



ANTI-FRAUD ADVICE

for the purchase of IT hardware and software under EU funded projects

OLAF Anti-fraud Knowledge Centre

July 2022

OLAF fights against fraud, corruption and any other illegal activity affecting the financial interests of the EU. Besides carrying out investigations, OLAF develops knowledge to inform sound anti-fraud policies, both at the EU and Member States level. This knowledge is the result of the analysis of information from various sources.

The Anti-fraud Knowledge Centre of OLAF has prepared this document, based on OLAF's investigative experience. This paper's purpose is to provide advice to competent national authorities for reducing the risk of irregularities, including fraud.

DISCLAIMER: This document is intended to feed into fraud prevention activities of the competent national authorities in the Member States. It does not represent an official position of the Commission.

INTRODUCTION

Digitalisation is one of Europe's key priorities. The European Structural and Investment Funds made available approximately EUR 21.4 billion for information and communication technology investments over the 2014-2020 funding period. Moreover, the Multiannual Financial Framework 2021-2027 is supporting digitalisation through a variety of funding instrument.

Under the Recovery and Resilience Facility (RRF), the key instrument at the heart of NextGenerationEU, national plans have to contain "*measures that effectively contribute to the digital transition or to addressing the challenges resulting therefrom, and that account for an amount which represents at least 20 %*"¹ of the plans' total allocation. In March 2022, expenditure committed to foster digital transition represented 26% of the already approved national plans.

In carrying out its mission to protect the EU's financial interests by investigating fraud, corruption and any other illegal activities, the European Anti-Fraud Office (OLAF) has investigated a number of cases related to digital transition investments in projects financed by the European Structural and Investment Funds. These cases reveal important shortcomings and weaknesses in the projects' implementation, management or control. These concern in particular:

- large projects involving a single purchase – in particular under framework agreements - of a high number of IT hardware equipment and/or IT software licenses and services, implemented by national public authorities (as beneficiaries of the EU funded project);
- several small IT innovative projects where a group of companies artificially created the conditions to unduly obtain EU funds, in particular by alternating as projects' beneficiaries and suppliers (to the projects' beneficiaries), and by presenting several times the same or very similar IT software as innovative products.

Based on the experience of these cases, OLAF has analysed the underlying problems, and identified related risks in order to formulate anti-fraud advice.

The present document describes the three main problem areas identified, for each of them providing a list of related red flags and suggestions for possible mitigating measures. A case study illustrates the problems encountered.

¹ Art. 19 of Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility, OJ L 57, 18.2.2021, p. 41.

Problem area 1: Use of inadequate framework agreements for the purchase of IT hardware equipment and software licenses and services in EU funded projects

Problem description:

- Public/contracting authorities (beneficiaries of EU funded projects) frequently use (or are obliged to use) framework agreements (with re-opening of competition) to purchase a large number of IT hardware equipment and software licenses and services. In some specific situations, those framework agreements might not be adequate.
- When different types of contracting authorities use the same framework agreement, best value for money might not be guaranteed as the prices under the agreement might not include any specific preferential price potentially applicable (e.g. for large quantities procured, for a specific category of public entity).
- When framework agreements are used, transparency is reduced as all flows of information stay between the contracting authority and the economic operators signatories to the agreement.
- Competition is reduced as framework agreements limit the number of potential bidders at the re-opening of competition. Hence, companies that signed a framework contract could more easily share out the (national) market.

Red flags:

- Mandatory use of framework agreements.
- A given contracting authority always has the same supplier.
- Single bid at the reopening of competition.
- Although several bids are submitted, unusual bid patterns can be observed (e.g. the bids' prices are an exact percentage apart; the winning bid is just under the threshold of acceptable prices, exactly at budget price, too high, too close, too far apart, round numbers, incomplete, etc.).
- Certain companies part of a framework agreement always bid against each other at the reopening of the competition, while others never do.
- Combining purchase of software and training/software support in the same public procurement.
- Pre-order of hardware or software from the producer before the award of contract.
- Transfer of software licenses from the producer to the end user ("preloading") before the award of contract.

Mitigating measures/solutions:

- Assessing the need and adequateness of framework agreements compared to other ways of procuring, e.g. through open procedures.
- Use of mandatory framework agreements only for groups of entities that fall under the same type of price categories.
- Ensure independent expert advice at public authority/beneficiary level to assess the needs and costs for IT projects.
- Use of different IT consultants for
 - preparing the project application
 - preparing the tender documents
 - supporting the tender evaluation and
 - the project's implementation.

Problem area 2: Lack of transparency of prices and sub-contracting chain

Problem description:

- The beneficiary/contracting authority does not know what potential special prices it is entitled to receive and whether/what extra discount was obtained by the supplier from the producer.
- The beneficiary might not be aware of the full sub-contracting chain.
- Corruption might appear because of the opacity of prices and sub-contracting chain for the final user/the contracting authority.

Red flags:

- Complex chain of sub-suppliers.
- Chain of sub-suppliers crossing borders.
- The chain of sub-suppliers include sub-suppliers, which have no experience and/or operational capacity in the given sector.

Mitigating measures/solutions:

- Including in the contract with the supplier a transparency clause, covering in particular any special price and extra discount agreed by the producer to the supplier compared to the price list of the (framework) contract.
- Including a contractual obligation for the supplier to declare to the contracting authority any sub-supplier in the chain between the supplier and the producer.
- Forbidding the transfer of software licenses from the producer to the end user prior to the award of contract.
- Forbidding any agreement or order between the contracting authority and the producer/reseller concerning the future contract before the award of the contract.
- When possible, contracting directly with the producer or its official re-seller. When not possible, contacting directly the producer to ask/negotiate for conditions for categories of buyers and special discounts (implement routine anti-fraud enquiry).

Problem area 3: Lack of technical expertise of government bodies and public entities in the implementation/control of digital transition investments

Problem description:

The lack of technical expertise at the level of government bodies and public entities can be a problem:

- when the government body/public entity is the contracting authority,
- when the government body/public entity is in charge of the management and control of the investment projects.

Red flags:

- Involvement of the producer in the definition of the subject of procurement or its technical specifications (this can occur at early stage, for example during the preparation of the EU project application).
- Controls by the government body/public entity in charge of the management and control are limited to formal aspects and do not include the content of the projects

Mitigating measures/solutions:

- Ensure that independent expertise is available at government/public authorities' services level to avoid the involvement of the IT software/hardware producer in assessing the needs for the purchase of given licenses or in choosing one or the other producer.
- For the contracting authority: for big projects, engage an IT expert company to prepare the project application and the tender specifications and a different company for the tender evaluation and project implementation.
- For the contracting authority: for big projects, engage an IT expert company to help with project preparation, if possible from another Member State.
- For the managing and control authority: if a given RRF measure includes a significant number of small IT innovative projects implemented by private companies, conduct sample-based controls and compare the project applications and project implementation reports to spot similarities, for example by using anti-plagiarism software.
- For the managing and control authority: if a given RRF measure includes a significant number of small IT innovative projects, the managing and control authority should identify when members of the same group of companies are alternating as beneficiaries and suppliers/sub-suppliers of the projects. The verification can be based on the data collected on final recipients, contractors, sub-contractors and beneficial owners in line with the obligation set out in the RRF Regulation².

The present document is designed to help public administrations in Member States assess the appropriateness of framework agreements, increase transparency when procuring, improve technical verifications carried out in addition to administrative checks and, thus, enhance the benefits of EU funds.

Member States are encouraged to take into consideration the anti-fraud elements included in this document in particular in the context of the implementation of the national plans under the RRF. However, as this document is the result of OLAF's investigative experience in the area of European Structural and Investment Funds, the national authorities responsible of the implementation, management and control of those funds in the current programming period could also benefit of the advice therein.

This document is part of OLAF's fraud prevention activities in relation to the Member States.

² Art. 22 of Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility, OJ L 57, 18.2.2021, p. 41.

CASE STUDY

OLAF opened an investigation into possible irregularities and fraud in the supply of IT software licenses in two projects implemented by a beneficiary consortium (government bodies/public entities) in a given Member State. The projects were 100% financed by the European Regional and Development Fund.

The **initial scope** of the projects was the development of a complex intelligent road control system. However, the Managing Authority (MA) and the beneficiary consortium signed **amendments** to the projects' grant agreements in order to add the purchase of IT software licenses into the scope of the projects and increase the projects' amount in accordance with the estimated public procurement value.

Prior to the signature of the amendments, the MA (respectively the intermediate body) had asked the beneficiary consortium to justify why it intended to purchase a specific IT software from a certain producer and not software developed by other companies or adapt open source software. The intermediate body had also asked how the price calculation was done.

The public entities concerned should make sure having or acquiring the necessary technical expertise to guarantee the validity of justifications and price estimations.

The local subsidiary and the future winning supplier ALPHA³ assisted the beneficiary consortium in drafting the justifications for the extension of project's scope and in the definition and the preparation of the price quotation for the project amendments.

There could be an underlying conflict of interest in the relation supplier – beneficiary. The prior involvement of a tenderer in the activity of the contracting authority is irregular.

The **IT software licenses** subject to the projects' amendments are sold through a two-level structure involving the producer's regional/local subsidiary and the national authorised local resellers. Purchasing government services in the Member State in question can benefit from a special volume-licensing program involving **different discounts**.

The beneficiary consortium launched a centralised procurement procedure based on a **framework agreement** with re-opening of competition (the use of which was mandatory). All five company-consortia signatories to the framework agreement were invited to bid. The winner was company ALPHA (one of the local resellers), who had provided the **only bid** during the second round procedure. The price offered by ALPHA included a relatively small **price discount** compared to the list of prices of the framework agreement but did not take into account the large price "one-time deal" discount the company had obtained from the producer thanks to the involvement of various sub-suppliers.

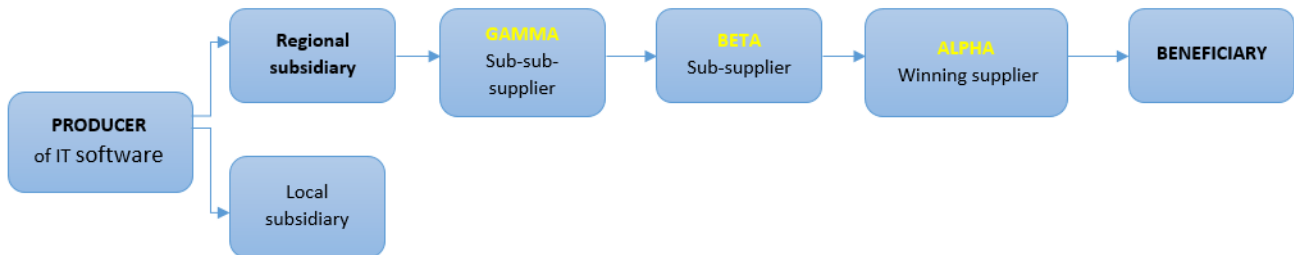
The (mandatory) use of framework agreements might not be appropriate: lack of transparency of prices/price discounts; risks of "bad deals"; reduced competition.

³ The company names used in this case study are fictitious.

Once the public procurement was finalised, the company BETA (another local reseller), which had also been invited to bid and had not submitted an offer, sold the software licenses it held to its “competitor”, ALPHA.

This situation could imply bid rigging.

The OLAF investigation disclosed the following scenario of **companies’ involvement** in relation to the public procurement procedure.



The local subsidiary obtained a high extra price “one-time deal” discount from the producer (through the regional subsidiary) for the future public procurement. However, the regional subsidiary sold the licenses not to the winning supplier but to GAMMA, a sub-sub-supplier located in another Member State, which sold it to a sub-supplier BETA. High profit margins were created at the various levels and the extra-discount never reached the beneficiary. The beneficiary was not aware of the complex sub-contracting chain and the extra discount approved by the producer.

Long/complex sub-contracting chains increase the risk of wrongdoings occurring. Transparency could prevent a situation in which any extra discounts are not being passed on to the end user.