A company or organisation should have an adequate whistleblower procedure for internally reporting suspicions of misconduct within the company or organisation. The importance of this should not be underestimated. The main objective is for management to become aware of dangerous or illegal activities that pose a risk for the company or organisation, its employees, the environment or society as a whole. A whistleblower procedure makes it possible for a company or organisation to take measures in a timely manner to stop misconduct before one of these risks is actually realised. A whistleblower procedure also unmistakeably strengthens a company’s corporate governance and can contribute to socially responsible business practice. Finally, a whistleblower procedure, in principle, results in misconduct being reported internally before being communicated externally. It helps protect a company from damage to its reputation.

The importance of a whistleblower procedure should not be underestimated.

---

**Legal framework**

In the Netherlands, the public sector has various whistleblower procedures for civil servants who discover misconduct in their own organisations. However, in the Netherlands there is no specific legislation dealing with whistleblower procedures in the private sector. Legislation does impose certain general requirements relating to such policies, including the Dutch Corporate Governance Code and the Dutch Data Protection Act.

Since the introduction of the 2002 US Sarbanes-Oxley Act (SOX), companies listed on the US stock market can, in principle, be required to create a whistleblower procedure for accounting and auditing issues. This also applies to Dutch companies listed on a US stock exchange, and to Dutch subsidiaries of companies listed on US exchanges. Furthermore, under SOX, a company is prohibited from taking measures against an employee who has cooperated in a whistleblower investigation.

**Dutch Corporate Governance Code**

In principle, the Dutch Corporate Governance Code (Code) is applicable to companies listed on the Dutch stock exchange. Article II.1.7 of the Code stipulates that these companies must have a whistleblower procedure:

> The Management Board shall ensure that employees have the possibility of reporting alleged irregularities of a general, operational and financial nature within the company to the Chairman of the Management Board or to an official designated by him, without jeopardising their legal position. Alleged irregularities concerning the functioning of Management Board...

---


2 See Coen Zoon, Mirjam Stuivenberg, Hans Nauta and Peter Donker van Heel, “Evaluatie zelfregulering klokkenluidesprocedures”, ECORYS, Arbeid en Sociaal beleid, Ministry of Social Affairs and Employment, 15 May 2006. Retrieved 26 March 2013 from http://docs.szw.nl/pdf/129/2006/129_2006_3_9270.pdf. (1) Employees working in a company with a whistleblower procedure have a greater tendency to report misconduct in a company (88%) than employees who work in a company without such a procedure (56%). (2) Of those employees who work in a company without whistleblower procedure, 11% tend to report misconduct only externally. If the company has a whistleblower procedure, the employees do not have this tendency. (3) In companies with a whistleblower procedure, there is a strong tendency to report misconduct internally. However, other factors often determine whether misconduct is actually reported, including company culture, the experiences of colleagues, and fear of the consequences of reporting misconduct.

---

---
The best practice provisions in the Code create a certain standard for the conduct of executive directors, supervisory directors and others. Listed companies are subject to the "comply or explain" principle. This means that companies may depart from Code provisions, but these departures must be explained and justified. Article 2:391(5) of the Dutch Civil Code sets out a company’s statutory obligation to state in its annual report that it complied with the provisions of the Code, and to provide an explanation for any departure from a provision.9

Privacy
In 2006, the Dutch Data Protection Authority (Authority) issued an opinion about the use of a whistleblower procedure that took the form of a whistleblower hotline within a multinational company.11 The Authority and the Article 29 Working Party largely have the same approach, but several additional requirements apply under the Act. (The Article 29 Working Party is the European Commission’s advisory body on privacy and has representatives from the 27 EU member states’ regulatory bodies.)

Basis
Under article 8 of the Act, there must be a basis for the processing of personal data in the context of a whistleblower procedure. This basis can be a requirement to comply with a legal obligation (article 8(c)) and the company having a justified interest that makes the procedure essential and that outweighs the privacy of the employees involved (article 8(f)).

The first basis does not apply if the legal obligation is a foreign one, including for example a SOX obligation. The obligation must be imposed by virtue of a generally binding regulation. The consequences for a controller if it does not comply with a foreign legal obligation (e.g. fines) must also be taken into consideration if the company wishes to rely on "justified interest".

The Authority’s position is that a company has a justified interest in having a whistleblower hotline, but this must be balanced with the fundamental rights and freedoms of the data subjects, in particular, the right to privacy.

This will usually support a whistleblower procedure if the intention is to identify substantial misconduct, i.e. presumably entailing a certain degree of seriousness with respect the facts or situations reported. The seriousness will depend on the circumstances of the case. How the misconduct is dealt with must also be proportional: the nature and seriousness of the misconduct affects how the report is made. According to the Authority, the suspicions of a whistle blowing employee must be based on reasonable grounds of possible or actual misconduct.

Suspicion of a criminal offence and special personal data
If the report contains information relating to a crime (i.e. a legitimate suspicion of a criminal offence) or special personal data (i.e. concerning a person’s religion, philosophy of life, race, political persuasion, health, sexual life or trade union membership), the company must follow a strict set of rules that applies to the processing of special personal data. In reports produced in the context of whistle blowing, this will primarily concern data relating to crime. The company may, in principle, process these data if a staff member has committed, or will imminently commit, a criminal offence.

Anonymous reporting
An organisation is not allowed to encourage the use of anonymous reporting. An organisation is not allowed to encourage the use of anonymous reporting. It must create a system in which it is a basic principle that the identity of the whistleblower is known. The

---

9 See footnote 4. This Code replaced the Dutch Corporate Governance Code (Tabaksblat Code) with effect from 1 January 2009, decree of 27 December 2004, Bulletin of Acts and Decrees 747, which includes a similar provision.
10 See also the Decree of 23 December 2004 to establish further rules for the content of the annual report. This decree was amended several times at a later stage.
11 Dutch Data Protection Authority, Opinion on permit application, by virtue of art. 77.2 of the Data Protection Act, 16 January 2006, 2004-1233.
13 Art. 16 to 23 of the Dutch Data Protection Act ("Act")
Authority’s position is that it is preferable to create a system that allows reports to be made confidentially, i.e. the whistleblower’s identity is known but only to a confidential adviser or is kept secret in another way.

Compliance with the duty to inform
The duty to inform entails informing a data subject when his or her data is being processed and also communicating clearly and transparently with staff members about the existence and functioning of the system. In this context, the scope of the system - i.e. which misconduct is to be reported - deserves special attention. Furthermore, it must be communicated that abuse of the system could lead to the imposition of disciplinary measures. This does not apply to reports submitted by an individual with the best intentions, but that ultimately turn out to be unfounded.

People named in a report must be informed that data concerning them is being processed within the whistle blowing system and this information must be given no later than at the time the data is recorded. In this way, data subjects are given the opportunity to exercise their rights, including the right to access. However, because this could potentially obstruct a criminal investigation, under article 43 of the Act, it is possible to delay informing the data subject as long as necessary for the purpose of securing the evidence. The Authority’s position is that this exception must be interpreted restrictively, and use of this exception must be properly substantiated on a case-by-case basis. The right to access may not be used to discern the identity of the whistleblower or the other parties involved.

Clear and transparent communication must take place with employees about the existence and functioning of the system.

Dealing with reports
According to the Authority, a report must be handled by an outside organisation or, if dealt with internally, by a unit specially designated for that purpose. The preference is to designate an organisation external to the original company or institution to deal with the first report. Access to the reports and the associated data must be limited. Staff members who have access to the information are subject to a duty of confidentiality. It may be necessary to transfer personal data to a third country; if so, any such transfer must satisfy the requirements imposed by the Authority. For more information, see also the chapter entitled “e-Discovery and privacy: the eternal dilemma”.

Dealing with complaints
A standard procedure is required to deal with complaints received through the whistleblower hotline. Particular attention should be paid to the rights of data subjects when dealing with complaints.¹³

Retention period
Data processing in the context of whistle blowing that turns out to be unfounded must cease immediately and the data must be deleted. Data relating to an open investigation may not be stored longer than two months after the investigation is completed, unless disciplinary measures are taken against the whistleblower (i.e. because of a false report) or the subject of the whistle blowing (i.e. because of a legitimate report).

Position of a whistle blowing employee
Under the Works Councils Act, the establishment of a whistle blower procedure requires the approval of the works council. It is often unclear to an employee what his or her position is if the employee suspects misconduct in the company. Moreover, whistleblower cases reveal that an employee who blows the whistle often does so to his or her own detriment.¹⁷ In Dutch employment law, an employer’s case against a whistleblower is usually based on article 7:611 of the Dutch Civil Code, which states that an employee is required to conduct himself or herself as a “good employee”. (The same standard applies to the employer.) Whether the actions of a whistleblower justify the measures taken by an employer (including, for example, summary dismissal) is a matter to be determined by the court.

Bill for a law protecting whistleblowers
On 14 May 2012, a bill for a whistleblower protection act having the following goal was introduced:

...to improve the conditions for reporting social misconduct, by making it possible to investigate misconduct and to better protect people who report misconduct.

¹³ Act, art. 35 et seq
¹⁶ Works Councils Act, art. 27.1(j)
The bill proposes the establishment of a "Whistleblower Office":

The legislation provides for a ‘Whistleblower Office’ that conducts investigation into social misconduct and makes recommendations to resolve problems. This Office will also provide support and guidance to the whistleblower, if desired. The legislation also provides for a Whistleblower Fund, which provides financial assistance to whistleblowers, if necessary. The Whistleblower Office will become part of the National Ombudsman, but will be open to reports from both the public and private sector. When carrying out its tasks, the Office may seek the assistance of existing organisations and experienced experts. The Office will issue an annual report on its activities. This report will set out the investigations conducted and the outcome of the recommendations.18

At present, it is not clear when the Whistleblower Office will be operational. The Council of State has already issued an opinion. The timeframe will be determined by Royal Decree.

**Design of the procedure**

Due to the statutory silence on this issue, a company may design its own whistleblower procedure. A good place to start is the 2003 “Statement on dealing with suspicions of misconduct in companies”, along with a model procedure prepared by the Dutch Labour Foundation (Stichting van de Arbeid or “STAR”).19 STAR notes that it must be clear to employees where they can make a report and what the procedure entails (i.e. what is done with a report and how the employee is informed about the progress of the case).20 It should also be clearly communicated to employees that this procedure is not intended for employee complaints about personal work issues. Complaint procedures already exist for this purpose. The whistleblower procedure is also not intended to be a means for employees to report ethical dilemmas encountered in the scope of normal business activities. In principle, the whistleblower procedure is also not a forum for employees to criticise the employer’s policy choices.

---

18 Parliamentary Documents II 2012/13, 33 258, no. 7, pages 1 and 2.
20 Statement (see footnote 19), page 2.

---

**Inform data subjects if their personal data is being processed in the context of the procedure.**

**Whistleblower Advisory Point**

The Dutch government established an independent agency called the Whistleblower Advisory Point on 1 October 2012.21 Advising and supporting both potential and actual whistleblowers, the Whistleblower Advisory Point focuses on public sector and private sector misconduct involving society as a whole. If the whistleblower considers the outcome of a company or government organisation’s internal report to be unsatisfactory, he may request the Whistleblower Advisory Point to provide a recommendation on an appropriate external organisation where the complaint may be notified (e.g. the relevant supervisory authority). However, it does not actually conduct investigations into misconduct itself. The Whistleblower Advisory Point also provides information to the public about whistleblowing and identifies developments and patterns important for whistleblower policy in the public and private sectors.22

21 Established based on the Decision of 27 September 2011 to establish the Committee for the Whistleblower Advisory and Referral Point (Temporary Decision on the Committee for the Whistleblower Advisory and Referral Point) and explanatory memorandum, Bulletin of Acts and Decrees 2011, 427.
22 See also http://www.adviespuntklokkenluiders.nl.
Tips & Tricks: Preparing a whistleblower procedure

- Prepare the procedure in consultation with the works council or body representing the employees (if any).
- Determine which cases are subject to the procedure.
- Encourage confidential reporting; curb anonymous reporting.
- The procedure should include at least the following elements (but see also STAR’s model procedure):
  - the appointment of one or more officers to whom employees can report incidents/suspicions;
  - a description of how the company deals with the internal report;
  - a description of how feedback is given to the person who submitted the report;
  - a description of the situations in which, and the way in which, the whistleblower may make an external report;
  - the protection of the rights of a whistleblower who has acted with due care.
- Inform employees about the existence and functioning of the procedure.
- Inform data subjects if their data is being processed in the context of the procedure.

The members of the Houthoff Buruma Privacy Team:

Wolter Wefers Bettink
Partner at Houthoff Buruma, Dutch lawyer specialising in IP and IT litigation, privacy and e-business
T +31(20)605 6167 | w.bettink@houthoff.com

Thomas de Weerd
Partner at Houthoff Buruma, Dutch lawyer specialising in IT law, outsourcing, privacy and e-business
T +31(20)605 6985 | t.de.weerd@houthoff.com

Copyright © 2013 Houthoff Buruma

All rights reserved. Short passages from this edition may be used in other publications, under the condition that the source is clearly cited. We prefer the use of the following form: “Privacy: Tips & Tricks for Companies, Houthoff Buruma”.

Apart from this, no part of this publication may be reproduced, stored in an automated filing system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of Houthoff Buruma. This publication is provided for informational purposes only and does not constitute legal advice. This publication has been compiled with the utmost care; nevertheless, Houthoff Buruma cannot be held liable for any errors or inaccuracies, nor any associated consequences.