Whistle blowing – opinion Dutch DPA – January 2006

In 2005, the Dutch Data Protection Authority received several requests from multinational companies for an authorisation to transfer data to companies' international ethics hotlines in the United States for so-called whistle blowing purposes. These requests entailed transfers both in the context of the obligations under article 301(4) of the US Sarbanes Oxley Act that "Each Audit Committee shall establish procedures for the confidential, anonymous submission by employees of the issues of concerns regarding questionable accounting or audting matters", and transfers with a wider purpose.

In January 2006, the Dutch Data Protection Authority informed several companies of the conditions it sets to the whistleblowing schemes. The following elements are, amongst others, considered relevant.

1. General conditions for a whistle blowing scheme

In principle, companies can have a legitimate interest in having an ethics hotline or whistle blowing scheme (article 7(f) of Directive 95/46/EC). The processing should however be necessary for the legitimate interest of the company, and the fundamental rights and interests of data subjects should not prevail. This balance of interest test should take into account issues of proportionality, subsidiarity, seriousness of the alleged offences that can be notified and the consequences for the data subjects. In the context of the balance of interest test, adequate safeguards will also have to be provided for.

In addition to that, other conditions for legitimate processing should be met. In particular, data should be processed fairly and lawfully, and should be processed for specified, explicit, and legitimate purposes. Data should be kept in a form which permits identification of data subjects for no longer than necessary, and be adequate, relevant and not excessive. Furthermore, they must be accurate, and, where necessary and kept up to date. The rules on sensitive data processing and the information duty must be obeyed, and adequate security measures must be taken.

2. Grounds for processing and transfer of data

National legal obligations could in principle be a basis for establishing a whistle blowing scheme under article 7(c) of Directive 95/46/EC. In case of foreign legal obligations, such as article 301 (4) of the Sarbanes Oxley Act, whistle blowing lines cannot be based on article 7(c) of Directive 95/46/EC. The only possible ground would then be article 7(f), under the general conditions mentioned above. Concretely, the obligations upon companies listed at the US stock exchange to install a whistle blowing line for the reporting of alleged accounting or auditing matters, are of interest to these companies. In this context, the scope is limited: Only procedures for the confidential, anonymous submission by employees of concerns regarding questionable accounting or auditing matters are covered. The consequences for the companies in case they cannot comply with these obligations will have to be taken into account when assessing the application of article 7(f). However, the mere existence of a foreign legal obligation does not in itself justify a legitimate interest under article 7(f) of Directive 95/46/EC.

The whistle blowing lines are used for other purposes as well, such as breach of company policy or national legal obligations.

Under normal circumstances, reports on improper conduct of any nature, should be handled through the regular channels, such as via the management hierarchy, a position involving confidentiality, human resources, the works council, or, in case of accounting, via the controller or external auditors. The use of a whistle blowing scheme should be redundant under normal circumstances and can therefore not take the place of regular reporting systems. Considering the subsidiary and complementary character of the whistle blowing lines, its purpose needs to be limited; the whistle blowing line should be used for reporting substantial offences. This presupposes a certain level of seriousness of the reported facts or situations.The seriousness of the case will depend on the circumstances. The reporting of an alleged abuse via a whistle blowing line must be proportionate: The character and seriousness of the offence determine the way the report should be made. The employee should also base his allegation on a reasonable suspicion that an offence has occurred or could occur.

In this context, also, transfer of data to the mother company (whether within the EU or not) will only be justified in case of substantial abuses that exceed the (national) level of the daughter company. In most cases, these will therefore concern cases of misconduct of higher management. Exceptionally, also offences of low rank employees are eligible for reporting to the mother company. The circumstances of the particular case would be decisive.

3. Anonymous reporting

The Dutch DPA favours whistle blowing schemes which enable confidential, rather than anonymous, reporting. This implies that the whistle blower makes his identity known to the person or committee handling his report, after which his identity is treated confidentially. Companies should set up a whistle blowing scheme which takes as a starting point confidential reporting whereby the identity of the whistle blower is recorded. Companies should encourage confidential reporting and curb or avoid anonymous reporting, and create the necessary trust in confidential reporting.

Non anonymous reports have several advantages: the limitation of false or slanderous reports; the protection of the whistle blower against retaliation; better handling of the report because additional details can be requested from the whistle blower.

To ensure protection of the whistle blower, his data should under no circumstances be provided to the person about whom a report is made, also in case that person places an access request under article 11 of Directive 95/46/EC.

4. Information to be given to data subjects

The information duty consists on the one hand of informing the data subject that a report on him has been filed, not later than at the moment of the recording of the information. If it is necessary for the assessment of the report, for example for the gathering of evidence, the information provision can temporarily be postponed on the basis of article 43 of the Dutch Data Protection Act (implementing article 13 Directive 95/46/EC). However, this exemption must be interpreted restrictively and needs to be argued case by case.

On the other hand, the information duty also obliges the controller to inform the employees in general in a clear and transparent manner about the existence, purposes and functioning of the whistle blowing scheme, and the controller(s) involved.

5. Treatment of the whistle blowing reports

The reports should be handled by a specialized (part of the) company. It is preferable to designate an external organisation to handle the first review and check whether the report is relevant considering the scope of the whistle blowing scheme and the other legal requirements. In this way, it is avoided that data, that should not be processed further, reaches the organisation of the client. Employees should be bound by a duty of confidentiality.

6. Storage limit

Processing of data should be stopped immediately if it is established a report was unfounded. Data related to a report should not be kept longer than two months after the finalisation of the investigation relating to the report, unless disciplinary measures are taken against the whistle blower (in case of a false report) or the person on whom a report was filed (founded report).