

(To be filled out in the EDPS' office)
REGISTER NUMBER: 977

(To be filled out in the EDPS' office)

NOTIFICATION FOR PRIOR CHECKING

DATE OF SUBMISSION: 17/05/2013

CASE NUMBER: 2013-0340

INSTITUTION: EUROPEAN COMMISSION

LEGAL BASIS: ARTICLE 27-5 OF THE REGULATION CE N° 45/2001⁽¹⁾

INFORMATION TO BE GIVEN²

1/ NAME AND ADDRESS OF THE CONTROLLER

CONTROLLER : MERCHAN CANTOS FRANCISCO

E-MAIL: francisco.merchan@ec.europa.eu

DELEGATE : SCHELFHOUT MARK

E-MAIL: mark.schelfhout@ec.europa.eu

2/ ORGANISATIONAL PARTS OF THE INSTITUTION OR BODY ENTRUSTED WITH THE PROCESSING OF PERSONAL DATA

THE EUROPEAN COMMISSION

DG EMPL - DIRECTORATE H

3/ NAME AND DESCRIPTION OF THE PROCESSING

NAME: Risk analysis for fraud prevention and detection in the management of ESF and ERDF

Directorate H of the Employment, Social Affairs and Inclusion DG and Directorate J of the Regional Development DG of the European Commission (EC) have the main responsibility of validating information (description of the Management and Control System, Audit Strategy, Annual Control Report/Annual Opinion, National Audit Reports, Annual Summaries) provided by the authorities covered by the European Social Fund (ESF) and European Regional Development Fund (ERDF), carrying out external audits within EU Member States, issuing timely reports and opinions,

¹ OJ L 8, 12.01.2001.

constantly updating a risk score table in order to allow a sound management of the Funds. Both DGs implement their policy through shared management, meaning that the Member States are still primarily responsible for the selection, verification and declaration of projects and project expenditure. Though, the Commission still has the final (financial) responsibility. Controller of this personal data processing is the Director of Directorate H of the Employment, Social Affairs and Inclusion DG.

Directorate J of the Regional Development DG is a co-controller for the personal data processed for the European Regional Development Fund.

The system ARACHNE aims at enriching a comprehensive and complete database of projects implemented under the Structural Funds in Europe with publicly available information in order to identify the most risky projects, based on a set of risk indicators. The system is based on the integration and customisation of an existing risk assessment tool, the GET application from Vadis company, 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. Currently GET is widely used in the bank sector, by the largest audit companies, by the private and public sector. 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 EC will be used to provide ARACHNE with this info.

The project data will be further elaborated and matched with public sources (*) within ARACHNE, which will calculate the risk indicators.

(*) The public sources will bring to the project information on companies and people involved/related. They are ORBIS (Bureau Van Dijk), World Compliance and Factiva.

Expenditure and beneficiary information is held by the Member States, who will need to identify them in order to allow a "case-by-case" analysis and determination of the possible risk criteria that enter into the tool.

The Commission services will have access to a dashboard indicating the evolution of risk on the overall ESF level but also on the single Operational Programme/Beneficiary level. Member States will receive access to the dashboard indicators pertaining to their individual programme(s), according to the responsibilities of the specific authority.

It is planned to update the information and to run risk scoring tests every quarter.

"Feedback loop" will be made available in order to ask rectification of public data. See section 12 for more details.

Operations start date is planned for Q2 2013.

Some processing operations performed by Arachne system are subject to prior checking by the EDPS, pursuant to paragraph 2, points a) of art. 27 of Reg.45/2001.

4/ PURPOSE OR PURPOSES OF THE PROCESSING, AND PROCESSORS

The purpose of this system, ARACHNE, is to respond to an increased demand for the creation of an adequate and accurate fraud prevention and detection strategy.

The need to implement such a system or instrument lies in the fact that Structural Fund assistance is implemented via the system of "shared management", meaning that the Member States are responsible for the implementation of the assistance but the Commission still has the final (financial)

responsibility. When considering that there are at present no adequate fraud/irregularity prevention systems, neither in the two competent DGs, nor in the Member States, resulting thus in high error rates for the expenditure, a system capable of managing fraud prevention and detection is dictated by a number of reasons:

- (1) Increased efficiency of Member States' and Commission verification;
- (2) Increased effectiveness of the controls and audits leading to a reduction of error rates (p.m. every reduction by 1% means economising 400Mio euro);
- (3) Identification of criticalities and risk management;
- (4) Audit resource management (staff/time/budget, to resolve conflicts and over allocations);
- (5) Better reporting;
- (6) Better monitoring of Operational Programmes.

The envisaged application will:

- Provide auditors and managers with up-to-date scientific information on risk and risk areas;
- Identify, assess and prioritize risks;
- View and update staff work and responsibilities within Audit Units;
- Integrate resource management, to allow proper placement of knowledge and expertise;
- Provide an additional important layer of assurance to the DG and to the Commission as a whole;
- Interoperate with office working tools (mail, office applications) and other applications, where necessary;
- Provide a dashboard showing detailed information on risk occurrence in the various programmes and projects, including a schematic overview of the evolution of risk per programme;

The main business opportunities can be summarised as follows:

- Harmonisation, standardisation and processing of structured project expenditure and beneficiary information;
- Complete access by auditors (and reviewers) to available information, anytime, anywhere; better risk management;
- Moving from ad hoc risk assessment to a risk assessment using CAAT's;
- Better identification of risk areas/programmes leading to an increase of effectiveness of audit resources;
- More accurate reporting for ESF and ERDF management;

No automated decisions will be taken upon the tool's outcome. The tool as such provides risk indicators but does not automatically reach the conclusion that something is wrong or irregular. It is up to the national authorities to look into these indicators and confirm or not the presence of an alleged irregularity and then plan possible audits to verify or to simply streamline the use of auditing resources for the mandatory activities provided by the regulations.

Fund granting will be assessed on objective criteria regulated by the applicable law and the system will not support this process.

PROCESSORS:

The contractor for this project is: ATOS Belgium NV/SA; Da Vincilaan 5 in 1930 Zaventem (Belgium). The sub-contractor is Vadis Consulting SA; Avenue de la Recherche 65 in 1070 Brussels (Belgium)

5/ DESCRIPTION OF THE CATEGORY OR CATEGORIES OF DATA SUBJECTS

The Data subjects are the beneficiaries, including their management and publicly known shareholders, receiving assistance from the ESF and/or the ERDF and possible other persons having relationships with them.

6/ DESCRIPTION OF THE DATA OR CATEGORIES OF DATA (*including, if applicable, special categories of data (Article 10) and/or origin of data*).

ARACHNE produces a series of pre-defined check categories to provide an objective view on the riskiness of projects and the related entities (i.e. beneficiaries, contracts, contractors/suppliers): procurement process, contract management, funding eligibility, company performance, funded projects concentration, basic logicity/reasonability of project data, reputational and fraud alerts. These risk checks result in risk indicators on projects.

The risk checks are performed processing, among other data categories, the following personal data.

1) From the ESF and ERDF managing authorities (through SFC2007):

- Beneficiaries: name, address, VAT number, role.
- Shareholders/management/key staff: name, function.
- Contractors: name, address, VAT number.
- Key experts for service contracts: name, date of birth

2) From the external public data sources:

a) From a commercial provider (Orbis database through VADIS ref.

<http://www.bvdinfo.com/Products/Company-Information/International/Orbis>):

- o Comprehensive information on companies (mainly as the info above)
- o Profiles of Politically Exposed Persons (PEP), as well as those of their family members and close associates. No political-party membership or other data prohibited by Art. 10 of the Regulation 45/2001 will be processed (eg 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)
- o Sanction list, which includes individuals and companies with the highest risk rating. Those lists are publicly available.
- o Enforcement List, including information received from regulatory and governmental authorities. It includes the content of warnings and actions against individuals and companies. Those lists are publicly available.
- o Monitoring of newspapers and magazines for risk relevant info

b) On-line media data of major newspapers in the EU member States

The contract and license agreement with ARACHNE provider ensures an adequate quality of public data sources used to produce ARACHNE database.

Personal data will be accessed on a need-to-know basis through a role-based approach. In detail

- each Member States will have access to enriched data related to beneficiaries only if they communicated the beneficiaries themselves to Vadis for processing
- the system grants access to users through the European Commission Authentication Service which asks and verifies the personal username and password

7/ INFORMATION TO BE GIVEN TO DATA SUBJECTS

Member States will proceed according to what provided for by Directive 95/46/EC. In the Europa Social Fund website a page will be dedicated to explain how risk management works and is performed, its legal basis and providing all the mandatory info as provided for by Reg.45/2001. Furthermore the page will contain the addresses of the national data protection authorities data subjects can address. Data subjects should refer in first instance to member state authority.

For the EC, 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. Furthermore, 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.

See attached Privacy statement for further details.

8/ PROCEDURES TO GRANT RIGHTS OF DATA SUBJECTS

Data subjects will contact the European Commission through the contact details provided in the Europa Social Fund (ESF) website page mentioned above. Fund managing authorities in the member states will make sure that the information provided to data subject at national level will also refer to the relevant Europa ESF web page.

The Member States are primarily responsible for the data provided by them. In case the data subject requests a change to his/her data, he/she should in first instance request the Member State authorities to implement these changes. Subsequently, the information will be processed (on a quarterly basis as described above) by the Commission and the changes will be taken into account in the risk scoring exercise. Anyhow, the Member State can immediately alter the risk score based on historical data in order to take direct account of the changes in data submitted by the data subject.

The data used for enrichment of the information received from the Member States is based on the annual accounts of beneficiaries. In case of data change requests, the data subject should submit changes to the organisations (national) responsible for the collection of annual accounts and similar. This information is updated by the external contractor on a monthly basis and the Commission's risk score will take this into account in the next risk score. Also here, the Member State can immediately alter the data in their dashboard and case management system.

Data subject could also contact the Member State Authorities in order to have their publicly available data to be rectified. A procedure called "Feedback loop" will be made available in order to ask rectification of public data:

- in case a user, i.e. the European Commission or a Member State, identifies an error or inconsistency (incorrect information on directorship, incorrect information on shareholder ship, incorrect information in press/media, incorrect name matches between data sources) in the external data, he/she can report this to Vadis through a "feedback loop"
- the users are required to provide sufficient supporting documentation to enable Vadis to review the reported error or inconsistency
- after review, and before resolving the reported error or inconsistency, Vadis will transfer the proposed modification to an authorized person at the European Commission for approval

The modifications introduced by the "feedback loop" will impact the system Arachne and its processing of personal data; not the source of information itself. Data subject should ask the source of the information in case he needs his rights granted further than the Arachne system.

Note: The EC can modify neither the data obtained from the external public data sources nor the data coming from the member states nor the calculated indicators.

9/ AUTOMATED / MANUAL PROCESSING OPERATION

Automated operations are performed by ARACHNE system.

Processing is based on:

- (a) The use of the SFC2007 Web Services interface to allow the Managing Authorities the transmission of the project related data (basically the content of Annex 3 of Regulation 1828/2006) and handling the Member State access for this particular purpose.
- (b) The customization of the Vadis GET (Group Exploration Tool) to perform a ratio, sanity, cross project checks at operational programme level. Average values/key indicators/figures for all projects within the same operational programme are calculated and utilized to identify projects with deviating ratios/exceptional key indicators/figures. Secondly, the results thus obtained are further enriched with external public data derived from info providers and the internet in order to identify financial, relationship, reputational, change, sanction and negative info alerts. The tool produces individual risk scoring sheets per project displaying alerts on the basis of risk scores or other key figures.

The ARACHNE data preparation process involves all data sources:

- operational information of projects gathered through SFC2007 (note that SFC2007 is not a source of information for Arachne but it is rather a communication channel) and provided by the member states
- and public source databases described in section 2.

It produces a series of pre-defined check categories providing an objective view on the riskiness of projects and the related entities (i.e. beneficiaries, contracts, contractors/suppliers).

Risk scoring indicators identifying possible irregularities need to be manually checked by the Managing Authorities and their Intermediate Bodies before drawing any conclusions and will not be used to take automatic decision. They are supplementary information that will be used to improve the overall risk management capability of the Member States and the Commission.

The data preparation process is carried out by the external contractor (Vadis). The resulting GET database is then provided to DIGIT (through a secure connection underpinned by a security convention with the EC), which hosts the GET application for the final users.

The high level data flow is described in the diagram attached.

10/ STORAGE MEDIA OF DATA

See schematic overview above (attachment at section 5). The final ARACHNE database, i.e. the enriched GET database, will be hosted at the DIGIT Data Centre. Some processing and storage will be hosted in the Vadis Data Centre.

- (i) Article 60 of Regulation 1083/2006 stipulating the obligations of the Managing Authorities;
- (ii) Article 61 of Regulation 1083/2006 stipulating the obligations of the Certifying Authorities;
- (iii) Article 62 of Regulation 1083/2006 stipulating the obligations of the Audit Authorities;
- (iv) Chapter IV, sections 1 and 2, of Regulation 1083/2006 stipulating the responsibilities of the Member States and of the Commission;
- (v) Article 69 of Regulation 1083/2006 on the information and publicity;
- (vi) Article 13 of Regulation 1828/2006 detailing the implementation rules for the Managing authority and controllers;
- (vii) Article 14 of Regulation 1828/2006 detailing the rules applicable to the accounting records of operations and data on implementation;
- (viii) Article 16 of Regulation 1828/2006 detailing the implementation rules for the Audits of operations;
- (ix) Article 19 of Regulation 1828/2006 describing the requirements on the availability of documents and data;
- (x) Article 37 of Regulation 1828/2006 describing the protection of personal data;
- (xi) Section 7 of Regulation 1828/2006 describing the electronic exchange of data;
- (xii) The Commission's communication on the Anti-Fraud Strategy OJ(2011)1965 – 22 June 2011, which states in chapter 2.2.3 " 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."
- (xiii) The Regulation (EU, EURATOM) No 966/2012 of the European Parliament and of the Council of 25 October 2012.

This processing is subject to be prior-checked by the EDPS as of article 27 of Regulation (EC) 45/2001.

This processing has to be evaluated against article 20.1 b) of Regulation (EC) 45/2001, in order to safeguard "an important economic or financial interest of a Member State or of the European Communities ...". More details in the Rights of Data Subject section.

Links to mentioned regulation:

1083/2006 - <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:210:0025:0025:EN:PDF>

1828/2006 - <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:371:0001:0001:EN:PDF>

45/2001 - <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:EN:PDF>

966/2012 - <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:298:0001:0096:EN:PDF>

12/ THE RECIPIENTS OR CATEGORIES OF RECIPIENT TO WHOM THE DATA MIGHT BE DISCLOSED

Recipients are ARACHNE users. Access to the tool is given to:

1) the Managing Authority and its Intermediary bodies in the Member States, their Certifying Authorities and the Audit Authorities.

Additional recipients are:

2) EC Directorate General for Employment, Social Affairs and Inclusion (limited to the auditors Unit);

3) EC Directorate General for Regional Policy (limited to the auditors Unit)

Further information recipients may be:

4) The European Court of Auditors (upon their request)

5) The OLAF (upon their request)

The Managing Authority and its intermediary bodies (MA/IB) will have read/write access, the rest will have limited access.

Personal data will be accessed on a need-to-know basis through a role-based approach. The system grants access to users through the Commission ECAS personal username and password.

13/ RETENTION POLICY OF (CATEGORIES OF) PERSONAL DATA

Data will be updated regularly, i.e. on a quarterly basis. For retention purposes, this data will be made available for three years following the closure of an operational programme and anyhow according to the requirements of Article 90 of Regulation 1083/2006.

1083/2006 - <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:210:0025:0025:EN:PDF>

13 A/ TIME LIMIT TO BLOCK/ERASE ON JUSTIFIED LEGITIMATE REQUEST FROM THE DATA SUBJECTS

One month.

14/ HISTORICAL, STATISTICAL OR SCIENTIFIC PURPOSES

If you store data for longer periods than mentioned above, please specify, if applicable, why the data must be kept under a form which permits identification.

N/A

15/ PROPOSED TRANSFERS OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

N/A

16/ THE PROCESSING OPERATION PRESENTS SPECIFIC RISK WHICH JUSTIFIES PRIOR CHECKING

Some processing operations performed by Arachne system as explained above are subject to prior checking by the EDPS, pursuant to art. 27, paragraph 2, (a), (b), and (c) of Reg.45/2001

Article 27.2.(a)

Processing of data relating to health and to suspected offences, offences, criminal convictions or security measures,

Article 27.2.(b)

Processing operations intended to evaluate personal aspects relating to the data subject,

Article 27.2.(c)

Processing operations allowing linkages not provided for pursuant to national or Community legislation between data processed for different purposes,

17/ COMMENTS

PLACE AND DATE: BRUXELLES, 17.05.2013

DATA PROTECTION OFFICER: FRIDA PACKER

INSTITUTION OR BODY: THE EUROPEAN COMMISSION

(To be filled out in the EDPS' office)

EDPS OPINION

OF DATE:

CASE NUMBER:

(To be filled out in the EDPS' office)

FOLLOW UP *(in case of acting measures to be taken)*