EUROPEAN ANTI-FRAUD OFFICE

Directorate C: Anti-Fraud Knowledge Centre

Director

Mr Jamie WABUNGO
Dijkstraat 2
9200 Termonde
Belgium

E-mail:

ask+request-8005-325b539e@asktheeu.org

ask+request-7946-e981da7b@asktheeu.org

Via e-mail

Brussels

Subject: **Your application for public access to documents, Ares(2020)3649457, Ares(2020)3550065**

Dear Mr Wabungo,

We refer to your message of 4 June 2020 addressed to DG DIGIT via AsktheEU website, Ares(2020)3649457 – 10/07/2020, by which you made an application for public access to documents under Regulation (EC) No 1049/2001[1] and to your request of 19 June 2020 addressed to DG DIGIT alike, Ares(2020)3550065 – 6/07/2020. OLAF was asked to reply to your requests.

1. Scope of your application

By your message of 4 June 2020, you requested all contracts for the development of OCM as well as the tender specifications with each subcontractor or contractors and the relevant tendering documents, including reasoning why they were selected and who were its competitors, if there were any.

By your message of 19 June 2020 you asked for exact amounts of forecasted expenses related to OCM planned for future years. You claimed that OCM would not be fully operational 4 years after its handover and you asked whether there were any financial penalties imposed on the contractors because of this reason.

2. Preliminary remarks

[1] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ L145, 31.05.2001, page 43.

With regard to your question on exact amounts of forecasted expenses related to OCM planned for future years, please be informed that OCM is a project delivered in different phases. Its first operational release dates back to October 2016. Since then many other releases have been implemented depending on the evolving project planning and business needs. OCM as a project will end in February 2021 and will then enter an evolutive maintenance mode. For the latter period, we are currently in the process of collecting and analysing the users' needs before we conclude on the exact cost by December 2020.

As regards your query on financial penalties imposed on the contractors, we wish to clarify that OCM has not been contracted out to an external company for development within a specific timeframe. OCM is managed and operated by external providers working on OLAF's premises under the supervision of OLAF staff. This was necessary due to special security provisions and to allow flexibility in development. As such, there are no financial penalties to impose on any contractor.

With reference to your request for contracts for the development of OCM as well as the tender specifications with each subcontractor or contractors and the relevant tendering documents, including reasoning why they were selected and who were its competitors, OLAF regrets to inform you that your application cannot be granted, as the disclosure is prevented by several exceptions to the right of public access to documents, laid down in Article 4 of Regulation 1049/2001.

3. Assessment of the documents and relevant applicable exceptions

a) Protection of the purpose of investigations (Article 4(2) third indent)

Article 4(2), third indent of Regulation 1049/2001 stipulates that the institutions shall refuse access to a document where disclosure would undermine the protection of the purpose of inspections, investigations and audits, unless there is an overriding public interest in disclosure.

The OCM system is designed and used for the operational activity of OLAF. OLAF is legally bound, pursuant to Article 339 of the Treaty on the Functioning of the European Union, Article 10 of Regulation (EU, Euratom) No 883/2013, and Article 17 of the Staff Regulations, to treat the information it obtains during an investigation as confidential and subject to professional secrecy. OLAF case files contain sensitive information, including but not limited to personal data, the unwarranted divulgation of which could seriously impact the reputation of individuals as well as economic operators.

Those parts of the deployment policy for the OCM which fall in the scope of the present request pursue the aim to support OLAF's commitment to the confidential treatment of the information in its case files and to implement the need-to-know principle for OLAF's case-related information. This ensures that only authorised staff has access to the information needed to fulfil their tasks and for as long as necessary. This policy helps also protect the system against external threats. Public disclosure of specific information on the deployment process and the access control policy for OCM might weaken or undermine the protection of OLAF investigation files.

b) Protection of the public interest as regards public security (Article 4(1)(a))

The disclosure of the documents at issue is also prevented by the exception of Article 4(1)(a), first indent of Regulation 1049/2001, which provides for the protection of the public interest as regards public security. The documents contain information on the deployment process of OCM and on the application. This information, if disclosed, would undermine the protection of public security as it would put in the public domain detailed knowledge about the internal case management system of OLAF.

c) Protection of commercial interests (Article 4(2) first indent)

Article 4(2) first indent of Regulation 1049/2001 provides that the institutions shall refuse access to a document where disclosure would undermine the protection of commercial interests of a natural or legal person, including intellectual property.

Specific contracts used by OLAF for OCM contain personal and commercial data on contractors' staff and prices. The disclosure of the requested documents would allow the public to gather important information of business relevance, which would be harmful for the entities that have delivered their data. Additionally, such divulgation may discourage commercial entities from collaboration with OLAF in the future.

The General Court found that documents, whose disclosure would seriously undermine the commercial interests of a legal person, 'contain commercially sensitive information relating, in particular, to the business strategies of the undertakings concerned or their commercial relations or where those documents contain information particular to that undertaking which reveal its expertise.'[2]

For these reasons, there is a real risk that public access to the above-mentioned information would negatively affect the commercial activities of the companies concerned and thus seriously undermine their commercial interests. Therefore, public access to the requested documents would undermine the protection of commercial interests of the persons and companies involved.

d) Protection of personal data (Article 4(1)(b))

The requested documents contain personal data that are subject to protection under EU law. Article 4(1)(b) of Regulation 1049/2001 provides that the EU institutions shall refuse access to a document where disclosure would undermine the protection of privacy and the integrity of the individual, which provision must be implemented in accordance with the relevant EU law on the protection of personal data.[3]

According to the definition provided for in Article 3(1) of Regulation 2018/1725[4], personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Therefore, public disclosure of the above-mentioned personal data, through the release of the requested documents containing them, would constitute processing (transfer) of personal data within the meaning of Article 3(3) of Regulation 2018/1725.

---

[2] Judgments of the General Court of 5 February 2018 in Case T-718/15 *PTC Therapeutics Ltd v. European Medicines Agency*, EU:T:2018:66, paragraphs 84-85 and in Case T-729/15 *MSD Animal Health Innovation GmbH v European Medicines Agency*, EU:T:2018:67, paragraphs 67– 68.

[3] Judgment of the General Court of 25 September 2018, *Psara et al. v European Parliament*, Joined Cases T-639/15 to T-666/15 and T-94/16, EU:T:2018:602, paragraph 44.

[4] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L295, 21.11.2018, page 39.

In its judgment in case C-28/08 P, *Bavarian Lager*[5], the Court of Justice ruled that, when a request is made for access to documents containing personal data, Regulation 45/2001 (now replaced by Regulation 2018/1725 referred to above) becomes fully applicable.

Article 9(1)(b) of Regulation 2018/1725 provides that personal data shall only be transmitted to recipients established in the Union other than Union institutions and bodies if the recipient establishes that it is necessary to have the data transmitted for a specific purpose in the public interest and the controller, where there is any reason to assume that the data subject's legitimate interests might be prejudiced, establishes that it is proportionate to transmit the personal data for that specific purpose after having demonstrably weighed the various competing interests. The processing (transfer) of personal data can occur only if the conditions set out under Article 9(1)(b) of Regulation 2018/1725 are fulfilled and if the transfer constitutes lawful processing in accordance with the requirements of Article 5 of that Regulation.

In that context, whoever requests such a transfer must first establish that it is necessary for a specific purpose in the public interest. If it is demonstrated to be necessary, it is then for the institution concerned to determine that there is no reason to assume that that transfer might prejudice the legitimate interests of the data subject[6]. Where there is any reason to assume that the data subject's legitimate interests might be prejudiced, the controller of personal data (i.e. the institution concerned) then establishes whether it is proportionate to transmit the personal data for that specific purpose, after having demonstrably weighed the various competing interests.[7]

Moreover, the Court of Justice clarified that the institution does not have to examine itself whether a need for the transfer of personal data exist.[8] In order to justify the transfer of personal data, the applicant must demonstrate that such transfer is necessary for the performance of a task carried out in the public interest. A mere *interest* of members of the public in obtaining certain personal data cannot be equated with a *necessity* to obtain the said data in the meaning of Regulation 45/2001.[9] Furthermore, if the condition of necessity laid down in Article 8(b) of Regulation 45/2001, which is to be interpreted strictly, is to be fulfilled, it must be established that the transfer of personal data is the most appropriate means for attaining the applicant's objective, and that it is proportionate to that objective.[10]

It should also be recalled that no automatic priority can be conferred on the objective of transparency over the right to protection of personal data.[11] Nonetheless, even if the necessity of transfer was established (which is not the case), there are reasons to assume that the data subjects' legitimate interests might be prejudiced by such disclosure.

4. Overriding public interest in disclosure

The exceptions laid down in Article 4(2) and 4(3) of Regulation 1049/2001 apply unless there is an overriding public interest in disclosure of the documents. For such an interest to exist, it, firstly, has to be a public interest and, secondly, it has to outweigh the interest protected by the exception to the right of access.

---

[5] Judgment of the Court of Justice of 29 June 2010, *European Commission v The Bavarian Lager Co. Ltd*, C-28/08 P, EU:C:2010:378, paragraph 59.
[6] Ibidem.
[7] Judgment of the Court of 16 July 2015, *ClientEarth and PAN Europe* v *EFSA*, C-615/13 P, paragraph 47.
[8] Judgment of the Court of Justice of 2 October 2014, *Strack v Commission*, C-127/13 P, EU:C:2014:2250, paragraph 106.
[9] Ibidem, paragraphs 107 and 108.
[10] Judgment of the General Court of 15 July 2015, *Dennekamp v European Parliament*, T-115/13, EU:T:2015:497, paragraph 77.
[11] Ibidem, paragraph 91.

OLAF has not identified an overriding public interest that would allow it not to apply the exceptions.

In addition, the requested documents also involve the protection of privacy and integrity of individuals (Article 4(1)(b) of Regulation 1049/2001) where overriding public interest in disclosure is not applicable.

Article 4(1)(a) of Regulation 1049/2001 equally does not include the possibility for the exceptions defined therein to be set aside by an overriding public interest.

5. Confirmatory application

In accordance with Article 7(2) of Regulation 1049/2001, you are entitled to make a confirmatory application requesting OLAF to review this position. Pursuant to Article 4 of Commission Decision 2001/937/EC, ECSC, Euratom, such a confirmatory application should be addressed within 15 working days upon receipt of this letter to the Director General of OLAF.

Any confirmatory application to OLAF should be sent to the following address:

Mr Ville ITÄLÄ
Director General OLAF
European Commission
B-1049 BRUXELLES
BELGIUM

Your attention is drawn to the privacy notice below.

Yours sincerely,

Beatriz SANZ REDRADO

Privacy notice

Pursuant to Articles 15 and 16 of Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by Union Institutions, bodies, offices and agencies and of the free movement of such data, please be informed that your personal data are stored in OLAF's electronic and paper files concerning this matter for the purposes of ensuring conformity with the requirements of Regulation 1049/2001 and Commission Decision 2001/937/EC.

The categories of your personal data being processed are identification and contact data and any other personal data provided by or to you in relation to your request. Officials within OLAF and other Commission services responsible for dealing with requests for access to documents, and third parties, within the meaning of Articles 4(4) and 3(b) of Regulation 1049/2001, and Article 5 of Commission Decision 2001/937/EC, have access to your personal data. Personal data that appear on the requested document may only be disclosed to the applicant

following an assessment under Article 9(b) of Regulation (EU) 2018/1725. There is no automated decision process by OLAF concerning any data subject.

All documentation concerning OLAF investigations are stored in the relevant OLAF investigation files and are retained for a maximum of 15 years. Thus personal data contained in requests for public access to documents concerning OLAF investigations are retained for a maximum of 15 years.

You have the right to request access to your personal data, rectification or erasure of the data, or restriction of their processing. Any request to exercise one of those rights should be directed to the Controller (OLAF-FMB-DATA-PROTECTION@ec.europa.eu). You may contact the Data Protection Officer of OLAF (OLAF-FMB-DPO@ec.europa.eu) with regard to issues related to the processing of your personal data under Regulation (EU) 2018/1725.

You have the right to have recourse to the European Data Protection Supervisor (edps@edps.europa.eu) if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by OLAF.

The complete privacy statements for this and all other OLAF personal data processing operations are available at http://ec.europa.eu/anti_fraud.