Opinion on a notification for Prior Checking received from the Data Protection Officer of the Trans-European Transport Network Executive Agency (TEN-T EA) on a Whistleblowing Procedures

Brussels, 28 October 2013 (Case 2013-0916)

1. PROCEEDINGS

On **31 July 2013**, the European Data Protection Supervisor (hereinafter "EDPS") received from the Data Protection Officer of the **Trans-European Transport Network Executive Agency (TEN-T EA)** a notification for prior checking regarding the **draft-whistleblowing procedures** to be established at the Agency.

Together with the notification, the DPO also filed:

- the Specific Privacy Statement for Whistleblowing procedures;
- the draft-Decision of the TEN-T EA Steering Committee Adopting the Guidelines on the Whistleblowing Procedure (the "**Guidelines**");
- the Communication from Vice-President Šefčovič to the Commission on Guidelines on Whistleblowing (the "**Commission's Guidelines**");
- an explanatory document entitled TEN-T EA Internal procedures to handle whistleblowing reports, including information on retention periods.

The EDPS requested supplementary information on 16 August 2013, which were received on 13 September 2013. On 22 October 2013 the EDPS sent the draft Opinion to TEN-T EA for comments which were received on 25 October 2013.

Pursuant to Article 27.4 of Regulation (EC) No 45/2001, the two-month period within which the EDPS must deliver an Opinion was suspended during the above interval.

2. FACTS

2.1. Purpose of the processing

Pursuant to Article 22a of the Staff Regulations "*any official who in the course of or in connection with the performance of his duties, becomes aware of facts giving rise to a presumption of possible illegal activity, including fraud or corruption, detrimental to the interests of the [EU], or of conduct relating to the discharge of professional duties which may constitute serious failure to comply with the obligations of officials of the [EU], shall without delay inform either his immediate superior or his Director-General or, if he considers it useful, the Secretary general, or the persons in equivalent positions, or the European Anti-Fraud Office*".

The notification illustrates the procedures to be established at TEN-T EA for the application of the provisions of the Staff Regulations concerning whistleblowing. It is necessary for the Agency and its staff that reports by staff concerning allegations of fraud, corruption and other serious wrongdoing are treated within a specific legal framework. The **purpose** of the processing is thus to provide safe channels to staff to report fraud, corruption or other serious wrongdoing at TEN-T EA, manage and follow-up reports and ensure protection of whistle-blowers in line with the Guidelines.

The draft-Decision is largely a transposition to TEN-T EA of the Commission's Guidelines. It recognises that the most effective way to encourage staff to report concerns is to provide assurance of protection of their position. Therefore, clearly defined channels for internal reporting, as well as safe and accepted routes through which staff may raise concerns outside the organisation as an option of last resort, should be in place. The Guidelines recognise that it is the Agency's duty to ensure that members of staff who report serious wrongdoings or concerns in good faith are treated with the utmost confidentiality and greatest degree of protection against any retaliation as a result of their whistleblowing.

2.2. Description of the processing

The Agency's whistleblowing rules and guidelines apply to all members of staff of the Agency, irrespective of their administrative position. A "Whistle-blower" is a member of staff, acting in good faith, who reports facts discovered in the course of or in connection with his or her duties which point to the existence of serious irregularities. The reporting should be done in writing and without delay.

The Guidelines establish the following main principles:

- Members of staff of the Agency have a duty to report serious irregularities.
- Members of staff have a choice between a number of reporting channels for whistleblowing. The principal channel is the normal chain of hierarchical command. However if staff considers it safer to bypass the normal chain of hierarchical command, they must be able to do so. Under certain conditions, staff may address their concerns to another EU institution as an option of last resort.
- Members of staff who report serious irregularities in good faith must not under any circumstances be subject to retaliation for whistleblowing. They must be protected and their identity must remain confidential if they so desire.
- The reported facts must be verified in the appropriate manner and, if they are confirmed, the Agency will take all necessary steps to ensure the appropriate follow-up.
- The rights of defence of any person implicated by the reported incidents must be respected.
- Malicious or frivolous denunciations will not be tolerated.

The reporting staff member is considered to be in good faith if he or she reasonably and honestly believes the transmitted information to be true. Good faith is presumed unless and until it is proven otherwise. Staff members who make a report in bad faith, particularly if it is based knowingly on false or misleading information, shall not be protected and shall normally be subject to disciplinary measures. The burden of proof in this context is on the Agency.

Under the whistleblowing rules, staff members are obliged to report serious irregularities (i.e. illegal activities, including fraud and corruption, and serious professional wrongdoings). As the whistleblowing arrangements are essentially a detection mechanism to bring cases to the

attention of OLAF, the duty to report concerns only serious professional wrongdoings, and particularly those that may be detrimental to the financial interests of the European Union. The Guidelines identify a number of areas, which normally fall outside the scope of the whistleblowing rules (e.g. information already in the public domain, unsubstantiated rumours or hearsay, matters of trivial nature, personnel issues where the staff has a personal interest in the outcome, harassment claims, etc.).

- Internal whistleblowing

Staff members who, in the course of or in connection with their duties, discover that serious irregularities may have occurred or may be occurring, are obliged to report this discovery forthwith and in writing to either their immediate superior, to the Ethic correspondent through the anonymous postal box (a locked letter box put at staff members' disposal in the Agency's cafeteria, which is accessible only to the Ethics Correspondent), or the Director of the Agency.

If there is a concern that this disclosure may lead to retaliation or that the intended recipient of the report is personally implicated in the serious irregularities, then the staff member may also bypass this direct means of internal reporting and address his or her report to the Chair of the Steering Committee of the Agency or directly to OLAF. OLAF may also be notified through the Fraud Notification System.

In any case, the recipient of the information is in turn obliged to transmit the information thus received without delay to OLAF. Therefore, while the staff member concerned has a choice of reporting channels, the information should ultimately reach OLAF in a short period of time.

- External whistleblowing

Upon receipt of the information reported internally, OLAF or the Agency must give the whistle-blower an indication of the period of time that it considers reasonable and necessary to take appropriate action, within 60 days of receipt of the information.

If no action is taken within that period of time, or if the whistle-blower can demonstrate that the period of time set is unreasonable in light of all the circumstances of the case, he or she may make use of the possibility of external whistleblowing as provided for in Article 22b of the Staff Regulations. Under this Article, if neither the Agency nor OLAF has taken appropriate action within a reasonable period, the staff member who reported the wrongdoing has thus the right to bring his or her concerns to the attention of the President of the Commission, or the Council, or the Parliament or the Court of Auditors, or to the Ombudsman. In this case, the whistle-blower protection continues to apply.[1]

- Internal procedure

The letter box is checked once a week by the Ethics Correspondent. On the basis of the reports, a confidential file is opened. Hard copies are stored in a safe and electronic copies are protected with a password with access by the Ethics Correspondent only. Reports are transmitted to the Ethics Correspondent (if not received through the letterbox) and then to the Director in a sealed and confidential envelope. After transmission the person receiving the

[1] However, the duties of discretion and of loyalty imply that this is an option of last resort, justifiable only if the official concerned honestly and reasonably believes that the information disclosed, and any allegation contained in it, are substantially true and if s/he has allowed the Agency or OLAF a reasonable period of time to take the appropriate action.

report (immediate superior) is reminded to destroy all copies and related documents. A meeting is held between the Director and the Ethics Correspondent to analyse the situation. The Head of the Legal Team and, if necessary, IDOC may be consulted. It may then be decided to forward the report to OLAF, IDOC or to close it. In case OLAF is consulted this is coordinated by the OLAF correspondent (Head of Legal the Team). Files on reports considered to be a "no case" are destroyed after two years.

- Protection measures

Any staff member who reports a serious irregularity, provided that this is done in good faith and, in compliance with the provisions of these Guidelines, shall be protected against any acts of retaliation. To minimise the risk of retaliation, the Guidelines provide for the following preventive measures. The identity of the whistle-blower will be kept confidential and will not be revealed to the potential wrongdoers, unless the whistle-blower authorises such disclosure or this is required by any subsequent criminal law proceedings. If the member of staff concerned wished to be moved to another office, the Agency will take any reasonable steps to facilitate such a move. Finally, particular care is taken during staff appraisal and promotion or reclassification procedures to ensure that the whistleblower suffers no adverse consequences in this context. The whistleblower will have the possibility to demand that the role of appeal assessor be taken on by the Chair of the Steering Committee. Anonymous reporting is not encouraged.

No members of staff or managers of the Agency may use their position to prevent other members of staff from complying with their obligation to report serious irregularities. Any form of retaliation undertaken by a staff member against any person for reporting a serious irregularity in good faith is prohibited. In such cases, disciplinary measures will normally be taken. Where members of staff consider that they have been the victim of retaliation as a result of the disclosure of a serious irregularity, they shall be entitled to ask for assistance from the Agency under Article 24 of the Staff Regulations and to request that protective measures be adopted. Such requests should be addressed to the Director of the Agency or, in duly justified cases, to the Chair of the Steering Committee of the Agency.

According to the Guidelines, the protection may be lost if the staff member makes unwarranted or damaging allegations that s/he cannot show to be honest or reasonable. The effect of this is that wherever a staff member is contemplating a disclosure in the sense of these guidelines, it is advisable to let the facts speak for themselves. Similarly, if the staff member makes the disclosure for purposes of private gain –for instance by selling the information to external parties– he or she will forfeit this protection as that would not be a legitimate disclosure in the sense of the whistleblowing rules. Finally, if the staff member is him or herself implicated in the serious irregularities and decides to come forward and report these irregularities, this fact may constitute a significant attenuating circumstance in any ensuing disciplinary proceedings, but it is not a qualifying disclosure in the sense of this policy and does not provide him or her with full protection against disciplinary consequences on the basis of the whistleblowing rules.

2.3. Data subjects

The notification mentions the following data-subjects:

- all Agency's staff (CA, TA, interim staff, trainees),
- staff of other EU institutions,

- external stakeholders (contractors of the Agency, Beneficiaries of grants managed by the Agency).

2.4. Categories of data

The personal data processed are contained in the report submitted by the whistle-blower. It may contain names, contact details other personal data and may be related to suspected offences, offences or criminal convictions and evaluation of personal aspects of the data subject (e.g. conduct).

2.5. Information rights

Information to data subjects is provided in the Specific Privacy Statement for Whistleblowing procedures annexed to the notification. Further information is disseminated through the Internal guidelines on whistleblowing and the Ethic guidelines published on the intranet. Information is provided also on Myintracomm.

2.6. Categories of recipients to whom data might be disclosed

The notification states that access may be granted strictly on a need to know basis, subject to necessity. The categories of recipients mentioned in the notification are the following: Head of Unit concerned, Director (AIPN), Head of Human Resources, Ethics Correspondent, Head of the Legal Team, Legal Adviser, Investigation and Disciplinary Office of the Commission (IDOC), Disciplinary Board members, Internal Auditor, IAS, European Court of Auditors, Legal Service, Civil Service Tribunal (other EU Courts), EDPS and OLAF.

2.7. Conservation of data

The notification provides the following regime for the retention of personal data in the framework of the whistleblowing procedure.

Reports on the basis of which no follow-up took place (no case) are kept for 2 years following the receipt.

Reports on the basis of which an administrative enquiry or disciplinary procedure was opened are kept in line with the respective retention period for those files:

- Files in cases where a decision has been taken to open disciplinary proceedings will be kept for 20 years from the date on which the Director of the Agency decides to close the disciplinary proceedings.
- Records of enquiries closed without disciplinary action being taken will be kept for 5 years from the date on which the Director of the Agency decides not to take action.
- Other cases falling into the 5 year category will include those closed without further action being taken at the end of the investigation phase (Article 3 of Annex IX of the Staff Regulations), those where a warning is issued after the investigation phase under Article 3 of Annex IX of the Staff Regulations and those where it has not been recommended opening an additional inquiry following positive or negative recommendations by OLAF.
- Files which did not lead to the opening of an enquiry ('non-case') will be kept for a period of 2 years from the date on which the Director of the Agency decides to close the file without follow-up. Reports which are relevant for OLAF cases with follow-up actions are retained for 20 years.

- Files of OLAF cases containing an investigation report, but closed without follow-up action are retained for 10 years.
- Files transmitted to OLAF and closed without investigation are retained for 5 years.

2.8. Rights of Access, Rectification, Blocking and Erasure

As mentioned in the Specific Privacy Statement, and in line with the Implementing Rules on data protection, data subjects may exercise their rights by addressing a written request to the controller.

2.9. Security measures

(…)

3. LEGAL ASPECTS

3.1. Prior checking

Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (hereinafter the "**Regulation**") applies to the *"processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system*" and to the processing "*by all [EU] institutions and bodies insofar as such processing is carried out in the exercise of activities all or part or which fall within the scope of [EU] law*"[2].

The EDPS considers that all the elements that trigger the application of the Regulation exist in the whistleblowing procedures. Firstly, the operation of the whistleblowing procedures entails the collection and further processing of *personal data* as defined under Article 2(a) of the Regulation. Indeed, as described in the notification for prior checking, personal data of individuals who make a report are processed, such as their name, contact details and the content of the report. Furthermore, personal information from individuals named by the whistle-blower is also collected and further processed. Secondly, as described in the notification (see e.g. section 10/ storage media of data) the personal data collected undergo "automatic processing" operations, as defined under Article 2 (b) of the Regulation.

Article 27.1 of the Regulation subjects to prior checking by the EDPS all "*processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes*". Article 27.2 of the Regulation contains a list of processing operations that are likely to present such risks. Under Article 27(2)(a) of the Regulation, processing operations relating to "*suspected offences, offences, criminal convictions or security measures*" shall be subject to prior checking by the EDPS. In the case in point, the processing operation could be related to the processing of these types of data. Furthermore, the EDPS considers that the notification also falls under Article 27(2)(b) of the Regulation (EC) No 45/2001 which stipulates that data operations which *"evaluate personal aspects relating to the data subject, including his or her (...) conduct*" shall be subject to prior checking by the EDPS. In the case under analysis, all sort of aspects related to data subjects are evaluated, from an evaluation of the whistle-blower to the evaluation of the conduct of individuals which are named by the call, thus triggering the application of Article 27(2)(b).

[2] *Ex* Article 3.2 of Regulation (EC) No 45/2001.

The notification of the DPO was received on 31 July 2013. According to Article 27(4) the present Opinion must be delivered within a period of two months. The procedure has been suspended during a total of 28 days in order for the EDPS to obtain necessary additional information.

The procedure was further suspended for 28 days to allow for provision of comments on the draft Opinion. Therefore, the present Opinion must be delivered no later than 28 October 2013.

3.2. Lawfulness of the Processing

Personal data may only be processed if legal grounds can be found in article 5 of Regulation (EC) No 45/2001.

As pointed out in the notification for prior checking, of the various grounds listed under Article 5 of the Regulation, the processing operation notified for prior checking falls under Article 5 a), pursuant to which data may be processed if the processing is "*necessary for performance of a task carried out in the public interest on the basis of the Treaties establishing the [EU] or other legal instruments adopted on the basis thereof*".

These requirements are indeed present in the processing operation under consideration. First, the processing is foreseen by the Staff Regulation, namely in Articles 22a and 22b thereof. Second, the processing is carried out in the public interest and is, in principle, necessary for the performance of the Agency's institutional tasks relating to prevention and combat of serious irregularities reported through the whistleblowing system.

3.3. Processing of Special Categories of Data

Taking into account that the purpose of the whistleblowing procedures is to facilitate the receipt of information about alleged wrongdoings affecting the EU financial interests, it is expected that in a number of cases this information will be related to offences or criminal convictions. In this regard, the EDPS recalls the application of Article 10.5 of the Regulation which establishes that *"[p]rocessing of data relating to offences, criminal convictions or security measures may be carried out only if authorised by the Treaties establishing the [EU] or other legal instruments adopted on the basis thereof or, if necessary, by the European Data Protection Supervisor"*. In the present case, processing of the mentioned data is authorised by the legal instruments mentioned in point 3.2 above.

As far as special categories of data are concerned, Article 10.1 of the Regulation establishes that "*the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and of data concerning health or sex life, are prohibited*". The notification for prior checking does not indicate that data falling under the categories of data referred to in Article 10.1 are processed in the context of the whistleblowing procedures. Taking into account the overall purpose of the processing operations, the EDPS understands that the collection of special categories of data is not TEN-T EA's main goal.

The EDPS considers nonetheless that TEN-T EA may become, perhaps involuntarily, in possession of special categories of data, which will often be of no interest/relevance to the investigation. In this regard, the EDPS recalls the application of the data quality principle, according to which data must be adequate, relevant and not excessive in relation to the purposes for which collected and/or further processed (Article 4.1.c). Pursuant to this

principle, if special categories of data that clearly are not relevant for the purposes of investigating fraud and other wrongdoings affecting the Community financial interests are collected through the whistleblowing procedure, they should be erased and not further processed. Investigators in charge of examining the reports should be made aware of this rule.

3.4. Data Quality

Pursuant to Article 4.1.c of the Regulation, personal data must be *"adequate, relevant and not excessive in relation to the purposes for which collected and/or further processed"*. This is referred to as the data quality principle.

The EDPS notes that it is up to individuals who decide to report a suspected irregularity to decide which information they want to provide to TEN-T EA. They may provide adequate and relevant information but they may also provide information that is completely irrelevant for the purposes sought by the whistleblowing procedure. On the other hand, TEN-T EA has the means to avoid or minimise this outcome in different ways. For example, it may indicate the type of information that is relevant and which falls within the scope of its competences. In this regard, the EDPS observes that the Guidelines clearly indicate in several instances the type of information which is relevant for the purpose of Article 22a of the Staff Regulation and the type of information which falls outside this scope (see in particular Section 1.4 of the Guidelines). This is helpful, but still not sufficient. If individuals file reports with information that is pointless for the purposes at stake, such information should not be retained. Irrelevant messages that constitute later on *prima facie* non cases should also be deleted as soon as possible. Furthermore, the personal data processed within the scheme should be limited to the data which is strictly and objectively necessary to verify the allegations made. TEN-T EA investigators should be made aware of this rule. The Guidelines should be updated to reflect the above requirements.

In addition to the above, it is important to recall the application of Article 4.1(d) of the Regulation requires that personal data must be *"accurate and where necessary kept up to date"*, and *"every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified"*. From a managerial and IT point of view, the competent TEN-T EA services should ensure that personal data kept in the context of the whistleblowing procedures are accurate and complete. This principle is very much connected to the exercise of the rights of access, rectification, blocking and erasure (see point 2.8 below). Obviously, if efforts have been put to ensure the accuracy and the update of personal data, there are likely to be fewer requests for rectification.

The EDPS welcomes the guarantees foreseen by the Guidelines for whistleblowers, especially that concerning confidential treatment. In this regard, the EDPS stresses that preserving the confidentiality of whistleblowers (and all informants in general) is of the utmost importance. Confidentiality should be ensured by default, without there being a need for specific request. Furthermore, confidentiality should be ensured not only vis-à-vis the accused persons, but more widely internally and externally. Internal disclosure should occur only where such disclosure is absolutely necessary for the purpose of the investigation. The confidentiality of whistleblowers should be guaranteed throughout the life span of a case. The identity of these persons should not be disclosed, except when this would contravene national rules on judicial procedures and/or where they maliciously make a false statement. In those cases, these personal data could only be disclosed to judicial authorities.

Finally, the provisions of the Guidelines governing the loss of confidential treatment contain an apparent contradiction which should be reviewed or clarified. On the one hand, the Guidelines first provide that good faith is presumed unless and until proven otherwise. Staff members who make a report in bad faith, particularly if it is based knowingly on false or misleading information, shall not be protected and shall normally be subject to disciplinary measures. The burden of proof in this context is on the Agency (Section 1.4). On the other hand, they provide that the protection may be lost if the staff member makes unwarranted or damaging allegations that s/he cannot show to be honest or reasonable (Section 3). It is therefore not clear whether it is for whistleblowing to prove the veracity of their statements or on the Agency to prove di false or misleading character. This aspect should be clarified.

3.5. Conservation of Data

The notification identifies different retention periods, according to whether or not the report has given rise to an investigation, disciplinary procedures, OLAF investigation, etc. Further to a specific question, TEN-T EA DPO clarified that these periods correspond to the retention periods set out in the Commission's Common Retention List ("CRL"). The DPO further clarified that TEN-T EA has no margin of manoeuvre when it comes to the fixing of these periods, which are basically binding on EU agencies such as TEN-T EA. In light of the above, the EDPS has decided to deal with the issue of retention periods set in CRL more broadly together with the Commission. The outcome of this analysis, which will result in a modification of the CRL will ultimately be binding also on TEN-T EA.

The notification sets out that the data concerning whistleblowing reports will be stored after the expiry of the conservation period in an anonymous form for statistical purposes. When requested to provide information on how the anonymity would be guaranteed, the DPO stated that she could not answer because there is no experience to date. The EDPS is concerned that in a relatively small professional environment, such as that of EU agencies, the simple withdrawal of the names of the individuals may not be enough to ensure full anonymity in line with Article 4(1)(e) of the Regulation. TEN-T EA should therefore pay particular attention to preserve anonymity of personal data retained for statistical purposes, with particular regard to all the measures necessary to avoid indirect identification. It should report on this point to the EDPS.

3.6. Transfer of Data

Articles 7, 8 and 9 of the Regulation set forth certain obligations that apply when data controllers transfer personal data to third parties. The rules differ depending on whether the transfer is made *ex* Article 7 to EU institutions or bodies, *ex* Article 8 to recipients subject to Directive 95/46 or to other types of recipients *ex* Article 9.

The notification lists a number of possible recipients all falling under the scope of Article 7 of the Regulation, as transfers within or between EU institutions or bodies. The EDPS has in principle no remarks concerning the identified categories, which all may be legitimately recipients of whistleblowing related data. However, he stresses that the requirements under Article 7 of the Regulation must be assessed on a case by case basis. In particular, data should be transferred on a strictly need to know basis, only where necessary for the legitimate performance of tasks covered by the competence of the recipient. The EDPS also considers that the identity of the person making the report should in principle not be disclosed.

The EDPS takes note of the fact that TEN-T EA does not foresee any transfer of the information contained in the report to entities falling under the scope of Articles 8 and 9 of the Regulation (e.g. national authorities). This is without prejudice of follow-up transfers carried out in the framework of ensuing administrative investigations and disciplinary proceedings, which however fall outside the present prior-check and should be notified separately.

3.7. Information to the Data Subject

Pursuant to Articles 11 and 12 of the Regulation, those who collect personal data are required to inform individuals to whom the data refers of the fact that their data are being collected and processed. Individuals are further entitled to be informed of, *inter alia,* the purposes of the processing, the recipients of the data and their specific rights as data subjects.

The EDPS welcomes that TEN-T EA has prepared a privacy statement which will be published in the Internet and on my Intracomm. The EDPS advises TEN-T EA to post the privacy policy either in a page through which visitors who want to report must necessarily go through or alternatively in a very prominent way, immediately after or before the information on the whistleblowing procedures.

While the provision of information through the privacy statement placed in the website is certainly a positive step, the EDPS considers that this is not sufficient. The EDPS is concerned that in some instances individuals may use the whistleblowing procedure without visiting TEN-T EA web site. He therefore recommends that TEN-T EA provide the individuals making a report with a specific privacy statement as soon as practically possible. In most cases, this may be done through an e-mail sent as soon as possible to the e-mail address of the recipient.

The EDPS has also checked the content of the information provided in the privacy statement and considers it to be in principle in line with the requirements of Articles 11 and 12 of the Regulation. However, concerning the statement that the right of rectification only applies to factual data, the EDPS would recommend reconsidering this limitation as it may not be excluded the need of a whistle-blower to rectify some non-factual information provided. Excluding in all cases rectification of non-factual data may be excessive. Furthermore, TEN-T EA should add information concerning confidential treatment and protection measures.

Having regard to the other persons named in the report, the EDPS recalls that *ex* Article 12 of the Regulation such individuals as well have the right to receive information about the processing of their data. The existence of a similar obligation under the Data Protection Directive was highlighted by the Article 29 Working Party in its Opinion on whistleblowing schemes[3]: "*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*". TEN-T EA should implement such an obligation.

[3] 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, WP 117, adopted on 1 February 2006. According to the Article 29 Working Party, the individual must be informed about "[1] the entity responsible for the whistle blowing 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".

The same Opinion recognises that "*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"*. A similar exception exists under Article 20 of Regulation (EC) No 45/2001. In particular, this Article provides for certain restrictions to the right of information notably where such a restriction constitutes a necessary measure to safeguard *"(a) the prevention, investigation, detection and prosecution of criminal offences; (b) an important economic or financial interest of a Member State or of the European Communities, including monetary, budgetary and taxation matters; (c) the protection of the data subject or of the rights and freedoms of others"*.

In the case in point, the application of Article 20 of the Regulation enables TEN-T EA to *defer* the provision of information to safeguard the interests mentioned in subsections (a), (b) and (c). TEN-T EA will have to assess whether the provision of information to the person named by the caller would jeopardise the values mentioned above under subsections (a), (b) and (c) of Article 20, in which case the provision of information may be deferred. When the information is deemed to be irrelevant, in most cases, the EDPS does not see any possible use of the exception (a) and (b) of Article 20 of the Regulation. Under these circumstances, in principle, there will be neither an investigation *per se* to protect nor a financial interest at stake. Yet, the controller may rely on section (c) if it considers that deferring the information is necessary in order to safeguard *"the protection of the data subject or of the rights and freedoms of others"*, for example, if it considers that the disclosure of information may reveal the identity of the whistleblower or informant which may be the case in a number of instances. In deciding whether it is under the obligation to provide information or whether an exception applies, TEN-T EA must engage in a case-by-case assessment of the circumstances of the particular data processing at stake.

If it uses an exception to defer the provision of information, TEN-T EA should take into account that the restrictions to a fundamental right cannot be applied systematically. It must assess in each case whether the conditions for the application of one of the exceptions, for example, Article 20.1.a or 20.1 c may apply. In addition, as foreseen in Article 20 of the Regulation, the measure has to be "necessary". This requires that the "necessity test" has to be conducted on a case-by-case basis. If it uses an exception, TEN-T EA must comply with Article 20.3 according to which *"the data subject shall be informed, in accordance with Community law, of the principal reasons on which the application of the restriction is based and of his or her right to have recourse to the European Data Protection Supervisor*". However, TEN-T EA may avail itself of Article 20.5 to defer the provision of this information as set forth in this Article: *"Provision of the information referred to under paragraphs 3 and 4 may be deferred for as long as such information would deprive the restriction imposed by paragraph 1 of its effect"*.

3.8. Rights of Access and Rectification

The right of access is the right of the data subject to be informed about any information relating to him or her that is processed by the data controller. According to Article 13 of the Regulation, the data subject shall have the right to obtain without constraint from the controller, communication in an intelligible form of the data undergoing the processing and any available information as to their source. The information can then be obtained directly by the data subject (this is the so-called "direct access") or, under certain circumstances, by a

public authority (this is the so-called "indirect access", normally exercised by a Data Protection Authority, being the EDPS in the present context).

As to the whistle-blowers, the privacy statement declares that individuals have such a right regarding the information that the controller holds about them. It gives the name and e-mail of the person in charge of the processing operations as the contact person to exercise such rights. The practice as described in the privacy statement is in line with the Regulation. Having regard to the persons named in a whistleblowing report, the EDPS reminds that such rights may be deferred if one of the conditions of sections (a), (b) and (c) of Article 20 the Regulation is present. The Article 29 Working Party's Opinion on Whistleblowing stressed that these rights "*may be restricted in order to ensure the protection of the rights and freedoms of others involved in the scheme*", which is the hypothesis foreseen under subsection (c) of Regulation (EC) No 45/2001.

In the context of exercising the right of access, the EDPS would like to stress the Article 29 Working Party's recommendations pursuant to which *"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 order to ensure compliance with the above, the EDPS recommends that when access is granted, personal information of third parties, such as informants or whistleblowers, be deleted. If providing access, even if the personal information is deleted, may reveal personal details of third parties such as whistleblowers and informants, access should be deferred.

3.9. Security measures

(…)

4. Conclusion

There is no reason to believe that there is a breach of the provisions of the Regulation, provided that the considerations in this Opinion are fully taken into account. In particular, TEN-T EA must implement the following recommendations:

- If special categories of data clearly not relevant for the underlying purposes, are collected through the whistleblowing report, they should be deleted and not further processed. TEN-T EA members in charge of reading and assessing reports should be made aware of this rule.

- Information that is irrelevant for the underlying purposes should not be retained and further processed. TEN-T EA members in charge of reading and assessing reports should be made aware of this rule. Also, irrelevant information that will constitute later on prima facie non cases should be deleted as soon as possible. The Guidelines should be updated accordingly.

- From a managerial and IT point of view, the competent TEN-T EA services should ensure that personal data kept in the context of the whistleblowing procedures are accurate and complete.

- Confidentiality should be ensured not only vis-à-vis the accused persons, but more widely internally and externally. Internal disclosure should occur only where such disclosure is absolutely necessary for the purpose of the investigation. The confidentiality of informants should be guaranteed throughout the life span of a case, except when this would contravene national rules on judicial procedures and/or where they maliciously make a false statement. In those cases, these personal data could only be disclosed to judicial authorities. The allocation of the burden of proof regarding good faith and false and/or misleading character of the information provided should be clarified.

- TEN-T EA should therefore pay particular attention to preserve anonymity of personal data retained for statistical purposes, with particular regard to all the measures necessary to avoid indirect identification. It should report on this point to the EDPS.

- The privacy statement should be amended in relation to the exclusion of the rectification of non-factual data. TEN-T EA should add information concerning confidential treatment and protection measures. TEN-T EA should provide the individuals making a report with a specific privacy statement as soon as practically possible.

- The EDPS calls upon TEN-T EA to ensure the rights to information and access of those people who have been named in whistleblowing reports, subject to the application of the exceptions of Article 20 of the Regulation (see Section 3.8). TEN-T EA must decide on a case-by-case basis whether the exceptions apply.

Done at Brussels, 28 October 2013

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor