Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Commission regarding the "Risk analysis for fraud prevention and detection in the management of ESF and ERDF" - ARACHNE

Brussels, 17 February 2014 (2013-0340)

1. PROCEEDINGS

On 17 May 2013, the European Data Protection Supervisor (**EDPS**) received a notification for prior checking relating to the processing of personal data "Risk analysis for fraud prevention and detection in the management of ESF and ERDF - ARACHNE" from the Data Protection Officer (**DPO**) of the European Commission (**COM**).

Questions were raised on 4 June 2013, to which the DPO of the COM replied on 26 June 2013. In the meantime, a meeting took place between the EDPS and COM services on 7 June 2013. Additional questions were sent on 27 June 2013; respective answers were received on 30 October 2013. The draft Opinion was sent to the DPO for comments on 18 November 2013. The EDPS received a reply on 26 November 2013, based on which on the same day the EDPS requested to receive a revised notification, which was received on 29 November 2013. A meeting was requested by the EDPS on 9 December 2013, which took place on 9 January 2014 and was followed-up by the submission of additional documents on 17 January 2014. A revised draft Opinion was sent to the DPO for comments on 24 January 2014, who confirmed on 13 February 2014 that he had no comments.

2. FACTS

The ARACHNE system is part of the COM's fraud prevention and detection strategy in the area of Structural Funds (European Social Fund -ESF- and European Regional Development Fund -ERDF-). Structural Fund assistance is implemented via a system of "shared management", meaning that the Member States are responsible for the implementation of the assistance, but the COM still has the final financial responsibility. Directorate H of the Employment, Social Affairs and Inclusion Directorate General (DG) and Directorate J of the Regional Development DG of the COM have the main responsibility of validating information provided by the authorities covered by the ESF and the ERDF[1], carrying out external audits within EU Member States, issuing timely reports and opinions and updating a risk score table in order to allow a sound management of the Funds.

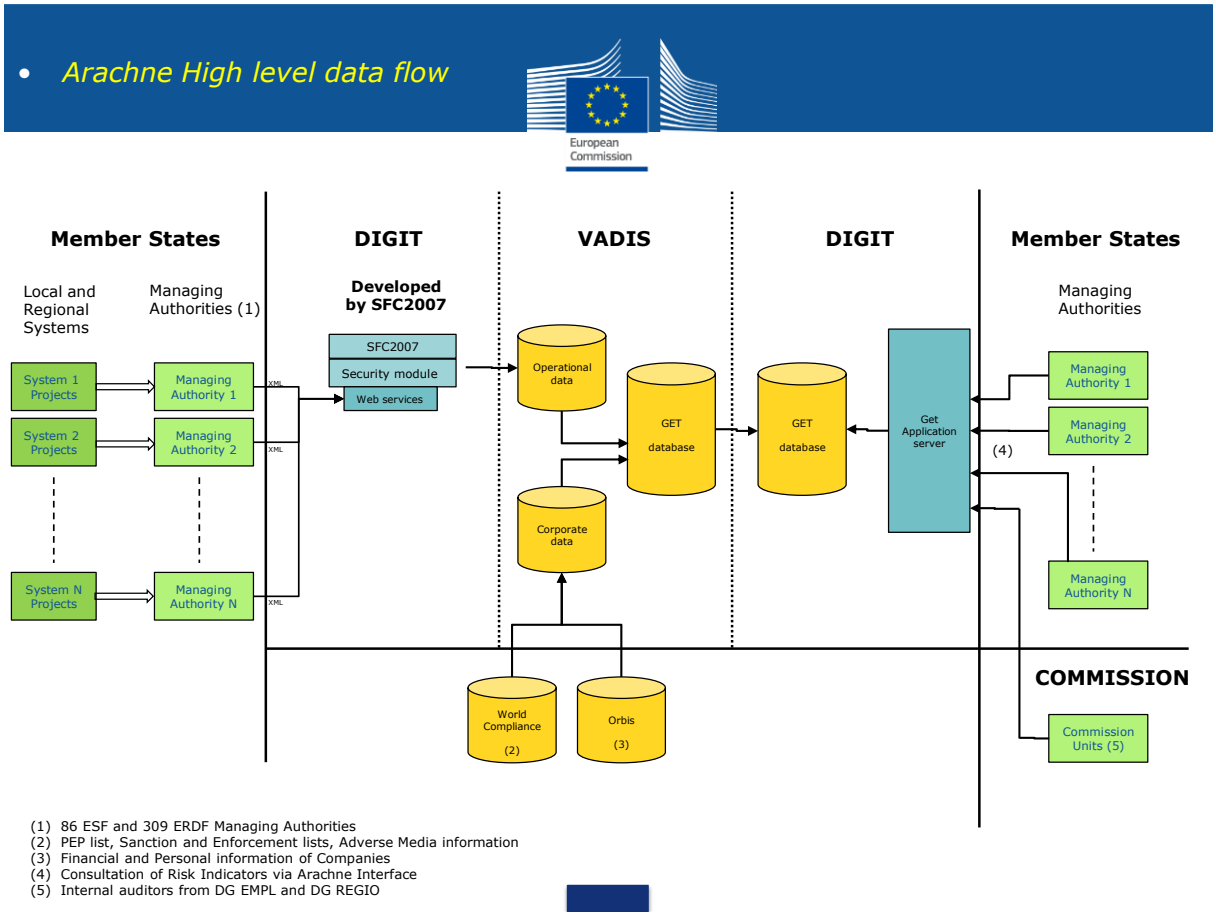
The **purpose** of the ARACHNE system is fraud detection. During the meeting of 9 January 2014, the COM explicitly confirmed that ARACHNE does not aim at assessing the particular

[1] Description of the Management and Control System, Audit Strategy, Annual Control Report/Annual Opinion, National Audit Reports, Annual Summaries.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30
E-mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

individual conduct of fund recipients and does not as such serve to exclude any beneficiaries from the Funds. ARACHNE complements an existing database of projects implemented under the Structural Funds (SFC) with publicly available information in order to identify the most risky projects, based on a set of risk indicators. It was highlighted during the meeting of 9 January 2014 that the risk score does not lead to any automatic decision against beneficiaries. Risk scores are used to help auditors in selecting/identifying future candidates for audit. ARACHNE as a system is based on the integration and customisation of an existing risk assessment tool, the GET application from *VADIS Consulting SA/NV*, with operational data provided by the ESF and ERDF managing authorities so as to provide risk scores to identify the most risky projects and the specific risk zones.

In a first step of the **procedure**, the current SFC2007 infrastructure, a web services implementation transmitting operational data of the projects from Member States' ESF and ERDF managing authorities to the COM, will be used to provide ARACHNE with operational data. In a second step, the project data will be further complemented with information from publically available sources. In a third step, ARACHNE will calculate individual risk indicators (risk scoring sheets per project) allowing for a sound management of the Funds, including ongoing monitoring for the purpose of auditing projects.



The **controller** is the COM, here jointly represented by the Director of Directorate H of the Employment, Social Affairs and Inclusion DG and Directorate J of the Regional Development DG. According to additional information received on 26 November 2013, the COM does not collect data itself, but all data comes from an existing database of projects implemented under the Structural Funds (SFC) or the external provider. *VADIS SA/NV*, as sub-contractor of *ATOS Belgium NV/SA*, carries out the processing operation on behalf of the COM in the sense of Article 23 of the Regulation No 45/2001 ("the Regulation"). *VADIS SA/NV* as **processor** provides the resulting GET database to the COM, which hosts the GET application for the

final users. As confirmed during the meeting of 9 January 2014, *VADIS SA/NV* does not transfer individual records or otherwise share information. This activity is governed by a written contract provided on 17 January 2014, which stipulates in particular that the processor acts on instructions from the controller and contains written clauses setting out the obligations in Articles 21 and 22 of the Regulation, which are incumbent on the processor.

Data subjects concerned are natural persons as the beneficiaries, respectively as the managers and publicly known shareholders of beneficiaries which are legal entities, receiving assistance from the ESF and/or the ERDF and possible other persons having relationships with them.

According to the notification, the **legal basis** of the ARACHNE system encompasses:

- Articles 60, 61, 62, 69 and Chapter IV, Sections 1 and 2, of Regulation 1083/2006[2];
- Articles 13, 14, 16, 19, 37 as well as Section 7 of Regulation 1828/2006[3] ;
- Chapter 2.2.3 of the Commission's Communication on the Anti-Fraud Strategy of 22 June 2011[4];
- Regulation 966/2012[5] in the light of Articles 325 and 317 of the Treaty on the functioning of the European Union (TFEU).

The **categories of data** processed are, according to the notification, the following:
1) From the ESF and ERDF managing authorities (through the SFC2007 infrastructure):
- Beneficiaries: name, address, VAT number, role;
- Key staff: name, function;
- Contractors: name, address, VAT number;
- Key experts for service contracts: name, date of birth.

2) From external public data sources provided by VADIS SA/NV:
a) From commercial provider ORBIS (http://www.bvdinfo.com/Products/Company-Information/International/Orbis):

- Comprehensive information on companies;
- Shareholders/management/key staff: name, function;

b) From commercial provider WORLD COMPLIANCE:

- Profiles of Politically Exposed Persons (PEP), as well as those of their family members and close associates;
- Sanction List, which includes individuals and companies with the highest risk rating;
- Enforcement List, including information received from regulatory and governmental authorities and the content of warnings and actions against individuals and companies;
- Monitoring of newspapers and magazines for risk relevant info (including information from major on-line newspapers in the Member States of the European Union and in third countries).

The **recipients** are the ARACHNE users:

[2] Council Regulation (EC) No 1083/2006 of 11 July 2006 laying down general provisions on the European Regional Development Fund, the European Social Fund and the Cohesion Fund (OJ L 210, 31.7.2006, p. 25).
[3] Commission Regulation (EC) No 1828/2006 of 8 December 2006 setting out rules for the implementation of Council Regulation (EC) No 1083/2006 laying down general provisions on the European Regional Development Fund, the European Social Fund and the Cohesion Fund and of Regulation (EC) No 1080/2006 of the European Parliament and of the Council on the European Regional Development Fund (OJ L 371, 27.12.2006, p. 1).
[4] COM(2011) 376 final, see http://ec.europa.eu/anti_fraud/documents/preventing-fraud-documents/ec_antifraud_strategy_en.pdf.
[5] Regulation No 966/2012 of the European Parliament and of the Council of 25 October 2012 on the financial rules applicable to the general budget of the Union (OJ L 298, 26.10.2012, p. 1).

- The Managing Authorities and their Intermediary Bodies in the Member States, their Certifying Authorities and the Audit Authorities;
- The COM's DG for Employment, Social Affairs and Inclusion and the DG for Regional Policy (in each case limited to the Auditors Unit), with the exception of Directorate H of the Employment, Social Affairs and Inclusion DG and Directorate J of the Regional Development DG;
- The European Court of Auditors and OLAF (upon their request).

Only the Managing Authority and its intermediary bodies will have read and write access. In case of technical problems, the information may be accessed by the COM's DG for Informatics and *VADIS SA/NV*.

Data subjects are **informed** of the processing operation by means of a Privacy Statement available on the Europa Social Fund website, which next to the mandatory information under Articles 11 and 12 of the Regulation explain how risk management in the context of ARACHNE works and is performed and refer to its legal basis.

Regarding the data subjects' **rights of access and rectification**, one needs to distinguish between (a) data held by the Managing Authorities and their Intermediary bodies in the Member States dealing with the ESF and ERDF funds or to other national competent authorities, which is subject to Directive 95/46/EC, and (b) data held by the COM, which is subject to the Regulation:

a) As noted in the Privacy Statement (re-notified on 29 November 2013), data subjects can exercise their rights of access and rectification of the data held on the legal entity they represent or regarding their personal data by making a request to the Managing Authorities and their Intermediary bodies in the Member States dealing with the ESF and ERDF funds or to other national competent authorities. In case of change of project data, the Member State authorities can immediately alter the data in the database of projects implemented under the Structural Funds (SFC). Data subjects are further informed that they may also contact their national personal data protection supervisory authority in case of any difficulties or for any questions relating to the processing of these data. According to the notification, "*Member States will proceed according to what provided for by Directive 95/46/EC*";

b) Regarding the information derived from external media sources, which the COM does not itself collect, but processes, the EDPS understands that the "*Data subject should ask the source of the information in case they need their rights granted <u>further than</u> the ARACHNE system*" (emphasis added). The granting of access and rectification rights in the context of the ARACHNE system does not go *beyond* that system.

According to the Privacy Statement, for the COM, *"Art. 20.1(b) of Reg.45/2001 applies. Data subjects' right of access pursuant to art. 13, will be assessed case by case and delayed in case this could give potential fraudsters opportunities to find possible weaknesses in the risk assessment process and thus circumvent it. Access will then be given once a decision of not auditing is taken or at the time of the performance of the audit.*". The notification mentions in this regard that "*...for the same reason, the logic leading to the risk assessment outcome will not be revealed. This is not a restriction of art. 13, though, since decisions are only supported by the system and not automated by it*.".

As regards the data obtained from external public data sources by the commercial providers, according to the notification (as provided on 29 November 2013), the system will be updated:

- quarterly with a complete new set of data from the commercial provider (this is based on the annual accounts of beneficiaries and allowing the COM to take this into account in the next risk score);
- weekly with new data coming from Member States (through SFC or through the feedback loop). Member States cannot alter the risk score or other imported data directly in ARACHNE, but can add a comment in ARACHNE to keep track of any requests made by data subject.
- Where an ARACHNE user, i.e. the COM or a Member State, identifies an error or inconsistency (incorrect information on directorship, incorrect information on shareholders, incorrect information in press/media, incorrect name matches between data sources) in the external data, he/she can report this to *VADIS SA/NV* through a procedure referred to as "feedback loop". The rectifications introduced by *VADIS SA/NV* via the "feedback loop" will impact on the ARACHNE system, not on the initial source of information itself. According to the notification "*Data subject should ask the source of the information in case they need their rights granted further than the ARACHNE system*".

In the Privacy Statement, data subjects are further informed that they can contact the COM's Data Protection Officer (whose email address is given) in case of any difficulties or for any questions relating to the processing of these data and that they can find more information about this personal data processing in the Notification Public Register searching for the notification number 3580.

As regards the **conservation of the data**, these are retained for three years following the closure of an operational programme and in accordance with the requirements of Article 90 of Regulation 1083/2006. According to the Privacy Statement, data will not be maintained for statistical purposes.

Definition of the foreseen system's technical architecture: (...)

3. LEGAL ANALYSIS

3.1. Prior checking

The notified operations constitute a processing of personal data ("*any information relating to an identified or identifiable natural person*") in the sense of Article 2(a) of Regulation (EC) 45/2001 ("the Regulation"). It is performed by a body of the EU in the exercise of activities which fall within the scope of the Treaties. The processing of the data is done, at least in part, through automatic means. Therefore, the Regulation is applicable.

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 non-exhaustive list of processing operations that are likely to present such risks. Letter (a) mentions among others processing data relating to suspected offences, offences and criminal convictions. Letter (b) mentions processing operations intended to evaluate personal aspects relating to the data subjects, including their conduct. Letter (c) refers to processing operations that allow linkages between data originally processed for different purposes not provided for in national or Union legislation. Finally, letter (d) subjects processing operations that have the

purpose of excluding individuals from a contract to prior checking. In the notification, all of these points were mentioned as reasons for prior checking.

During the meeting of 9 January 2014, the COM explicitly confirmed that ARACHNE does not aim at assessing the particular individual conduct of fund recipients in the sense of Article 27(2)(b). However, as described above in Section 2, personal data related to (suspected) offences in the sense of Article 27(2)(a) may be processed (Sanction list by WORLD COMPLIANCE). For this reason, the processing operation is subject to prior checking.

The notification of the DPO was received on 17 May 2013. The draft Opinion was sent to the DPO for comments on 18 November 2013. The EDPS received a reply on 26 November 2013 and a revised notification and Privacy Statement on 29 November 2013. A meeting was requested by the EDPS on 9 December 2013, which took place on 9 January 2014 and was followed-up by the submission of additional documents on 17 January 2014. A revised draft Opinion was sent to the DPO for comments on 24 January 2014. According to Article 27(4) of the Regulation, the present Opinion must be delivered within a period of two months. In total, the case has been suspended for 216 days. In consideration of all the periods of suspension, the Opinion must therefore be rendered no later than 17 February 2014.

3.2. Lawfulness of the processing

Under Article 5(a) of the Regulation[6], a two-step test needs to be carried out to assess: (1) whether either the Treaty or other legal instruments foresee a public interest task on the basis of which the data processing takes place (legal basis), and (2) whether the processing operations are indeed necessary for the performance of that task.

In the notification, the COM refers to provisions of Regulation 1083/2006 and Regulation 1828/2006, the COM's Communication on the Anti-Fraud Strategy as well as Regulation 966/2012 as possible legal bases. Several of these provisions do not constitute appropriate legal bases for the notified processing operation, as will be discussed below:

- **Regulation 966/2012** contains the financial rules applicable to the general budget of the Union. From the text alone, the COM's activities relating to ARACHNE would not be foreseeable. For example, data subjects would not be in a position to understand the extent to which personal data about themselves might be collected and further processed within ARACHNE. Regulation 966/2012 is, as such, therefore too general to serve as a legal basis under Article 5(a);

- **Regulation 1083/2006**: Article 60(c) of Regulation 1083/2006 stipulates that the managing authority shall be responsible for, in particular, "*ensuring that there is a system for recording and storing in computerised form accounting records for each operation under the operational programme and that the data on implementation necessary for financial management, monitoring, verifications, audits and evaluation are collected; ...*". Under Article 61(e) of Regulation 1083/2006, the certifying authority of an operational programme shall be responsible in particular for "*maintaining accounting records in computerised form of expenditure declared to the Commission...*". Whilst both provisions refer to an IT based monitoring system, they empower the management and the certification authority, thus Member State entities under Article 59(a) of Regulation 1083/2006 and not the COM to operate it. The EDPS considers,

[6] Article 5(a) of the Regulation authorises a processing that is "*necessary for performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof*".

however, that the legal basis for the purpose of Article 5(a) must be found in legal provisions which are directly applicable to the COM.

Article 66 of Regulation 1083/2006 notes that for the purpose of ensuring the quality of the implementation of the operational programme, "*Data exchange between the Commission and the Member States...shall be carried out electronically, in accordance with the implementing rules of this Regulation adopted by the Commission in accordance with the procedure referred to in Article 103(3)*". Whilst this provision can serve as the legal basis of the current SFC2007 infrastructure (web services implementation) for the transmission of the operational data of the projects from the managing authorities of the Member States to the COM, it does not refer to the purpose of fraud prevention pursued by ARACHNE.

- **Regulation 1828/2006**: Under Article 19(1) of Regulation 1828/2006, for the purposes of Article 90 of Regulation (EC) No 1083/2006 (entitled "*Availability of documents*"), *"...the managing authority shall ensure that a record is available of the identity and location of bodies holding the supporting documents relating to expenditure and audits, which includes all documents required for an adequate audit trail*.". Where documents exist in electronic version only, Article 19(6) of Regulation 1828/2006 stipulates that "*the computer systems used must meet accepted security standards that ensure that the documents held comply with national legal requirements and can be relied on for audit purposes*.". Whilst these provisions refer to an IT based monitoring system, they empower the management authority, thus Member State entities, and not the COM to operate it. The EDPS considers, however, that the legal basis for the purpose of Article 5(a) must be found in legal provisions which are directly applicable to the COM.

  Article 34 of Regulation 1828/2006 stipulates that "*The Commission may use any information of a general or operational nature communicated by Member States under this Regulation to perform risk analyses and may, on the basis of the information obtained, produce reports and develop early-warning systems serving to identify risks more effectively*" (emphasis added). **Section 7** of Regulation 1828/2006 ("*Electronic exchange of data*") foresees the establishment of a computer system for the exchange of data as a tool for the exchange of all data relating to the operational programme (Article 39(1)), which "*shall be accessible to the Member States and the Commission either directly or via an interface for automatic synchronisation and recording of data with national, regional and local computer management systems*"(Article 42(1)).
  Whilst this would seem to be a sufficient legal basis to develop IT risk assessment tools, it is circumscribed by the limitation to information obtained from Member States *in the context of the current SFC2007 infrastructure* (web services implementation) for the transmission of the operational data of the projects from the managing authorities of the Member States to the COM ("*on the basis of the information obtained*..."). ARACHNE, however, goes beyond such information, as according to the notification, the project data will be further complemented with information from publically available sources. Article 34 of Regulation 1828/2006 is therefore not a comprehensive legal basis under Article 5(a) for the ARACHNE system.

- The COM's **Communication on the Anti-Fraud Strategy** states in Chapter 2.2.3 that "*The Services will assess the need to improve fraud risk assessment by developing a more systematic and formalised process for identifying areas of fraud risk. In parallel, making the most efficient use of existing resources, they should introduce smart controls using the IT tools, duly adapted to their needs, which have been developed by some Services in collaboration with OLAF. Such tools enable, for example, the pooling of*

existing data linked to closed or ongoing EU-funded projects. This is useful for fraud prevention purposes, but can also detect plagiarism and fraudulent double funding. These tools will be fully effective only if the relevant information systems contain complete, consistent and reliable data on EU funds. The possibility of analysing data for fraud prevention purposes should also be taken into consideration when defining business requirements for new IT systems.".

In view of the above, the EDPS considers that the combination of Article 34 and Section 7 of Regulation 1828/2006 as well as Chapter 2.2.3 of the COM's Communication on the Anti-Fraud Strategy constitute a sufficient legal basis for the purposes of Article 5(a) of the Regulation.

The notified processing operations also appear in principle necessary for the purpose of fraud detection and prevention. Without risk scores to identify the most risky projects and the specific risk zones resulting from all sources feeding information into ARACHNE for ongoing monitoring, the COM would not be able to detect and prevent fraud in the area of Structural Funds to the same extent. It should be borne in mind, however, that necessity is a question of degree, and the COM must ensure that such monitoring does not exceed what is appropriate and proportionate to the aim pursued. These aspects will be analysed in Section 3.4 below.

3.3. Processing of special categories of data

Article 10(1) prohibits the processing of personal data revealing racial or ethnic origin, political opinion, religious or philosophical beliefs, trade-union membership, and of the data concerning heath or sex life. The processing of these special categories of data is prohibited unless one of the exceptions under Article 10(2) applies. Account should also be taken of Article 10(4) of the Regulation stating that "*[s]ubject to the provision of appropriate safeguards, and for reasons of substantial public interest, exemptions in addition to those laid down in paragraph 2 may be laid down by the [EU Treaties] or other legal instruments adopted on the basis thereof or, if necessary, by decision of the European Data Protection Supervisor*".

According to the notification, the controller did not identify any special categories of data among those mentioned in Article 10(1)[7].

However, even if the processing of special categories of data is not the primary purpose of the processing, it cannot be excluded that processing of such data may occur. For example, the use of the Sanction List may well reveal political opinions, religious or philosophical beliefs. In these cases, the EDPS recalls that the prohibition under Article 10(1) must be respected or otherwise it has to be evaluated in a restricted manner whether the application of an exception would be necessary. In any case, recipients must be made aware of this rule and avoid processing special categories of data unless one of the exceptions foreseen in Article 10(2) or Article 10(4) applies.

Article 10(5) allows "*processing of data relating to offences, criminal convictions or security measures [...] only if authorised by the Treaties [...] or other legal instruments adopted on the basis thereof or if necessary, by the European Data Protection Supervisor, subject to*

[7] The notification mentions with regard to PEP as well as their family members and close associates that *"No political-party membership or other data prohibited by Article 10 of the Regulation 45/2001 will be processed (e.g. the name of the president of a state may be processed for its official role but not for being member of a specific political party)..."*.

appropriate safeguards". Regulation 1828/2006 or any of the other legal instruments brought forward in the notification as legal basis does not appear to contain any specific reference to the fact that COM would be collecting and processing data relating to offences under Article 10(5). However, whilst the COM's Communication on the Anti-Fraud Strategy[8] is not a legal instrument, it implements the obligations incumbent on the COM under Article 32(4)(a) of Regulation 966/2012 to implement "*an appropriate risk management and control strategy coordinated among appropriate actors involved in the control chain*" and under Article 60(c) of Regulation 1083/2006 to ensure "*that there is a system for recording and storing in computerised form accounting records for each operation under the operational programme and that the data on implementation necessary for financial management, monitoring, verifications, audits and evaluation are collected*". These obligations are more broadly reflected in Articles 325 and 317 TFEU.

The EDPS therefore suggests that the COM consider adopting a more specific legal basis (a decision at the appropriate administrative level) authorising the COM to process data under Article 10(5) in application of the relevant provisions of Regulations 966/2012 and 1083/2006. The processing of special categories of data should in any case be limited to the extent necessary for complying with legal obligations regarding both Regulations. Appropriate safeguards to ensure necessity, proportionality and data quality should be set out in this respect (see also below Section 3.4).

3.4. Processing of personal data on behalf of the controller

VADIS SA/NV as processor carries out the data collection and preparation process. This activity is governed by a written contract stipulating in particular in its Annex I, Article II.6 that the processor acts on instructions from the controller and contains written clauses setting out the obligations in Articles 21 and 22 of the Regulation, which are incumbent on the processor (Annex I, Article II.6.6).

The COM thus in principle complies with Article 23 of the Regulation. Nevertheless, the EDPS would be in favour of a data protection clause about the obligations of the processor exclusively. The processor should rather be informed about the conditions surrounding the processing of his data by the Commission through a privacy statement. Moreover a processing operation involving complex technology could benefit from a specific data protection clause (see for e.g. our recommendation in point 3.6).

3.5. Data Quality

Article 4(1)(c) of the Regulation states that data must be adequate, relevant and non excessive in relation to the purposes for which collected and/or further processed. This includes that data must be kept accurate and up to date; every reasonable step must be taken to ensure that inaccurate or incomplete data are rectified or erased (Article 4(1)(d) if the Regulation).

[8] In its chapter 2.2.3, it explicitly states that "*The Services will assess the need to improve fraud risk assessment by developing a more systematic and formalised process for identifying areas of fraud risk. In parallel, making the most efficient use of existing resources, they should introduce smart controls using the IT tools, duly adapted to their needs, which have been developed by some Services in collaboration with OLAF. Such tools enable, for example, the pooling of existing data linked to closed or ongoing EU-funded projects. This is useful for fraud prevention purposes, but can also detect plagiarism and fraudulent double funding. These tools will be fully effective only if the relevant information systems contain complete, consistent and reliable data on EU funds. The possibility of analysing data for fraud prevention purposes should also be taken into consideration when defining business requirements for new IT systems.*".

In the case at hand, some of the data categories can be reasonably assumed to be of high enough quality, such as identification data supplied by data subjects themselves to the ESF and ERDF managing authorities (available within ARACHNE through the SFC2007 infrastructure) or extracts from the Sanctions and Enforcement Lists.

For those data based on external public data sources, this cannot be affirmed. In the context of the processing at hand, these are obtained from two commercial providers (who inter alia monitor newspapers and magazines for risk relevant info). Here, the COM must take appropriate steps to ensure a high level of accuracy.

a) The EDPS welcomes the existence of the procedure referred to as "feedback loop". However, the EDPS would like to note that, according to the notification, an ARACHNE user identifying an error or inconsistency in the external data *can* report this to *VADIS SA/NV*. There thus seems to be *no obligation* to report errors or inconsistencies for ARACHNE users. This is not sufficient to ensure an appropriate degree of accuracy of the personal data. The EDPS recommends that reporting identified error or inconsistency in the external data to *VADIS SA/NV* becomes obligatory for ARACHNE users.

b) Regarding the information derived from external media sources, the EDPS understands that the "*Data subject should ask the source of the information in case they need their rights granted further than the ARACHNE system*" (emphasis added). The EDPS acknowledges that the granting of access and rectification rights in the context of the ARACHNE system does not go *beyond* that system.

However for information derived from external media sources, the EDPS recommends that the COM develops and implements effective measures in the context of its contractual relationship with the processor (*VADIS SA/NV*) to guarantee a high level of data quality that go beyond the procedure referred to as "feedback loop". These measures could for example cover the following[9]:

- individuals performing monitoring of external media sources should receive training on how to conduct it in a manner which is compliant with data protection requirements, in particular the strict and clear application of the purpose limitation principle;
- a description of if and how factual data, opinion data, intelligence data and the data collected for different categories of data subjects are distinguished;
- further steps should include abstaining from using unreliable press reports and cross-checking information obtained from press reports against reliable independent sources.

3.6. Conservation of data / Data retention

As outlined in Section 2 of this Opinion, data are kept for three years, in accordance with the requirements of Article 90 of Regulation 1083/2006, and no further processing for statistical purposes is foreseen. Against this background, the EDPS has no reason to believe that personal data is kept in a form which permits identification of data of data subjects for longer than is necessary for which the data are collected and/or further processed in the sense of Article (4)(1)(e) of the Regulation. The EDPS would nonetheless recommend including a respective obligation for *VADIS SA/NV* to delete personal data after the end of the retention period in the written contract concluded.

3.7. Transfer of data

[9] See similar recommendations in the EDPS Opinion in case 2012-0326 on the European Investment Bank's AML-CFT data processing.

Transfers of data to recipients subject to the Regulation are governed by Article 7 of the Regulation; transfers to recipients subject to the national laws implementing Directive 95/46/EC are regulated by Article 8 of the Regulation.

- Article 7(1) establishes that data shall only be transferred within or between EU institutions and bodies if they are "*necessary for the legitimate performance of tasks covered by the competences of the recipient*". Article 7 transfers occur both within the COM and to other EU institutions or bodies. Internal transfers may happen to the extent necessary for reaching funding decisions and internal control functions. According to the notification, transfers to other EU institutions and bodies concerns transfers to OLAF and the European Court of Auditors. Where these transfers relate to the investigation of specific cases, they are in principle covered under Article 7(1) of the Regulation. A case-by-case analysis, however, has to be performed to evaluate whether the conditions for the transfer are actually fulfilled.

- Transfers to the Managing Authorities and their Intermediary Bodies in the Member States, their Certifying Authorities and the Audit Authorities are subject to Article 8 of the Regulation. Article 8(a) allows transfers of personal data to such recipients "*if the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority*". This provision covers transfers to such Member State authorities in the context of fraud detection and prevention in accordance with the Commission's Communication on the Anti-Fraud Strategy.

According to the notification, no transfers under Article 9 of the Regulation, e.g. to third countries, are foreseen.

3.8. Rights of access and rectification

Articles 13 and 14 of the Regulation establish that data subjects shall be able to access and rectify data stored about them at any time.
In the notification, the COM mentions that these rights might be limited in accordance with Article 20(1)(b) of the Regulation. The EDPS highlights that any restrictions on the rights of access and rectification must only be used on a case-by-case basis and only as long as *necessary* for this purpose. Appropriate procedures should be put in place to allow the exercise of these rights in these cases. In any case, Article 20(3) of the Regulation has to be respected by the COM: *"[i]f a restriction provided for by paragraph 1 is imposed, 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 right to have recourse to the European Data Protection Supervisor."*.

According to the Privacy Statement, "*Data subjects' right of access pursuant to art. 13, will be assessed case by case and delayed in case this could give potential fraudsters opportunities to find possible weaknesses in the risk assessment process and thus circumvent it. Access will then be given once a decision of not auditing is taken or at the time of the performance of the audit.*".

In the light of this explanation provided to data subjects, the EDPS takes note of the case-by-case approach and has no reason to believe that the COM applies restrictions on the rights of access and rectification for longer than necessary.

3.9. Information to the data subject

Where data is not collected from the data subject as in the case of the ARACHNE system, the information to be provided to data subjects must comprise at least the following (see Article 12 of the Regulation):

- Identity of the controller;
- Purposes of the processing operation;
- Recipients or categories of recipients;
- Categories of data collected;
- Existence of the rights to access and rectification;
- Legal basis for the processing;
- Retention periods;
- The right to have recourse to the EDPS;
- The origin of the data, except where the controller cannot divulge this for reasons of professional secrecy.

Concerning the means for providing this information, the EDPS considers that the publication of the Privacy Statement on the Europa Social Fund website does not in itself suffice to ensure that data subjects effectively receive the information. As a matter of fact, not all possible data subjects will read the information published on the website. The EDPS therefore considers that this publication must be complemented, to the extent possible, by some form of individual information containing the necessary information pursuant to Article 12 of the Regulation.

Where data is obtained from the ESF and ERDF managing authorities (through the SFC2007 infrastructure), it has been at least partially previously collected from the data subjects themselves. The EDPS therefore recommends providing the necessary information pursuant to Article 12 of the Regulation at that point.

3.10. Automated individual decisions

Article 19 of the Regulation provides that "*[t]he data subject shall have the right not to be subject to a decision which produces legal effects concerning him or her or significantly affects him or her and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him or her, such as his or her performance at work, reliability or conduct, unless the decision is expressly authorised pursuant to national or Community legislation or, if necessary, by the European Data Protection Supervisor. In either case, measures to safeguard the data subject's legitimate interests, such as arrangements allowing him or her to put his or her point of view, must be taken*".

According to the notification and as explicitly confirmed during the meeting on 9 January 2014, no automated decisions will be taken exclusively based on the risk indicators produced by ARACHNE, as the system does not automatically allow for the conclusion that something is wrong or irregular[10].

3.11. Security measures

[10] The notification further explicitly mentions that "*...the logic leading to the risk assessment outcome will not be revealed. This is not a restriction of art. 13, though, since decisions are only supported by the system and not automated by it*.".

(...)

4. CONCLUSION

There is no reason to believe that there is a breach of the provisions of Regulation (EC) 45/2001 providing the considerations contained in this Opinion are fully taken into account. In particular, the COM should:

- Consider adopting a more specific legal basis (a decision at the appropriate administrative level) authorising the COM to process data under Article 10(5) of the Regulation in application of the relevant provisions of Regulations 966/2012 and 1083/2006. The processing of special categories of data should in any case be limited to the extent necessary for complying with legal obligations regarding both Regulations. Appropriate safeguards to ensure necessity, proportionality and data quality should be set out in this respect;
- In the context of the "feedback loop", make reporting by ARACHNE users of identified error or inconsistency in the external data to *VADIS SA/NV* obligatory;
- Develop and implement effective measures to guarantee a high level of data quality regarding the information derived from external media sources in line with the recommendations made in Section 3.4 above;
- Ensure that transfers to OLAF and the European Court of Auditors under Article 7 of the Regulation take place following a case-by-case analysis;
- Include an obligation for *VADIS SA/NV* to delete personal data after the end of the retention period in the written contract concluded;
- For data obtained from the ESF and ERDF managing authorities (through the SFC2007 infrastructure), provide the necessary information on the processing operations under the ARACHNE system pursuant to Article 12 of the Regulation when the data is initially collected from the data subjects themselves;
- Review the user management processes to include a review of all user accounts used by the ARACHNE system and provide guidelines to the Member States to promote a consistent approach to user management.

Done at Brussels, 17 February 2014

(**signed**)

Giovanni BUTTARELLI