Alþingi, nefndasvið
b.t. efnahags- og viðskiptanefndar,
Austurstræti 8 - 10
150 Reykjavík

Persónuvernd

Rauðarárstíg 10 105 Reykjavík
sími: 510 9600 bréfasími: 510 9606
netfang: postur@personuvernd.is
veffang: personuvernd.is

Reykjavík, 16. mars 2017
Tilvísun: 2017020363GIÁ/--

Efni: Frumvarp til laga um breytingu á lögum nr. 161/2002, um fjármálafyrirtæki, með síðari breytingum, og lögum nr. 87/1998, um opinbert eftirlit með fjármálastarfsemi, með síðari breytingum (Tilkynningar um brot á fjármálamarkaði).

Persónuvernd vísar til beiðni efnahags- og viðskiptanefndar frá 24. febrúar 2017 um umsögn stofnunarinnar um drög að frumvarpi til laga um breytingu á lögum nr. 161/2002, um fjármálafyrirtæki, með síðari breytingum, og lögum nr. 87/1998, um opinbert eftirlit með fjármálastarfsemi, með síðari breytingum.

Með frumvarpinu er m.a. lagt til að við lög nr. 161/2002, bætist tvær nýjar greinar, 60. gr. a og 60. gr. b, sem annars vegar kveði á um skyldu fjármálafyrirtækis til þess að hafa ferla til þess að taka við og fylgja eftir tilkynningum frá starfsmönnum þess um brot í starfsemi fjármálafyrirtækis og hins vegar um vernd fyrir þá starfsmenn sem tilkynna um slík brot. Bæði ákvæðin byggja á skyldum sem lagðar eru á aðildarríki Evrópska efnahagssvæðisins með 71. gr. tilskipunar 2013/36/ESB. Þá er lagt til að við lög nr. 87/1998 bætist einnig ný grein sem kveði á um skyldu Fjármálaeftirlitsins til þess að setja upp ferla til að taka við og fylgja eftir tilkynningum um brot í starfsemi aðila sem lúta opinberu eftirliti með fjármálastarfsemi.

Í 2. málsl. a-liðar 1. mgr. 1. gr. og 1. málsl. 2. mgr. 3. gr. frumvarpsins er lagt til að fjármálafyrirtækjum og Fjármálaeftirlitinu verði heimilt að taka á móti nafnlausum tilkynningum. Í athugasemdum sem fylgja ákvæðunum segir m.a. að ferlar skuli tryggja að hægt sé að tilkynna um brot á nafnlausan hátt. Möguleiki á nafnleynd kunni að veita starfsmönnum ákveðið öryggi sem geti orðið þeim hvatning til að tilkynna um brot. Þrátt fyrir að ferlar heimili nafnlausar tilkynningar beri ekki að skilja slíka heimild með þeim hætti að verið sé að hvetja til nafnleyndar.

Það liggi í hlutarins eðli að erfitt geti reynst að rannsaka brot án þess að fullnægjandi upplýsingar liggi fyrir. Ef tilkynnt sé um brot undir nafni leiði tilkynning fremur til þess að unnt verði að rannsaka og upplýsa brot. Þá kemur fram að sambærilegt ákvæði sé að finna í dönskum rétti um þetta efni. Hins vegar virðist mega ráða af efni frumvarpsins að þessi leið hafi ekki verið farin í Noregi eða Svíþjóð.

Með vísan til þess sem segir í frumvarpinu vill Persónuvernd koma á framfæri eftirfarandi:

Um nafnlausar tilkynningar er fjallað í hjálögðu áliti nr. 1/2006 frá starfshópi samkvæmt 29. gr. persónuverndartilskipunarinnar 95/46/EB sem skipaður er fulltrúum persónuverndarstofnana í aðildarríkjum ESB og gegnir ráðgefandi hlutverki um túlkun og beitingu tilskipunarinnar. Vinnuhópurinn telur að ýmis tormerki séu á nafnlausum tilkynningum. Bendir hópurinn m.a. á að nafnleysi komi ekki í veg fyrir að aðrir geti getið sér til um hver hafi tilkynnt brot; erfiðara geti verið að rannsaka mál þar sem ekki sé hægt að ráðfæra sig við tilkynnandann; auðveldara sé að vernda tilkynnandann gegn hefndaraðgerðum (e. *retaliation*), sérstaklega ef slík vernd sé veitt í lögum, ef fyrir liggur hver hann er; að innan fyrirtækis kunni það að verða venjubundið að sendar séu nafnlausar tilkynningar til að koma höggi á menn; og að andrúmsloftið innan fyrirtækis kynni að verða slæmt ef starfsmenn væru sér meðvitaðir um að sendar kynnu að verða um þá nafnlausar tilkynningar (bls. 10 og 11 í álitinu).

Í ljósi þessa telur vinnuhópurinn að almennt eigi aðeins að taka við tilkynningum undir nafni. Lítur hann þar til þess grundvallarskilyrðis að vinnsla á að vera sanngjörn. Engu að síður telur hann ekki hægt að útiloka nafnlausar tilkynningar, enda geti það verið svo í ákveðnum tilvikum að tilkynnandi sé ekki í aðstöðu til að koma fram undir nafni. Ekki beri hins vegar að hvetja til nafnlausra tilkynninga. Þá eigi m.a. að fræða þá sem hyggjast senda inn tilkynningu um að komi þeir fram undir nafni verði því haldið leyndu að því undanskildu að nauðsynlegt geti verið að greina þeim sem koma að meðferð máls, s.s. innan dómskerfisins, frá því hverjir þeir séu (bls. 11 í álitinu). Segir að þetta sé nauðsynlegt til að slíkar upplýsingagáttir, sem hér um ræðir, komi að tilætluðum notum. Þá segir að nafn tilkynnenda skuli ekki gefið upp gagnvart þeim sem ásökun lýtur að nema þegar vísvitandi hefur verið send röng tilkynning og sá sem tilkynnt var um hyggst leita réttar síns gagnvart tilkynnanda af því tilefni, t.d. með því að höfða meiðyrðamál (bls. 15 í álitinu).

Samkvæmt 7. gr. laga nr. 77/2000, um persónuvernd og meðferð persónuupplýsinga, að finna ýmsar meginreglur sem *ávallt* skal taka mið af við vinnslu persónuupplýsinga. Í þeim felst m.a. að við meðferð persónuupplýsinga skal þess gætt að þær séu áreiðanlegar og uppfærðar eftir þörfum og að skráðar upplýsingar séu réttar og að hægt sé að leita til þess sem veitti upplýsingarnar til þess að afla frekari skýringa eða eftir atvikum staðfestingar á málsatvikum. Telur stofnunin því að almennt sé æskilegt að tilkynningar til viðkomandi fjármálafyrirtækis/Fjármálaeftirlitsins séu settar fram undir nafni, en að þeir starfsmenn, sem falið hefur verið að taka á móti slíkum tilkynningum gæti þá að nafnleynd þess sem sendir inn tilkynningu.

Í þessu samhengi má hafa hliðsjón af úrskurði Persónuverndar nr. 2014/1068, sem laut m.a. að heimildum stjórnvalds til að taka við nafnlausum ábendingum frá almenningi og 1. mgr. 19. gr. barnaverndarlaga nr. 80/2002 þar sem segir að hver sá sem tilkynnir til barnaverndarnefndar skuli segja á sér deili. Er þar um að ræða tilkynningar um að börn búi við óviðunandi uppeldisaðstæður, verði fyrir áreitni eða ofbeldi eða stofni heilsu sinni og þroska í alvarlega hættu. Hafi menn ástæðu til að ætla að um slíkt sé að ræða er þeim skylt að senda barnaverndarnefnd tilkynningu þar að lútandi, sbr. m.a. 16. gr. laganna. Ef tilkynnandi samkvæmt þeirri grein óskar nafnleyndar gagnvart öðrum en nefndinni skal það virt nema sérstakar ástæður mæli gegn því. Barnaverndarlög gera hins vegar ráð fyrir að nefndin viti ávallt hver tilkynnandi

er.

Af ákvæðinu má ráða þá afstöðu löggjafans að vafasamt geti verið, í ljósi sjónarmiða um gagnsæja málsmeðferð, að stjórnvöld veiti sérstaklega kost á nafnlausum ábendingum um meint lögbrot. Í því sambandi má nefna að í athugasemdum við umrætt ákvæði í því frumvarpi, sem varð að barnaverndarlögum, kemur fram að ítarlegt hagsmunamat liggur að baki ákvæðum þess. Eins og segir í athugasemdunum geta barnaverndarnefndum óumbeðið borist nafnlausar tilkynningar þrátt fyrir umrætt ákvæði. Tekið er fram að engu að síður geti þá verið fullt tilefni fyrir barnaverndarnefnd til að hefja rannsókn máls og grípa til ráðstafana ef því er að skipta. Ekki er því um að ræða bann við að mál séu tekin upp á grundvelli nafnlausra ábendinga, en ljóst er hins vegar að barnaverndarnefndir eiga almennt ekki að veita kost á þeim.

--

Í ljósi framangreindra sjónarmiða telur Persónuvernd eðlilegt að þegar opnaður er vettvangur til tilkynninga um meint lögbrot einstaklinga skuli þeir sem senda inn slíkar tilkynningar koma fram undir nafni. Er þá einkum litið til sjónarmiða um sanngirni og áreiðanleika. Verður ekki litið fram hjá hættu á því menn sendi í skjóli nafnleyndar inn ábendingar til þess að koma höggi á aðra. Slíkar ábendingar geta - jafnvel þótt þær eigi ekki við rök að styðjast - haft í för með sér alvarlegar afleiðingar fyrir þá sem bent er á, auk þess sem upplýsingaréttur kann að vera brotinn á málsaðila. Þá telur Persónuvernd að sú tillaga frumvarpsins að taka sérstaklega fram að heimilt sé að taka á móti nafnlausum tilkynningum gæti verkað sem hvatning til einstaklinga til að gera slíkt, jafnvel þó svo að í athugasemdum með frumvarpinu sé tekið fram að það sé ekki markmið ákvæðisins.

Persónuvernd leggur því til að þau ákvæði frumvarpsins, þar sem fjármálafyrirtækjum og Fjármálaeftirlitinu er sérstaklega heimilað að taka á móti nafnlausum tilkynningum, verði felld brott. Í því sambandi skal þó tekið fram að það er mat Persónuverndar að brottfall þeirra ákvæða komi ekki í veg fyrir að þessum aðilum berist í afmörkuðum tilvikum nafnlausar tilkynningar sem bregðast þurfi við.

F.h. Persónuverndar,

Alma Tryggvadóttir Þórður Sveinsson

Hjálagt: Álit nr. 1/2006 frá starfshópi samkvæmt 29. gr. persónuverndartilskipunarinnar 95/46/EB

00195/06/EN

WP 117

Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime

Adopted on 1 February 2006

TABLE OF CONTENTS

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,[1]

Having regard to Articles 29 and 30(1)(c) and (3) of that Directive,

Having regard to its Rules of Procedure, and in particular to Articles 12 and 14 thereof,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

This opinion provides guidance on how internal whistleblowing schemes can be implemented in compliance with the EU data protection rules enshrined in Directive 95/46/EC.[2]

The number of issues raised by the implementation of whistleblowing schemes in Europe in 2005, including data protection issues, has shown that the development of this practice in all EU countries can face substantial difficulties. These difficulties are largely owed to cultural differences, which themselves stem from social and/or historical reasons that can neither be denied nor ignored

The Working Party is aware that these difficulties are partly related to the breadth of the scope of issues which may be reported through internal whistleblowing schemes. It is also aware that whistleblowing schemes raise specific difficulties in some EU countries with regard to labour law aspects, and that work is ongoing on these issues which will require further attention. The Working Party also needs to take into account the fact that in some EU countries the functioning of whistleblowing schemes is provided for by law, while in the majority of EU countries no specific legislation or regulation exists on this issue.

As a result, the Working Party deems it premature to adopt a final opinion on whistleblowing in general at this stage. By adopting this opinion, it has decided to address those issues on which EU guidance is most urgently needed. Considering this, and for reasons mentioned in the document, this opinion is formally limited to the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing mattrers, fight against bribery, banking and financial crime.

---

[1] OJ L 281, 23.11.1995, p. 31, available at: http://europa.eu.int/comm/internal_market/privacy/law_en.htm

[2] In accordance with the specific mandate of the Working Party, this working document does not address other legal difficulties raised by whistleblowing schemes, in particular in relation to labour law and criminal law.

The Working Party adopted this opinion on the clear understanding that it needs to further reflect on the possible compatibility of EU data protection rules with internal whistleblowing schemes in other fields than the ones just mentioned, such as human resources, workers' health and safety, environmental damage or threats, and commission of offences. It will pursue its analysis over the coming months to determine whether EU guidance is also needed on these issues, in which case the principles developed in this document might be supplemented or adapted in a subsequent document.

II. JUSTIFICATION FOR THE LIMITED SCOPE OF THE OPINION

The Sarbanes-Oxley Act (SOX) was adopted by the US Congress in 2002 following various corporate financial scandals.

SOX requires publicly held US companies and their EU-based affiliates, as well as non-US companies, listed in one of the US stock markets to establish, within their audit committee, *"procedures for the receipt, retention and treatment of complaints received by the issuer regarding accounting, internal accounting controls or auditing matters; and the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters"*.[3] In addition, Section 806 of SOX lays down provision aimed at ensuring the protection for employees of publicly traded companies who provide evidence of fraud from retaliatory measures taken against them for making use of the reporting scheme.[4] The Securities and Exchange Commission (SEC) is the US authority in charge of monitoring the application of SOX.

These provisions are mirrored in the Nasdaq[5] and New York Stock Exchange (NYSE)[6] rules. If listed on either Nasdaq or NYSE, companies must certify their accounts to those markets yearly. This certification process implies that companies are in a position to assert that they comply with a number of rules, including whistleblowing rules.

Companies which fail to comply with these whistleblowing requirements are subject to heavy sanctions and penalties by Nasdaq, NYSE or the SEC. As a result of the uncertainty as to the compatibility of whistleblowing schemes with EU data protection rules, the companies concerned are facing risks of sanctions from EU data protection authorities if they fail to comply with EU data protection rules, on the one hand, and from US authorities if they fail to comply with US rules, on the other.

The applicability of some SOX provisions to European subsidiaries of US companies and to European companies listed in US stock markets is at present under judicial review in

---

3 Sarbanes-Oxley Act, Section 301(4).

4 Sarbanes-Oxley Act, Section 406, and, more particularly, regulations enacted by major US stock exchange institutions (NASDAQ, NYSE) also lay down that companies listed in those markets adopt "codes of ethics" applicable to senior financial officers and directors, concerning accounting, reporting and auditing matters, that should provide for enforcement mechanisms.

5 Rule 4350 (D) (3): "Audit Committee Responsibilities and Authority"

6 New York Stock Exchange (NYSE), Section 303A.06: "Audit Committee"

the United States.[7] Despite this relative uncertainty as to the applicability of all of the SOX provisions to companies established in Europe, companies which are subject to SOX on the basis of clear extraterritorial provisions in this Act also want to be in a position to comply with the specific whistleblowing provisions of SOX.

Due to the risk of sanctions facing EU companies, the WP29 has deemed it urgent to concentrate its analysis primarily on whistleblowing systems established for the reporting of potential breeches in accounting, internal accounting control and auditing matters, such as referred to in the Sarbanes-Oxley Act, and on related matters mentioned below. In so doing, the Working Party intends to contribute to the provision of legal certainty to companies which are subject both to EU data protection rules and to SOX.

III. PARTICULAR EMPHASIS PUT BY DATA PROTECTION RULES ON THE PROTECTION OF THE PERSON INCRIMINATED THROUGH A WHISTLEBLOWING SCHEME

Internal whistleblowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of companies. Whistleblowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel. It supplements the organisation's regular information and reporting channels, such as employee representatives, line management, quality control personnel or internal auditors who are employed precisely to report such misconducts. Whistleblowing should be viewed as subsidiary to, and not a replacement for, internal management.

The Working Party stresses that whistleblowing schemes must be implemented in compliance with EU data protection rules. As a matter of fact, the implementation of whistleblowing schemes will in the vast majority of cases rely on the processing of personal data (i.e. on the collection, registration, storage, disclosure and destruction of data related to an identified or identifiable person), meaning that data protection rules are applicable.

Application of these rules will have different consequences on the set-up and management of whistleblowing schemes. The whole range of these consequences is detailed below in this document (see Section IV).

The Working Party notes that while existing regulations and guidelines on whistleblowing are designed to provide specific protection to the person making use of the whistleblowing scheme ("the whistleblower"), they never make any particular mention of the protection of the accused person, particularly with regard to the processing of his/her personal data. Yet, even if accused, an individual is entitled to the rights he/she is granted under Directive 95/46/EC and the corresponding provisions of national law.

---

[7] The U.S. Court of Appeals (1st Circuit) held on 5 January 2006 that SOX provisions on the protection of whistleblowers do not apply to foreign citizens working outside the US for foreign subsidiaries of companies required to comply with the remaining provisions of SOX.

Applying EU data protection rules to whistleblowing schemes means giving specific consideration to the issue of the protection of the person who may have been incriminated in an alert. In this respect, the Working Party stresses that whistleblowing schemes entail a very serious risk of stigmatisation and victimisation of that person within the organisation to which he/she belongs. The person will be exposed to such risks even before the person is aware that he/she has been incriminated and the alleged facts have been investigated to determine whether or not they are substantiated.

The Working Party is of the view that proper application of data protection rules to whistleblowing schemes will contribute to alleviate the above-mentioned risks. It also takes the view that, far from preventing these schemes from functioning in accordance with their intended purpose, application of these rules will generally contribute to the proper functioning of whistleblowing schemes.

IV. ASSESSMENT OF THE COMPATIBILITY OF WHISTLEBLOWING SCHEMES WITH DATA PROTECTION RULES

The application of data protection rules to whistleblowing schemes implies deal with the question of the legitimacy of whistleblowing systems (1); application of the principles of data quality and proportionality (2); the provision of clear and complete information about the scheme (3); the rights of the person incriminated (4); the security of processing operations (5); the management of internal whistleblowing schemes (6); issues related to international data transfers (7); notification and prior checking requirements (8).

1. Legitimacy of whistleblowing systems (Article 7 of Directive 95/46/EC)

For a whistleblowing scheme to be lawful, the processing of personal data needs to be legitimate and satisfy one of the grounds set out in Article 7 of the data protection Directive.

As things stand, two grounds appear to be relevant in this context: either the establishment of a whistleblowing system is necessary for compliance with a legal obligation (Article 7(c)) or for the purposes of a legitimate interest pursued by the controller or by the third party to whom the data are disclosed (Article 7(f)).[8]

i) Establishment of a whistleblowing system necessary for compliance with a legal obligation to which the controller is subject (Article 7(c))

The establishment of a reporting system should have the purpose of meeting a legal obligation imposed by Community or Member State law, and more specifically a legal obligation designed to establish internal control procedures in well-defined areas.

At the present time, such an obligation exists in most EU Member States in the banking sector, for instance, where governments have decided to strengthen internal control, in particular with regard to the activities of credit and investment companies.

---

[8] Companies should be aware that in some Member States the processing of data on suspected criminal offences is subject to further specific conditions relating to the legitimacy of their processing (see *infra*, section IV, 8).

Such a legal obligation to put in place reinforced control mechanisms also exists in the context of combating bribery, in particular as a result of the implementation in national law of the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (OECD Convention of 17 December 1997).

By contrast, an obligation imposed by a foreign legal statute or regulation which would require the establishment of reporting systems may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate. Any other interpretation would make it easy for foreign rules to circumvent the EU rules laid down in Directive 95/46/EC. As a result, SOX whistleblowing provisions may not be considered as a legitimate basis for processing on the basis of Article 7(c).

However, in certain EU countries whistleblowing schemes may have to be put in place by way of legally binding obligations of national law in the same fields as those covered by SOX.[9] In other EU countries where such legally binding obligations do not exist, the same result may, however, be achieved on the basis of Article 7(f).

ii) Establishment of a whistleblowing system necessary for the purposes of a legitimate interest pursued by the controller (Article 7(f))

The establishment of reporting systems may be found necessary for the purposes of a legitimate interest pursued by the controller or by the third party to whom the data are disclosed (Article 7(f)). Such a reason would only be acceptable on condition that such legitimate interests are not "overridden by the interests for fundamental rights and freedoms of the data subject".

Major international organisations, including the EU[10] and the OECD,[11] have recognised the importance of relying on good corporate governance principles to ensure the adequate functioning of organisations. The principles or guidelines developed in these forums consist in enhancing transparency, developing sound financial and accounting practices, and thus improving the protection of stakeholders and the financial stability of markets. They specifically recognise an organisation's interest in putting in place appropriate procedures enabling employees to report irregularities and questionable accounting or auditing practices to the board or the audit committee. These reporting procedures must ensure that arrangements are in place for the proportionate and independent investigation of facts reported, which includes an adequate procedure of selection of the persons involved in the management of the scheme, and for appropriate follow-up action.

---

9 Dutch Corporate Governance Code, 9.12.2003, Section II, 1.6
Spanish Draft of Unified Code on corporate governance of listed companies, Chapter IV, 67(1)d). This Code has still to be examined by the Spanish Data Protection Authority in order to consider data protection implications.

10 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, 25.2.2005, p. 51).

11 OECD: OECD Principles of Corporate Governance. 2004. Part One, Section IV.

Moreover, these guidelines and regulations stress that the protection of whistleblowers should be ensured and there should be appropriate guarantees protecting whistleblowers against retaliatory measures (discriminatory or disciplinary actions).[12]

Indeed, the goal of ensuring financial security in international financial markets and in particular the prevention of fraud and misconduct in respect of accounting, internal accounting controls, auditing mattets and reporting 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. Ensuring that reports on suspected accounting manipulations or defective account auditing, which may have an impact on the financial statements of the company and concern the legitimate interests of stakeholders in the financial stability of the company, actually reach the Board of directors with a view to appropriate follow-up is a critical concern for a public company, especially those listed in financial markets.

In this context, the US Sarbanes-Oxley Act may be considered as one of these initiatives adopted to ensure the stability of financial markets and the protection of legitimate interests of stakeholders by laying down rules that guarantee appropriate corporate governance of companies.

For all these reasons, the Working Party considers that in those EU countries where there is no specific legal requirement imposing the implementation of whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, and combating against bribery, banking and financial crime, data controllers still hold a legitimate interest in implementing such internal schemes in those fields.

However, Article 7(f) requires a balance to be struck between the legitimate interest pursued by the processing of personal data and the fundamental rights of data subjects. This balance of interest test should take into account issues of proportionality, subsidiarity, the 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 put in place. In particular, Article 14 of Directive 95/46/EC provides that, when data processing is based on Article 7(f), individuals have the right to object at any time on compelling legitimate grounds to the processing of the data relating to them. These points are developed below.

2. Application of the principles of data quality and proportionality (Article 6 of the Data Protection Directive)

In accordance with Directive 95/46/EC, personal data must be processed fairly and lawfully;[13] they must be collected for specified, explicit and legitimate purposes[14] and not be used for incompatible purposes. Moreover, the processed data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.[15] Combined, these latter rules are sometimes referred to as the

---

[12] See, for instance, UK Public Interest Disclosure Act 1998.

[13] Article 6(1)(a) Directive 95/46/CE

[14] Article 6(1)(b) Directive 95/46/CE

[15] Article 6(1)(c) Directive 95/46/CE

"proportionality principle". Finally, appropriate measures have to be taken to ensure that data which are inaccurate or incomplete are erased or rectified.[16] The application of these essential data protection rules has a number of consequences as to the way in which reports may be made by an organisation's employees and processed by that organisation. These consequences are studied below.

i) Possible limit on the number of persons entitled to report alleged improprieties or misconduct through whistleblowing schemes

In application of the proportionality principle, the Working Party recommends that the company responsible for the whistleblowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistleblowing scheme, in particular in the light of the seriousness of the alleged offences to be reported. The Working Party acknowledges, however, that the categories of personnel listed may sometimes include all employees in some of the fields covered by this opinion.

The Working Party is aware that the circumstances of each case will be decisive. Thus, it does not want to be prescriptive on this point and leaves it to data controllers, with possible verification by the competent authorities, to determine whether such restrictions are appropriate in the specific circumstances in which they operate.

ii) Possible limit on the number of persons who may be incriminated through a whistleblowing scheme

In application of the proportionality principle, the Working Party recommends that the company putting in place a whistleblowing scheme should carefully assess whether it might be appropriate to limit the number of persons who may be reported through the scheme, in particular in the light of the seriousness of the alleged offences reported. The Working Party acknowledges, however, that the categories of personnel listed may sometimes include all employees in some of the fields covered by this opinion.

The Working Party is aware that the circumstances of each case will be decisive. Thus, it does not want to be prescriptive on this point and leaves it to data controllers, with possible verification by the competent authorities, to determine whether such restrictions are appropriate in the specific circumstances in which they operate.

iii) Promotion of identified and confidential reports as against anonymous reports

The question of whether whistleblowing schemes should make it possible to make a report anonymously rather than openly (i.e. in an identified manner, and in any case under conditions of confidentiality) deserves specific attention.

Anonymity might not be a good solution, for the whistleblower or for the organisation, for a number of reasons:

- being anonymous does not stop others from successfully guessing who raised the concern;
- it is harder to investigate the concern if people cannot ask follow-up questions;

---

[16] Article 6(1)(d) Directive 95/46/CE

- it is easier to organise the protection of the whistleblower against retaliation, especially if such protection is granted by law,[17] if the concerns are raised openly;
- anonymous reports can lead people to focus on the whistleblower, maybe suspecting that he or she is raising the concern maliciously;
- an organisation runs the risk of developing a culture of receiving anonymous malevolent reports;
- the social climate within the organisation could deteriorate if employees are aware that anonymous reports concerning them may be filed through the scheme at any time.

As far as data protection rules are concerned, anonymous reports raise a specific problem with regard to the essential requirement that personal data should only be collected fairly. As a rule, the Working Party considers that only identified reports should be communicated through whistleblowing schemes in order to satisfy this requirement.

However, the Working Party is aware that some whistleblowers may not always be in a position or have the psychological disposition to file identified reports. It is also aware of the fact that anonymous complaints are a reality within companies, even and especially in the absence of organised confidential whistleblowing systems, and that this reality cannot be ignored. The Working Party therefore considers that whistleblowing schemes may lead to anonymous reports being filed through the scheme and acted upon, but as an exception to the rule and under the following conditions.

The Working Party considers that whistleblowing schemes should be built in such a way that they do not encourage anonymous reporting as the usual way to make a complaint. In particular, companies should not advertise the fact that anonymous reports may be made through the scheme. On the contrary, since whistleblowing schemes should ensure that the identity of the whistleblower is processed under conditions of confidentiality, an individual who intends to report to a whistleblowing system should be aware that he/she will not suffer due to his/her action. For that reason a scheme should inform the whistleblower, at the time of establishing the first contact with the scheme, that his/her identity will be kept confidential at all the stages of the process and in particular will not be disclosed to third parties, either to the incriminated person or to the employee's line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. It is also necessary to make whistleblowers aware that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of the enquiry conducted by the whistleblowing scheme.

The processing of anonymous reports must be subject to special caution. Such caution would, for instance, require examination by the first recipient of the report with regard to its admission and the appropriateness of its circulation within the framework of the scheme. It might also be worth considering whether anonymous reports should be investigated and processed with greater speed than confidential complaints because of the risk of misuse. Such special caution does not mean, however, that anonymous reports should not be investigated without due consideration for all the facts of the case, as if the report were made openly.

---

[17] E.g. under the UK Public Interest Disclosure Act

iv) Proportionality and accuracy of data collected and processed

In accordance with Article 6(1)(b) & (c) of the Data Protection Directive, personal data has to be collected for specified, explicit and legitimate purposes and must be adequate, relevant and not excessive in relation to the purposes for which they are collected or further processed.

Given that the purpose of the reporting system is to ensure proper corporate governance, the data collected and processed through a reporting scheme should be limited to facts related to this purpose. Companies setting up these systems should clearly define the type of information to be disclosed through the system, by limiting the type of information to accounting, internal accounting controls or auditing or banking and financial crime and anti-bribery. It is recognised that in some countries the law may expressly provide for whistleblowing schemes also to be applied to other categories of serious wrongdoing that may need to be disclosed in the public interest[18] but these are outside the scope of this opinion; they may not apply in other countries. The personal data processed within the scheme should be limited to the data strictly and objectively necessary to verify the allegations made. In addition, complaint reports should be kept separate from other personal data.

When facts reported to a whistleblowing scheme do not relate to the areas of the scheme in question, they could be forwarded to proper officials of the company/organisation when the vital interests of the data subject or moral integrity of employees are at stake, or when, under national law there is a legal obligation to communicate the information to public bodies or authorities competent for the prosecution of crimes.

v) Compliance with strict data retention periods

Directive 95/46/EC lays down that personal data processed shall be kept for the period of time necessary for the purpose for which the data have been collected or for which they are further processed. This is essential to ensure compliance with the principle of proportionality of the processing of personal data.

Personal data processed by a whistleblowing scheme should be deleted, promptly, and usually within two months of completion of the investigation of the facts alleged in the report.

Such periods would be different when legal proceedings or disciplinary measures are initiated against the incriminated person or the whistleblower in cases of false or slanderous declaration. In such cases, personal data should be kept until the conclusion of these proceedings and the period allowed for any appeal. Such retention periods will be determined by the law of each Member State.

Personal data relating to alerts found to be unsubstantiated by the entity in charge of processing the alert should be deleted without delay.

---

[18] For instance, UK Public Interest Disclosure Act 1998.

Furthermore, any national rules relating to archiving of data in the company remain applicable. These rules may in particular access to the data kept in such archives, and specify the purposes for which such access is possible, the categories of persons who may have access to those files, and all other relevant security regulations.

3. Provision of clear and complete information about the scheme (Article 10 of the Data Protection Directive)

The requirement of clear and complete information on the system obliges the controller to inform data subjects about the existence, purpose and functioning of the scheme, the recipients of the reports and the right of access, rectification and erasure for reported persons.

Data controllers should also provide information on the fact that the identity of the whistleblower shall be kept confidential throughout the whole process and that abuse of the system may result in action against the perpetrator of the abuse. On the other hand, users of the system may also be informed that they will not face any sanctions if they use the system in good faith.

4. Rights of the incriminated person

The legal framework set by Directive 95/46/EC specifically emphasises the protection of the data subject's personal data. Accordingly, from a data protection point of view, whistleblowing schemes should focus on the data subject's rights, without damage to the whistleblower's ones. A balance of interests should be established between the rights of the parties concerned, including the company's legitimate investigation needs.

i) Information rights

Article 11 of Directive 95/46/EC requires individuals to be informed when personal data are collected from a third party and not from them directly.

The person accused in a whistleblower's report shall be informed by the person in charge of the scheme as soon as practicably possible after the data concerning them are recorded. Under Article 14, they also have the right to object to the processing of their data if the legitimacy of the processing is based on Article 7(f). This right of objection, however, may be exercised only on compelling legitimate grounds relating to the person's particular situation.

In particular, the reported employee must be informed about: [1] the entity responsible for the whistleblowing scheme, [2] the facts he is accused of, [3] the departments or services which might receive the report within his own company or in other entities or companies of the group of which the company is part, and [4] how to exercise his rights of access and rectification.

However, where there is substantial risk that such notification would jeopardise the ability of the company to effectively investigate the allegation or gather the necessary evidence, notification to the incriminated individual may be delayed as long as such risk exists. This exception to the rule provided by Article 11 is intended to preserve evidence by preventing its destruction or alteration by the incriminated person. It must be applied restrictively, on a case-by-case basis, and it should take account of the wider interests at stake.

The whistleblowing scheme should take the necessary steps to ensure that the information disclosed will not be destroyed.

ii) Rights of access, rectification and erasure

Article 12 of Directive 95/46/EC gives the data subject the possibility to have access to data registered on him/her in order to check its accuracy and rectify it if it is inaccurate, incomplete or outdated (right of access and rectification). As a consequence, the setting-up of a reporting system needs to ensure compliance with individuals' right to access and rectify incorrect, incomplete or outdated data.

However, the exercise of these rights may be restricted in order to ensure the protection of the rights and freedoms of others involved in the scheme. This restriction should be applied on a case-by-case basis.

Under no circumstances can the person accused in a whistleblower's report obtain information about the identity of the whistleblower from the scheme on the basis of the accused person's right of access, except where the whistleblower maliciously makes a false statement. Otherwise, the whistleblower's confidentiality should always be guaranteed.

In addition, data subjects have the right to rectify or erase their data where the processing of such data does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data (Article 12(b)).

5. Security of processing operations (Article 17 of Directive 95/46/EC)

i) Material security measures

In accordance with Article 17 of Directive 95/46/EC, the company or organisation responsible for a whistleblowing scheme shall take all reasonable technical and organisational precautions to preserve the security of the data when it is gathered, circulated or conserved. Its aim is to protect data from accidental or unlawful destruction or accidental loss and unauthorised disclosure or access.

The reports may be collected by any data processing means, whether electronic or not. Such means should be dedicated to the whistleblowing system in order to prevent any diversion from its original purpose and for added data confidentiality.

These security measures must be proportionate to the purposes of investigating the issues raised, in accordance with the security regulations established in the different Member States.

Where the whistleblowing scheme is run by an external service provider, the data controller needs to have in place a contract for adequacy and, in particular, take all the appropriate measures to guarantee the security of the information processed throughout the whole process.

ii) Confidentiality of reports made through whistleblowing schemes

Confidentiality of reports is an essential requirement to meet the obligation provided for by Directive 95/46/EC to comply with the security of processing operations.

In order to meet the objective for which a whistleblowing scheme has been established and encourage persons to make use of the scheme and report facts which may show misconduct or illegal activities by the company, it is essential that the person who reports be adequately protected, by guaranteeing the confidentiality of the report and preventing third parties from knowing his/her identity.

Companies establishing whistleblowing schemes should adopt the appropriate measures to guarantee that the whistleblowers' identity remains confidential and is not disclosed to the incriminated person during any investigation. However, if a report is found to be unsubstantiated and the whistleblower to have maliciously made a false declaration, the accused person may want to pursue a case for libel or defamation, in which case the whistleblower's identity may have to be disclosed to the incriminated person if national law allows. National laws and principles on whistleblowing in the field of corporate governance also provide for the whistleblower to be protected from retaliatory measures for making use of the scheme, such as disciplinary or discriminatory action being taken by the company or the organisation.

The confidentiality of personal data must be guaranteed when it is collected, disclosed or stored.

6. Management of whistleblowing schemes

Whistleblowing schemes require careful consideration of how the reports are to be collected and handled. While favouring internal handling of the system, the Working Party acknowledges that companies may decide to use external service providers to which they outsource part of the scheme, mainly for the collection of the reports. These external providers must be bound by a strict obligation of confidentiality and commit themselves to complying with data protection principles. Whatever the system established by a company, the company must comply in particular with Articles 16 and 17 of the Directive.

i) Specific internal organisation for the management of whistleblowing schemes

A specific organisational must be set up within the company or the group dedicated to handling whistleblowers' reports and leading the investigation.

This organisation must be composed of specially trained and dedicated people, limited in number and contractually bound by specific confidentiality obligations.

This whistleblowing system should be strictly separated from other departments of the company, such as the human resources department.

It shall ensure that, insofar as is necessary, the information collected and processed shall be exclusively transmitted to those persons who are specifically responsible, within the company or the group to which the company belongs, for the investigation or for taking the required measures to follow up the facts reported. Persons receiving this information shall ensure that the information received is handled confidentially and subject to security measures.

ii) Possibility of using external service providers

Where companies or groups of companies turn to external service providers to outsource part of the management of the whistleblowing scheme, they still remain responsible for the resulting processing operations, as those providers merely act as processors within the meaning of Directive 95/46/EC.

External providers may be companies running call centres or specialised companies or law firms specialising in collecting reports and sometimes even conducting part of the necessary investigations.

These external providers will also have to comply with the principles of Directive 95/46/EC. They shall ensure, by means of a contract with the company on behalf of which the scheme is run, that they collect and process the information in accordance with the principles of Directive 95/46/EC; and that they process the information only for the specific purposes for which it was collected. In particular, they shall abide by strict confidentiality obligations and communicate the information processed only to specified persons in the company or the organisation responsible for the investigation or for taking the required measures to follow up the facts reported. They will also comply with the retention periods by which the data controller is bound. The company which uses these mechanisms, in its capacity as data controller, shall be required to periodically verify compliance by external providers with the principles of the Directive

iii) Principle of investigation in the EU for EU companies and exceptions

The nature and structure of multinational groups means the facts and outcome of any reports may need to be shared throughout the wider group, including outside the EU.

Taking the proportionality principle into account, the nature and seriousness of the alleged offence should in principle determine at what level, and thus in what country, assessment of the report should take place. As a rule, the Working Party believes that groups should deal with reports locally, i.e. in one EU country, rather than automatically share all the information with other companies in the group.

The Working Party acknowledges some exceptions to this rule, however.

The data received through the whistleblowing system may be communicated within the group if such communication is necessary for the investigation, depending on the nature or the seriousness of the reported misconduct, or results from how the group is set up. Such communication will be considered as necessary to the requirements of the investigation, for example if the report incriminates a partner of another legal entity within the group, a high level member or a management official of the company concerned. In this case, data must only be communicated under confidential and secure conditions to the competent organisation of the recipient legal entity, which provides equivalent guarantees as regards the management of whistleblowing reports as the organisation in charge of handling such reports in the EU company.

7. Transfers to third countries

Articles 25 and 26 of Directive 95/46/EC apply where personal data are transferred to a third country. Application of the provisions of Articles 25 and 26 will be relevant, namely, when the company has outsourced part of the management of the whistleblowing scheme to a third party provider established outside of the EU or when the data collected in reports are circulated inside the group, thus reaching some companies outside of the EU.

These transfers are particularly likely to occur for EU affiliates of third country companies.

Where the third country to which the data will be sent does not ensure an adequate level of protection, as required pursuant to Article 25 of Directive 95/46/EC, data may be transferred on the following grounds:

[1] where the recipient of personal data is an entity established in the US that has subscribed to the Safe Harbor Scheme;

[2] where the recipient has entered into a transfer contract with the EU company transferring the data by which the latter adduces adequate safeguards, for example based on the standard contract clauses issued by the European Commission in its Decisions of 15 June 2001 or 27 December 2004;

[3] where the recipient has a set of binding corporate rules in place which have been duly approved by the competent data protection authorities.

8. Compliance with notification requirements

In application of Articles 18 to 20 of the Data Protection Directive, companies which set up whistleblowing schemes have to comply with the requirements of notification to, or prior checking by, the national data protection authorities.

In Member States providing for such a procedure, the processing operations might be subject to prior checking by the national data protection authority in as much as those operations are likely to present a specific risk to the rights and freedoms of the data subjects. This could be the case where national law allows the processing of data relating to suspected criminal offences by private legal entities under specific conditions, including prior checking by the competent national supervisory authority. This could also be the case where the national authority considers that the processing operations may exclude reported individuals from a right, benefit or contract. The evaluation of whether such processing operations fall under prior checking requirements depends on the national legislation and the practice of the national data protection authority.

V – CONCLUSIONS

The Working Party acknowledges that whistleblowing schemes may be a useful mechanism to help a company or an organisation to monitor its compliance with rules and provisions relating to its corporate governance, in particular accounting, internal accounting controls, auditing matters, and provisions relating to the fight against bribery, banking and financial crime and criminal law. They may help a company to duly implement corporate governance principles and to detect facts that would impact on the position of the company.

The Working Party emphasises that the establishment of whistleblowing schemes in the areas of accounting, internal accounting controls, auditing matters, and fight against bribery, banking and financial crime, to which the present opinion relates, must be made in compliance with the principles of protection of personal data, as enshrined in Directive 95/46/EC. It considers that compliance with these principles helps companies and whistleblowing schemes to ensure the proper functioning of such schemes. Indeed, it is essential that in the implementation of a whistleblowing scheme the fundamental right to the protection of personal data, in respect of both the whistleblower and the accused person, be ensured throughout the whole process of whistleblowing.

The WP stresses the principles of data protection, as laid down in Directive 95/46/EC, must be applied in full to whistleblowing schemes, in particular with regard to the rights of the accused person to information, access, rectification and erasure of data. However, given the different interests at stake, the WP recognises that application of these rights may be the object of restriction in very specific cases, in order to strike a balance between the right to privacy and the interests pursued by the scheme. However, any such restrictions should be applied in a restrictive manner to the extent that they are necessary to meet the objectives of the scheme.

Done at Brussels, 1 February 2006

For the Working Party

The Chairman
Peter Schaar