notification	18
b) Employee participation	19
12. Poland	19
a) Notification	19
b) Employee participation	19
13. Portugal	19
a) Notification	19
b) Employee participation	19
14. Sweden	19
a) Notification	20
b) Employee participation	20
15. Hungary	20
a) Notification	20
b) Employee participation	20
16. Czech Republic	21
a) Notification	21
b) Employee participation	21
17. Luxembourg	22
a) Notification	22
b) Employee participation	22
18. Slovakia	22
a) Notification	22
19. Switzerland	22
a) Data privacy and notification.....	22
20. Bulgaria	23
a) Employee participation	23
C. Conclusion	23

A. Legal Background in the EU

I. Introduction

Whistleblower channels as part of a Code of Conduct are becoming increasingly popular amongst US and European companies. Specifically companies listed on a stock exchange are obliged to establish a method for employees to anonymously report concerns about financial and accounting matters (whistleblowing system) and to implement a code of ethical conduct which should support the reporting of breaches of the code of conduct.

European subsidiaries of U.S. corporations have experienced problems in attempting to implement internal codes of conduct including Whistleblower channels required by their parents. Codes of Conduct venture into the domain of employee privacy which in Europe has been a cause for concern in relation to data protection laws as some companies have gone as far as to say what employees may or may not do in their spare time. In Europe such reporting systems may substantially affect the private sphere of the individuals concerned and may be contrary to European or national law as well as custom.

In Europe in general, whistleblowing systems of the type established in the United States seem strange because European ideas about data privacy protection and personality rights differ from the U.S. approach. Because of the forced whistleblowing during the Nazi-Regime in Germany and in countries being occupied during World War II, attempts to require employees to report misconducts brush up against the social norms and historical backgrounds in many countries. There has thus been a clash between the US perspective (The US have now one company in eight with such a Code of Conduct) and European ideas regarding co-determination and personality rights through enforcing these codes. Indeed the Sarbanes-Oxley Act, that was introduced in the US after the various financial scandals surrounding Enron, requires that companies failing to comply with their "whistleblowing" requirements will face hefty sanctions and therefore an EU committee set up for the purpose of examining the implementation of data protection law (the so-called Working Party) has investigated the problems of the US rules clashing with data protection rules in Europe. Without a resolution to this cross border dispute over implementation of Codes of Conduct, companies may face heavy sanctions in both, Europe and the States. Especially the implementation of "whistleblowing" schemes as a part of the Codes of Conduct will more often than not require the processing of personal data (that is, the collection, registration, storage, disclosure and destruction of data relating to an identifiable person) such that

data protection rules will come into force. The broad law is governed under the European Directive of 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The three conditions that need to be met in order to justify the processing of personal data are transparency, legitimate purpose and proportionality.

II. Legal Background of whistleblower channels

In the European Union data privacy protection is subject to the EU Directive on Data Privacy (95/46/EC) and to national legislation. Specifically subjects, such as data quality, criteria for processing personal data, access to data and conditions of data export are regulated by the EU Directive (i.e., by national laws conforming to the Directive). Workplace monitoring and questions of codetermination are still subject to national laws and court rulings. Workplace monitoring depends on fundamental rights and freedoms. Thus national differences exist in detail but the basic principles are very similar in every member state. Concerning the rights of the works council or other employee representation committees, the national rules of codetermination apply; EU legislation has little impact on this.

III. Recommendations of the Article 29 data protection Working Party

The Article 29 data protection Working Party (the Article 29 Group) consists of the data protection commissioners of the 25 member states of the European Union; on February 1, 2006 they issued a statement on data privacy protection requirements for whistleblowing systems.¹ The recommendations of the Article 29 Group aim at making it easier for companies required to implement whistleblowing systems due to the Sarbanes-Oxley Act, to structure such systems in compliance with the data privacy protection laws and thus to meet the requirements of the EC Data Privacy Protection Directive.² In conclusion, the Article 29 Group considers whistleblowing systems to be admissible, but places their admissibility under strict prerequisites. A prerequisite of Directive 95/46/EC is that either the collection of the data is necessary in order to comply with a legal obligation to which the data collecting party is subject or the processing is necessary for the realization of a legitimate interest safeguarded either by the data collecting party or the third party.

The Article 29 Group assumes that a company could have a legitimate interest in processing data by means of a whistleblowing hotline. The legitimating interest of the company, however, must outweigh the interest and the fundamental rights of the data subject. The

¹ See http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_en.pdf.

² Directive 95/46/EC = http://byds.juris.de/byds/061_9.9_95_46_EG_rahmen.html.

Article 29 Group acknowledges that large international organizations such as the European Union³ and the OECD⁴ consider “good” corporate governance an important aspect of a “well” functioning corporation. The principles, established by the EU and the OECD aim at a maximum level of transparency and stable accounting and finance systems in order to protect vested interests such as shareholders and market stability in general. In this context, the Article 29 Group recognizes the legitimate interest of companies to implement systems enabling the employees to report irregularities.

Furthermore the Article 29 Group considers the obligation to implement a whistleblowing system arising from the Sarbanes-Oxley Act to be an opportunity to increase stability of financial markets and improve protection of shareholders. In this respect, the Article 29 Group is of the opinion that the interest of a company required to implement a whistleblowing system under the Sarbanes Oxley Act is legitimate.

In addition, however, the company’s interest in the data processing has to be weighed against the rights of the data subject in a review of proportionality. For this purpose, the Article 29 Group established the following guidelines:

Limit on the number of persons to report through whistleblowing system

Applying the principle of proportionality, the Article 29 Group recommends limiting the number of potential whistleblowers. In this respect, the number of persons who are eligible can vary according to the sector involved and it may be necessary to determine in each individual case whether or not the whistleblower in question is included in the Group. The limitation can, for example be specified for certain divisions.

Limit on the number of persons who may be incriminated through a whistleblowing system

The Article 29 Group further recommends assessing whether it might be appropriate to limit the number of persons who may be reported through a whistleblowing system and in particular to take measures in order to prevent false accusations from launching an investigation and thus data processing.

³ European Community: Commission Recommendation of 15 February 2005 on the role of non-executive or supervisory directors of listed companies and on the committees of the (supervisory) board (OJ L 52, 25 February 2005, p.51).

⁴ OECD: *OECD Principles of Corporate Governance*. 2004 part one, section IV.

Encouraging identified and confidential reports instead of anonymous reports

The Article 29 Group attaches particular importance to the question of whether a whistleblower should remain anonymous or should be identified, under conditions of confidentiality. In the view of the Group, the arguments against anonymous whistleblowing include:

- The company will in any case be unable to ensure that the identity of the whistleblower is not revealed some other way, despite anonymous reports.
- It is more difficult for the company to verify allegations if it is not possible to ask follow-up questions.
- Anonymous whistleblowing may lead to the development of a culture of (anonymous) denunciation. The social climate in an organization can deteriorate if employees are aware that anonymous reports concerning them can be filed at any time.

To ensure the fair practice of data collection, the Article 29 Group therefore recommends that whistleblowing should not be anonymous. Exceptions from this rule are possible in specific cases. Companies should thus encourage the employees not to report anonymously via the hotline. Of course, this requires security for potential whistleblowers that their reports will be treated with the utmost discretion and confidentiality. The information must remain confidential throughout the whole process and must not be passed on to third parties. However, the company should make it clear that in the event of further investigations the whistleblower's identity will have to be revealed to the persons involved in the investigation.

Data processing only for the purpose of processing the report

Pursuant to the Directive 95/46/EC on the protection of data privacy, personal data may be collected only for specified and lawful purposes and may not be used in any way that is incompatible with these purposes. Given that the purpose of a whistleblowing system is to ensure good corporate governance, the data collected and processed must be related to this purpose. Therefore companies should limit any reporting via the hotline to certain areas. These can be accounting, banking and financial crime. The data processed in these areas must be limited to the data strictly and objectively necessary to verify the allegations made.

Compliance with data retention periods

To comply with the principle of proportionality, personal data should be deleted without undue delay, that is, within two months of completion of the investigation. Only if the com-

pany takes further legal action against the incriminated person or against the whistleblower in cases of false or slanderous declaration may data be kept for a longer period of time.

Clear information about the whistleblowing system

It is the duty of the company introducing the whistleblowing system to inform the potential data subjects about the existence and the purpose of such a system, the recipients of the reports and the right of access and rectification for reported persons. Furthermore, the company should notify the employees that the whistleblower's identity will be kept confidential throughout the whole investigation process, but that legal action will be taken against the whistleblower in the event of abuse of the telephone hotline.

Rights of the incriminated person

The Directive requires individuals to be informed when personal data are collected from a third party and not from them directly. The information must include the identity of the entity responsible for the data processing, the purposes of the processing, the recipients or categories of recipients of the data and the existence of the right of access to and rectification. These provisions of the directive may, however, jeopardize the ability of the company to gather more information and conduct an efficient investigation. The Article 29 Group therefore allows notification to be delayed as long as the incriminated individual is able to jeopardize the collection of evidence. The Directive gives the data subject the possibility to have access to the data registered on him/her at reasonable intervals and without excessive delay in order to check its accuracy and if necessary rectify it. The whistleblowing system must guarantee these rights. The exercise of these rights may be restricted in exceptional cases in order to protect the rights of others involved. This has to be decided on a case-by-case basis. Under no circumstances can the person accused in a whistleblower's report obtain information about the whistleblower's identity on the basis of the accused person's right of access unless the whistleblower maliciously makes false allegations against a person. The whistleblower's confidentiality should always be guaranteed.

B. Details of Individual EU-Countries

While in a number of European States, especially in Eastern Europe, there seems to be no particular discussion on the compliance of whistleblower channels with national and European data privacy protection law. There are some debates in France and Germany on how companies can comply with both the Sarbanes Oxley Act and European data privacy protection law. However, there is to date no leading prevailing opinion giving guidance for all questions arising in this context. The United Kingdom, Ireland and Poland, show lower

opposition to the system of whistleblower channels in practice and therefore have fewer problems in integrating such systems into their legal order.

1. France

In France employers must pay special attention to the correct implementation of the whistleblower channel and to the notification procedure to the CNIL. France is especially suspicious of whistleblower systems. Several courts have rendered decisions on telephone hotlines and declared the specific systems incompatible with French law.

a) Data protection

In May 2005 the French Commission Nationale de l'Informatique et des Libertés (CNIL) declared the two whistleblower hotlines of McDonald's and CEAC illegal for data privacy protection reasons⁵. But the CNIL also stated that, despite its objections in the particular cases, it accepts such systems in principle (Deliberation 2005-305, Annex). The CNIL initiated the discussion on the European level that led to the opinion of the Working Party several months later. Earlier than the Working Party, the CNIL set up a list of criteria that must be fulfilled in order to comply with French data privacy protection law⁶. In summary, these criteria are more restrictive than the exigencies established by the Working Party. It is unclear whether the CNIL will broaden its interpretations following the Working Party of February 2006 or if it will pursue a more restricted path within the margin opened by the opinion of the Working Party. The CNIL established the following criteria⁷:

- Complementary character of the whistleblower channel
- Restricted field of application
- Facultative use
- Restricted definition of persons who may be subject to incriminations
- Restricted use of anonymous calls
- Clear and complete information on the aims/scope of the whistleblower channel
- Data stored by the system to be objective, not exhaustive and explicitly presumptuous
- Collection by a specific organization within the company (or by a third party)
- Personnel involved limited by number, specially trained and bound to a greater extent than usual to data privacy protection principles
- Destruction of data two months after closure of investigation

⁵ CNIL decision 2005-110 of 26 May 2005 (McDonald's Group France); CNIL decision 2005-111 of 26 May 2005 (Exide Technologies).

⁶ Articles 6 and 7 of French law n° 78-17 of 6 January 1978.

⁷ Available under:

<http://www.cnil.fr/fileadmin/documents/uk/CNIL-recommandations-whistleblowing-VA.pdf>.

- Precise information of the incriminated person
- Respect of right of access and rectification

However, the CNIL position is still in the process of development. It is likely that under the European influence of the Working Party it will be open to compromises. Further French law requires that a whistleblower channel must be optional, not mandatory. This requirement is not contrary to SOX which merely obliges companies outside the United States to “promote” reporting by “senior financial officers” on any auditing or accounting frauds they witness.⁸ In contrast the company’s “attorneys” have to be obliged to report in this case.

b) Authorization procedure

Employers must obtain the authorization of the CNIL to operate the whistleblower channel. All automated data processing (i.e., all electronic data storage, transmission, etc) requires previous authorization by the CNIL. Whistleblower hotlines that are restricted to financial matters receive authorization without examination by the CNIL. Systems that go beyond matters concerning audit and finance will be examined by the CNIL. While the CNIL accepts whistleblower systems for financial matters and offers online a “unique authorisation”⁹ for this aim, it is more reluctant when the scope of the whistleblower channel includes other issues. Under the “unique authorisation” the following issues may be reported to the whistleblower channel:

- Accounting and account auditing disorders
- False entries
- Tax evasion
- Fictitious personnel employment
- Bribery of public agents
- Terrorism funding
- Money laundering

If employers do not restrict the channels to financial matters a so-called “unique authorisation” will be insufficient. Other facts may be reported to the whistleblower system despite their non-financial character if the particular seriousness provides justification. The CNIL outlines the following examples¹⁰:

- Threat to the safety of another employee
- Moral harassment
- Sexual harassment

⁸ Section 406 of SOX.

⁹ www.cnil.fr/index.php?id=1758

¹⁰ <http://www.cnil.fr/index.php?id=1982#10>: FAQs on whistleblowing systems: Question Nr. 10: What should the scope of the whistleblowing system be?

- Discrimination
- Insider trading
- Conflict of interests
- Serious environmental breaches or threats to public health
- Disclosure of a manufacturing secret
- Serious risks to the company's information system security

c) Practical procedure

If the employer wishes to have a quick authorization by the CNIL, he should consider re-restricting the scope of the whistleblower scheme to financial issues in order to obtain the formalized unique authorization while waiting for the lengthier standard review process of the expanded whistleblower channel.

d) Labor law and employee participation

As to labor law questions, the CNIL simply states: whistleblower channels are neither provided for nor prohibited by the French Labor Act¹¹. Several legislative provisions actively require persons to report certain specific crimes or malpractice and employees also must notify their employer if they are aware of a situation in which it may be reasonable to believe there is danger to their health or safety. Employees are also protected under French law in respect of certain disclosures. Employees who report instances of discrimination, sexual harassment or bullying cannot be subject to disciplinary measures or dismissal. The ruling of the Tribunal de Grand Instance de Libourne of 15 September 2005 clarifies that works councils need to be informed and consulted and must have an opportunity to give their opinion. Furthermore, the decision contends that the very eventuality of corporate wrongdoing violates personal rights when whistleblowers use hotlines in cases where there are only subjective assumptions and no evidence.

2. Germany

No notification to data privacy protection authorities is required in Germany; employers have to convince their company data privacy protection officer of the legality of the system.

a) Data Protection

Most of the telephone hotlines implemented in German companies allow employees to pass on information without restrictions. The Federal Data Privacy Protection Act provides that, first the employer must have a legitimate interest in the collection of data and second the employee's interest in preventing the processing or use of the data concerning him does not outweigh the interest of the employer. The opinion of the Article 29 Group pro-

¹¹ Deliberation 2005-305, Annex.

vides key points for weighing the interests of the parties involved in consideration of the need for proportionality. Taking the recommendations of the Article 29 Group into account and considering the decisions rendered by judges in France, companies should make sure when implementing a whistleblowing system that the report is not made anonymously. Further they should make sure that the content of the report is restricted to certain areas and therefore to a certain group of employees and that the whistleblower's identity is protected as far as possible. It is very likely that national courts and data protection agencies will follow the recommendations of the EU Working Party and therefore strike down any whistleblowing scheme that goes beyond the allowed scope.

b) Employee participation

The implementation of a whistleblower hotline requires the consent of the works council. The competent level is the group works council ("Gesamtbetriebsrat") since a whistleblower hotline is introduced uniformly within the whole group. A well known decision on whistleblowing via a hotline to date in Germany is the decision known as the "Wal-Mart Judgment" by the Labor Law Court of Wuppertal¹² and the subsequent application for review of a point of law filed with the Labor Court of Appeals of Düsseldorf¹³. The works council under the German Works Constitution Act needs to give its approval if the employer wishes to introduce rules that directly affect the behavior of an employee within his sphere of work at the company. Therefore the following were held by the court to be subject to co-determination with the works council:

- Code of ethics violations to be reported through an anonymous hotline
- Prohibiting, demanding, requesting or receiving gifts or special payments
- The rule that no statements were to be given to the press without consent from the company communications department
- Rules on harassment
- Company inspection rights
- Rules concerning romantic relationships
- Rules on drug and alcohol abuse
- Ban on the display of posters advertising the disallowance of accepting of gifts and reporting of violations through a hotline.

The Court of Appeal even went further by holding the "no dating rule" invalid because of the breach of general personality rights of the individual employees. The works council has joint decision-making authority with management at the introduction and operation of tech-

¹² ArbG Wuppertal, 15.06.2005, Az: 5 BV 20/05.

¹³ LAG Düsseldorf, 14.11.2005, Az: 10 TaBV 46/05; Revision to BAG is pending, Az: 1 ABR 1/06.

nical devices to monitor the behavior or performance of the employees¹⁴ and matters relating to the rules of operation of the establishment and the conduct of employees in the establishment.¹⁵ According to the Labor Court of Appeals it is irrelevant for codetermination whether the use of the hotline is voluntary or not. Failure to obtain the consent of the works council would render the introduction of the whistleblower hotline impermissible.

To implement a whistleblower channel in Germany, employers need to conclude a works agreement with the works council.

c) Practical procedure

The usual way to obtain the consent of the works council and the management is to agree upon a works agreement. Failure to reach an agreement leads to a decision of a conciliation board. Without agreement with the works council or a decision of the conciliation board, it is not possible to implement a whistleblower hotline.

3. United Kingdom

Operating a whistleblower channel does not present any major problems in the United Kingdom. Here, restrictions to the scope do not seem to be necessary.

a) Data protection

The UK Information Commissioners Office (ICO) does not follow the strict French and German point of view. It considers that proportionate use of whistleblower lines does not in principle raise concerns. However, the data privacy protection laws of the United Kingdom must be respected. These are very similar to the other European Union data protection laws but the interpretation here seems to be broader when it comes to practical application.

b) Notification

In general all data processors have to notify the data protection agency. But, there are exemptions for specific cases.

c) Employee participation

There is no general system of informing and involving employees in the United Kingdom. In England, the rights of union representatives at the establishment level (shop stewards) are based on relevant provisions in collective agreements or on voluntary agreements.

¹⁴ Section 87 No. 6 of the German Works Constitution Act.

¹⁵ Section 87 No. 1 of the German Works Constitution Act.

Therefore employers should only pay attention to whether there are any relevant provisions in collective agreements or other agreements when implementing the whistleblower channel.

4. Spain

Spanish regulations do not impose a general obligation regarding the implementation of whistleblowing procedures. But the Spanish data protection agency has published in July 2007 its position regarding whistleblowing after a Spanish company submitted a request for a ruling¹⁶. In general, the Spanish data protection agency follows the opinion of Article 29 Group.

Case law has held it to be illegal for an employer to discipline or dismiss an employee who has reported malpractice to the authorities (whether this relates to actions which are contrary to law or good faith or which violate rights protected by the Spanish Constitution). Disclosures made by employees are protected if they relate to malpractice or criminal matters. This applies regardless of whether the disclosure was made by the employee in good or bad faith. If there is a whistleblowing policy or a collective agreement dealing with whistleblowing, the procedures for reporting concerns internally as set out in that policy must be followed, provided that the disclosure does not relate to criminal malpractice. Currently this is debate in Spain on a draft of Unified Code on corporate governance of listed companies. If in future such code contains provisions for a whistleblower channel then the necessary data processing may be based on this law.

a) Notification

Every data controller is required to give notification. Here, exemptions do not apply.

Employers have to notify the data protection agency about the processing of data.

b) Employee participation

The powers and competences of the works council and the employee delegates encompass rights to be informed and to be involved. However, Spanish law does not contain provisions on genuine codetermination. The employee representatives have a right among other things to draw up reports and opinions prior to the implementation of measures by the employer that concern the introduction or change of systems, relating to work organization and monitoring (time recording systems, introduction of bonus and incentive systems, evaluation systems). In our opinion, a whistleblower channel can be deemed such a monitoring system. Employers should give the employee representatives an opportunity to draw up a report or to present their opinion prior to implementation.

¹⁶ Agencia Espanola de Proteccion de datos; Creacion de sistemas de denuncias internas en las empresas (mecanismos de "whistleblowing")

5. Netherlands

Employers should negotiate the whistleblower channel with the works council. The above-defined scope should be acceptable under Dutch data privacy protection law.

a) Corporate governance law

Besides the non-binding recommendations on whistleblowing policies (best practice provisions) in the Dutch Corporate Governance Code of 9 December 2003 (Code Tabaksblad) which protects employees who blow the whistle on their employers, the Dutch Privacy Act (Wbp) regulates data transfer. The Dutch Privacy Act has largely adopted the recommendations of the Article 29 Group. Thus, only substantial abuses are to be notified by the whistleblower channel and only if they can not be handled locally. Case law requires that employees must raise any suspicions they have with their employer first – external disclosures are only justifiable in exceptional circumstances.

b) Notification

The controller of certain data processing operations must notify the Dutch data protection agency prior to processing of data. Data can only be processed if the processing is found to be lawful by the data protection agency. However, there exists an exemption decree that provides exceptions for complaint procedures. Considering the whistleblower channel is intended as a means through which complaints may be registered, this exception applies.

Generally employers do not have to notify the Dutch data protection agency prior to data processing to receive its authorization.

c) Employee participation

The implementation of a whistleblower channel will require the approval of the works council. The legal basis for the establishment of a works council is the WOR (*Wet op Ondernemingsraden*). A works council must be established in companies having more than 50 employees. Similar to those provided for in the German Works Constitution Act, the codetermination rights can be divided into the right to be informed, the right to be heard and the right to grant approval. The rights to grant approval listed in Article 27(1) of the *Wet op Ondernemingsraden* are similar to the codetermination rights relating to social matters listed § 87(1) of the German Works Constitution Act. The right to grant approval, according to Article 17 of the *Wet op Ondernemingsraden* also applies to decisions relating to the processing of complaints. The right to grant approval also includes a veto right. If the works council decides not to grant its approval, the employer may appeal to the district court of the canton and file a petition for the court to grant approval as a substitute for the approval of the works council.

Employers should therefore contact the works council and negotiate with it to the extent necessary in order to obtain its approval.

6. Austria

In Austria employers should hear the works council prior to the introduction of the whistleblower channel. As to data privacy there are apparently no special requirements to be met.

a) Notification

Every data controller has to file a notification to the data protection commission for the purpose of registration in the data processing register before starting to process data.¹⁷

The subject matter of the notification is a “data application”. This is a notification of certain data for a specific purpose (e.g., “personnel administration”, “customer relations”, etc.).

Therefore employers have to notify the data protection commission (“Datenschutzkommission”) prior to any data processing.

The notification must include information on the data controller, purposes of data processing, data recipient, etc.. For this purpose standard notification forms are used.

b) Employee participation

In Austria the establishment of a works council is regulated by the Labor Constitution Act (*ArbVG, Arbeitsverfassungsgesetz*). The rights to be involved include rights relating to supervision, information and consultation. There is no explicit specification of approval for the processing of complaints comparable to that in Article 27 of the Dutch *Wet op Ondernemingsraden*. The supervision rights¹⁸ refer to the review of wage and salary lists, the supervision of personnel files and the implementation and observance of the provisions of laws concerning employee protection, social security and company pensions. The rights to be informed and heard with regard to social matters¹⁹ refer only to measures concerning safety issues and women as well as company training and retraining. However, a general clause²⁰ provides for a right of the works council **to be heard** with regard to all matters relating to employees. It is possible that hearing the works council with regard to the establishment of so-called help hotlines might also fall under this general language.

Employers should inform the works council. It will not ultimately be necessary to heed a refusal.

7. Belgium

To our knowledge as to data protection, no specific provisions of statutory law or case law are to be taken into account in Belgium.

¹⁷ According to §17(1) of the DP Act of 2000.

¹⁸ Based on § 89 of the Labour Constitution Act.

¹⁹ Specified in §§ 92a (1), 92b, 94 (1) of the Labour Constitution Act.

²⁰ § 90 (2) of the Labour Constitution Act.

a) Notification

In Belgium every data controller has to notify the data protection agency ("*Commission de la protection de la privée*"). But there are some exemptions. These apply if certain conditions are fulfilled. Most of these conditions have in common that they guarantee that the processing will only have a slight impact on privacy.

Employers will have to notify the data protection agency.

The notification has to include -among other things- information on the data controller, the purpose of the data processing, the legal basis for processing of particularly sensitive data and the period of time data will be kept by the data controller. Forms are available for the notification. A fee has to be also paid.

b) Employee participation

Basically the works council may not interfere with the actual management of a business. It has an advisory role and is entitled to receive information on the business operations of the company. Therefore the consent of the works council is not required.

8. Denmark

We have no comments on the particular data privacy situation in Denmark.

a) Notification

Generally all private data controllers processing sensitive data either electronically, in manual filing systems, or in a non-electronic systematic manner have to notify the data protection agency. However, exemptions do exist. We do not have detailed information about these exemptions.

Therefore, we recommend employers to notify the data protection agency.**b) Employee participation**

Codetermination rights of the employees are exercised by representatives and general committees responsible for cooperation in the business establishment, among others. In addition, the staff can be represented by labor unions. It is not apparent that Danish employee representatives would be able to prevent the implementation of the whistleblower channel.

9. Greece

We have no comments on the particular data privacy situation in Greece.

a) Notification

In general data controllers are required to give notification. However, some exemptions do exist. We do not have detailed information about these exemptions.

Therefore we recommend employers to notify the data protection agency.

b) Employee participation

Employees have a right to complete decision-relevant codetermination with regard to among others and the implementation of technology for the purpose of monitoring the conduct or the performance of employees. This right only applies if there is no labor union at the business establishment and if the relevant matter has not already been regulated by a company-level collective agreement. The work council has a codetermination right with regard to the implementation of a whistleblower channel if there is no union at the establishment and if the implementation of a whistleblower channel is not already regulated in a company-level collective agreement. Employers must then conclude a works agreement with the works council and this works agreement will have to be submitted to the competent office of the Federal Ministry of Labor and displayed on the bulletin board.

10. Ireland

Ireland has implemented EU-conform data privacy legislation. There are no peculiarities to be observed as to whistleblowing.

a) Notification

In general data controllers are required to give notification but some exemptions do exist. We do not have detailed information about these exemptions.

Therefore we recommend employers to notify the data protection agency.

b) Employee participation

There is no right of employee participation for the implementation of a whistleblower channel in the private sector of the economy.

11. Italy

In Italy employees can blow the whistle by way of complaint to their manager, to their employee representatives or even directly to the labor court. However, there is no specific whistleblowing legislation and general principles of contract and labor law need to be applied. If an employer wants to implement a specific policy, it should be circulated to employees with instructions that they should read and keep a copy of it and return a signed acknowledgement confirming receipt and consenting to the policy terms. In addition, after being translated into Italian, the policy must be posted in the employer's premises in a place where each employee can easily read and understand it.

a) Notification

In general data controllers are required to give notification. However, some exemptions do exist depending on the entity processing the data and/ or the relevant purposes. We do not have detailed information about these exemptions.

Therefore we recommend employers to notify the data protection agency.

b) Employee participation

There is no system of codetermination in Italy.

12. Poland

Poland complies formally with the EU data protection directive.

a) Notification

In principle every data controller has to notify the data protection agency unless there is an exemption from this obligation. Notification can be required prior to processing of data.

We therefore recommend employers to notify the data processing agency prior to data processing.

b) Employee participation

There is no employee participation within companies of the private sector.

13. Portugal

We have no comments on the particular data privacy situation in Portugal.

a) Notification

All data controllers have to notify the data protection agency. However, there are exemptions. All the authorizations for exemptions are issued by the data protection agency. The Data Protection Act specifies which data processing operations are submitted to prior checking. The data protection agency has to issue a formal authorization, stating the conditions under which data processing may be carried out.

Employers have to notify the data protection agency prior to data processing in order to receive its authorization.

b) Employee participation

The employee representatives have only rights to be informed to be heard and to be involved in an advisory capacity as well as improvement-related supervisory rights. There are no substantive rights to be involved, to demand restrictions or to veto or any codetermination rights that can be enforced judicially.

With regard to the implementation of a whistleblower channel, employers can be required to inform the works council in due time. In addition, the works council could have supervisory power.

14. Sweden

We have no comments on the particular data privacy situation in Sweden.

a) Notification

All data controllers except those who have appointed a personal data representative or who's processing, falls under any of the other exemptions in the Personal Data Act, the Personal Data Ordinance or the Data Inspection Board Code of Statutes.

Therefore we recommend employers to notify the data protection authority about the processing of data.

b) Employee participation

Only a few business establishments in Sweden have works councils. There is no right of codetermination. Employees' involvement and codetermination are regulated in Sweden by collective agreements. There are statutory provisions in the Swedish Joint Regulation Act (*Medbestämmandelagen*). According to these provisions attention must be paid when implementing whistleblower channels to whether there are relevant provisions in collective agreements that would prevent the implementation without the involvement of the labor unions.

15. Hungary

There is no specific whistleblowing legislation relating to employees in Hungary. Under criminal law a failure to report certain crimes to the authorities is illegal including crimes against the state and violation of state secrets. This law is applicable to all persons in Hungary and not only to employees. While Hungarian law does not specify the types of disclosures that can be made as a general rule, a disclosure that is made in compliance with the law and the employer's whistleblowing policy if any, will be protected. If the whistleblower makes false disclosures or disclosures in bad faith, he can be disciplined.

a) Notification

In general all data controllers are required to notify the data protection agency. Data processing shall not be notified to the register of processing operations amongst other exemptions when it concerns the data of the data processor's employees.

Employers should contact the data processing agency to find out if notification is required in case of the whistleblower channel.

b) Employee participation

If there is a works council, the employer must obtain its opinion with regard to the implementation of the whistleblower channel. However, this opinion will have no binding effect on the employer. If the works council fails to give its opinion within 15 days after having received the documentation, this is deemed to be consent.

Prior to making certain decisions, the employer must obtain the opinion of the works council especially with regard to measures concerning the details of the system of personnel

registration. Further the data must be registered or the content of the data sheet legally provided for or the social plan and also with regard to the implementation of new methods of work organization and performance requirements as well as the drafting of internal rules that affect material interests of the employee. If the opinion of the works council has to be obtained it has 15 days after having received the documentation to give its opinion on the planned measure. If this deadline is not met, this is deemed to be consent. However, the opinion of the works council does not bind the employer. Ignoring, it can at most have an impact on the working atmosphere. It is not permitted to implement measures without having obtained the opinion of the works council at all. If the employer should fail to obtain the opinion of the works council (if there is one) the implementation of the whistleblower channel would be impermissible.

16. Czech Republic

The Czech Republic complies formally with the EU data protection directive.

a) Notification

In principle all data controllers have to notify the office for personal data protection (*Úřad pro ochranu osobních údajů*). Exempted are controllers to whom Article 3(6) and Article 18 of Act 101/2000 coll. applies. Therefore a notification is not necessary where the controller is required by a specific act to process personal data for specific purposes on condition that the additional features of the processing are set out in said act. When necessary after a notification has been assessed a request for supplement could be issued. After the supplement has been assessed either the registration is confirmed or the processing is refused.

Employers will have to notify the office for personal data protection prior to processing data by using a notification form.

The notification requires among other things information on the data controller, information on the data processor, the purposes for the processing and security measures. Employers are also required to report manual filing systems.

b) Employee participation

There are no works councils in the Czech Republic. Therefore it is not necessary to involve the employees. However, pursuant to the Employment Law Code²¹ the labor union has a right to be involved in the event rules for work are issued. If the implementation of a whistleblower channel falls under this heading, employers must obtain the approval of the union.

²¹ § 82 (3) of the Employment Law Code.

17. Luxembourg

There is no specific whistleblowing legislation in Luxembourg. General principles of data privacy and labor law are applicable.

a) Notification

In principle all data controllers have to notify the data protection agency. One exemption is amongst others if data controller has designated a data protection officer.

If employers have not designated a data protection officer, notification to the data protection agency is required.

b) Employee participation

Employees have enforceable codetermination rights in Luxembourg with regard to the implementation or change of controls for the employees.

18. Slovakia

Slovakia complies formally with the EU data protection directive. Slovakia does not have specific whistleblowing legislation. Whistleblowers are protected under general labor law. In the absence of specific legislation companies should have in place whistleblowing policies that:

- Set out procedures for “blowing the whistle” (to encourage employees to raise concerns internally first)
- Include a detailed procedure for dealing with any concerns raised
- Provide for fair treatment of individuals, against whom concerns are raised, giving them a chance to defend themselves.

a) Notification

With a few exemptions every data controller is obligated to notify the data protection agency. We do not have detailed information about these exemptions.

Therefore we recommend employers to notify the data protection agency.

19. Switzerland

Switzerland has EU-conform data protection legislation. Thus for practical purposes, employers should apply the EU Working Party recommendations when implementing the whistleblower channel in Switzerland since there are no specific instructions for Switzerland.

a) Data privacy and notification

In general every data controller is required to notify the data protection agency about the data processing. For forwarding data to a third party consent of the employee is generally required even if the third party is part of the company Group.

Prior to data processing employers have to notify the data protection agency. It is recommendable for employers to inform employee representatives prior to implementing a whistleblower channel.

20. Bulgaria

Since joining the European Union on 1 January 2007, Bulgaria is obligated to comply with the EU data protection directive. Therefore employers should apply the principles of the data protection directive as well as the recommendations of the Working Party in Bulgaria.

a) Employee participation

Works councils do not exist in Bulgaria. However, in certain cases provided for by law, employees are entitled to participate in discussion related to the management of the enterprise through their elected representatives whether or not the employees are represented by a trade union. Since the implementation of a whistleblower channel does not affect the management of the enterprise, employees do not have a right of participation in that matter.

C. Conclusion

To avoid risking a violation of data privacy protection legislation, businesses in Europe should review their existing whistleblowing systems with regard to scope and following the recommendation of the Article 29 Group structure. Or, if necessary, limit them to avoid lawsuits relating to data privacy protection. The data should be limited to the areas specified by the Article 29 Group: billing, finance, banking and financial crime. U.S. companies wishing to introduce a whistleblowing system, in particular should schedule adequate lead time in order to create a global arrangement from the beginning that will be in line with the requirements of both employment law and data privacy protection law in the European Union states and still warrants that the obligations resulting from the Sarbanes-Oxley Act are met. Further reaching reporting obligations will probably no longer be accepted by the data protection agencies as well as the work councils which in some countries will have a right to be involved in the establishment of a hotline.

Overview on details for individual EU-countries:

Country	Deviation from Art. 29 Working Group (+) additional list of criteria	Notification Requirement (+) simplified if financial matters only (-)	Employee Participation (+) information and consultation
France	(+) company's data privacy protection officer has to consent, requirement of proportionality	(+)	(+) works agreement with the works council inevitable
Germany	(-) broader interpretation	(+)	(+/-) depending on collective agreements
UK	(-)	(+)	(+) opinion of employee representation
Spain	(-)	(-)	(+) approval of the works council
The Netherlands	(-)	(+)	(+) works council to be heard
Austria	(-)	(+)	(-)
Belgium	(-)	(+)	(-)
Denmark	(-)	(+)	(+)
Greece	(-)	(+)	(+) only if no union or no collective agreement
Ireland	(-)	(+)	(-)
Italy	(-)	(+)	(-)
Poland	(-)	(+)	(-)
Portugal	(-)	(+)	(+) information and supervisory rights only

Sweden	(-)		(+) but exemptions	(-) but collective agreements, might provide for this
Hungary	(-)		(+) exemptions (e. g data processor's employees)	(+) if works council exists, opinion must be obtained
Czech Republic	(-)		(+)	(-) but union may have to be involved if rules for work are issued
Luxembourg	(-)		(+) exemptions (e. g existence of a data protection officer)	(+)
Slovakia	(-)		(+) few exemptions	
Switzerland	(-)	EU-conform data protection legislation	(+)	(+) employee's consent is generally required prior to forwarding data
Bulgaria	(-)			(-)

BERLIN

Markgrafenstrasse 36
Carree am Gendarmenmarkt
10117 Berlin
Tel.: +49 (0) 30/203 60-0
Fax: +49 (0) 30/203 60-290
E-Mail: Berlin@cms-hs.com

FRANKFURT / MAIN

Barckhausstrasse 12-16
60325 Frankfurt/Main
Tel.: +49 (0) 69/7 17 01-0
Fax: +49 (0) 69/7 17 01-40410
E-Mail: Frankfurt@cms-hs.com

COLOGNE

Theodor-Heuss-Ring 19-21
50668 Cologne
Tel.: +49 (0) 221/77 16-0
Fax: +49 (0) 221/77 16-110
E-Mail: Cologne@cms-hs.com

MUNICH

Briener Strasse 11/V
80333 Munich
Tel.: +49 (0) 89/2 38 07-0
Fax: +49 (0) 89/2 38 07-110
E-Mail: Munich@cms-hs.com

CHEMNITZ

Hartmannstrasse 7
09111 Chemnitz
Tel.: +49 (0) 371/3 69 74-0
Fax: +49 (0) 371/3 69 74-21
E-Mail: Chemnitz@cms-hs.com

BELGRADE

Knez Mihailova 33
11000 Belgrade
Tel.: +381 (0) 11/30 30-136
Fax: +381 (0) 11/30 30-137
E-Mail: Belgrade@cms-hs.com

MOSCOW

Korobejnikov Per., 1, Geb. 1a
119034 Moscow
Tel.: +7 (095) 739 00 44
Fax: +7 (095) 739 00 55
E-Mail: Moscow@cms-hs.com

DUESSELDORF

Bankstrasse 1
40476 Duesseldorf
Tel.: +49 (0) 211/49 34-0
Fax: +49 (0) 211/49 200-97
E-Mail: Duesseldorf@cms-hs.com

HAMBURG

Stadthausbruecke 1-3
20355 Hamburg
Tel.: +49 (0) 40/3 76 30-0
Fax: +49 (0) 40/3 76 30 40-600
E-Mail: Hamburg@cms-hs.com

LEIPZIG

Augustusplatz 9
04109 Leipzig
Tel.: +49 (0) 341/2 16 72-0
Fax: +49 (0) 341/2 16 72-33
E-Mail: Leipzig@cms-hs.com

STUTTGART

Schoettlestrasse 8
70597 Stuttgart
Tel.: +49 (0) 711/97 64-0
Fax: +49 (0) 711/97 64-900
E-Mail: Stuttgart@cms-hs.com

DRESDEN

An der Dreikoenigskirche 10
01097 Dresden
Tel.: +49 (0) 351/82 64-40
Fax: +49 (0) 351/82 64-716
E-Mail: Dresden@cms-hs.com

BRUSSELS

Avenue Louise 200
1050 Brussels
Tel.: +32 (0) 2/65 00-420
Fax: +32 (0) 2/65 00-422
E-Mail: Bruessel@cms-hs.com

PRAGUE

Karoliny Svetle 25
11000 Prague 1
Tel.: +420 (0) 2/96 798-111
Fax: +420 (0) 2/21 098-000
E-Mail: Prague@cms-hs.com

www.cms-hs.com