

# Combating fraud in Cross-border Cooperation Programme Poland-Belarus-Ukraine 2014-2020

Manual

Warsaw, April 2018

## Table of contents

|  |    |
|--|----|
| 1. Legal basis.....  | 3  |
| 2. Glossary of terms and abbreviations.....  | 4  |
| 3. Scope and purpose of the Manual .....   | 6  |
| 4. Anti-fraud cycle .....  | 7  |
| 4.1. Prevention .....  | 7  |
| 4.1.1. Ethical culture.....  | 8  |
| 4.1.2. Policy, responsibilities, training, reporting mechanisms.....                       | 9  |
| 4.1.3. Internal control system .....   | 11 |
| 4.1.4. Fraud risks analysis.....   | 13 |
| 4.1.5. Preventing conflict of interests .....  | 15 |
| 5. Fraud detection .....   | 18 |
| 5.1. Control system.....   | 18 |
| 5.2. Control system supporting mechanisms .....  | 19 |
| 5.3. Analysis of available data .....  | 20 |
| 6. Correction.....   | 21 |
| 7. Prosecution.....  | 22 |
| 7.1. Sources of information on fraud .....   | 22 |
| 7.2. Procedure in the case of information on fraud suspicion from particular sources ..... | 23 |
| 7.2.1. Information from employees .....  | 23 |
| 7.2.2. Information from law enforcement bodies.....  | 24 |
| 7.2.3. Information obtained from other sources .....                                       | 24 |

## **1. Legal basis**

The regulations in this Manual result in particular from EU and national legislation, *inter alia* from:

1. Treaty on the Functioning of the European Union (Chapter 6: Combatting Fraud), OJ C 83, 30.03.2010 (Article 325);
2. Regulation (EU) no. 232/2014 of the European Parliament and of the Council of 11 March 2014 establishing a European Neighbourhood Instrument (OJ L 77, 15.3.2014, p. 27-43);
3. Regulation (EU) no. 236/2014 of the European Parliament and of the Council of 11 March 2014 laying down common rules and procedures for the implementation of the Union's instruments for financing external action (OJ L 77, 15.3.2014, p. 95-108);
4. Commission Implementing Regulation (EU) no. 897/2014 of 18 August 2014 laying down specific provisions for the implementation of cross-border cooperation programmes financed under Regulation (EU) no. 232/2014 of the European Parliament and the Council establishing a European Neighbourhood Instrument (OJ L 244, 19.8.2014, p. 12-54), hereinafter referred to as Implementing Regulation;
5. Regulation (EU, Euratom) 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 and repealing Council Regulation (EC, Euratom) No 1605/2002 (OJ L 298, 26.10.2012, p. 1, as amended), hereinafter referred to as the Financial Regulation;
6. Commission Delegated Regulation (EU) No 1268/2012 of 29 October 2012 on the rules of application of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council on the financial rules applicable to the general budget of the Union;
7. Council Regulation (EC, Euratom) No 2988/95 of 18 December 1995 on the protection of the European Communities financial interests (OJ L 312, 23.12.1995, p. 1);
8. Convention on the Protection of the European Communities' Financial Interests done at Brussels on 26 July 1995 (Journal of Laws of 2009, No 208, item 1603);
9. Regulation (EC) No 1073/1999 of the European Parliament and of the Council of 25 May 1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF) (OJ L 136, 31.5.1999);
10. Council Regulation (Euratom) No 1074/1999 of 25 May 1999 concerning investigations conducted by the European Anti-Fraud Office (OCAF) (OJ L 136, 31.5.1999);
11. Council Regulation (Euratom, EC) No 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and other irregularities (OJ L 292, 15.11.1996);
12. Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, p. 65), hereinafter referred to as the Public Procurement Directive;

13. European Commission's Guidance for Member States and Programme Authorities: Fraud Risk Assessment and Effective and Proportionate Anti-Fraud Measures of 16 June 2014 (EGESIF\_14-021-00-16/06/2014), hereinafter referred to as EC Guidance;
14. Guidelines for national anti-fraud strategies for European Structural and Investment Funds (ESIF);
15. Identifying conflicts of interests in public procurement procedures for structural actions. A practical guide for managers elaborated by a group of Member States' experts coordinated by OLAF's unit D2 – Fraud Prevention (the document was endorsed by the COCOLAF Fraud Prevention Group on 12 November 2013);
16. Detection of forged documents in the field of structural actions. A practical guide for managing authorities elaborated by a group of Member States' experts coordinated by OLAF's unit D2 – Fraud Prevention (the document was endorsed by the COCOLAF Fraud Prevention Group on 12 November 2013);
17. National anti-corruption policy regulations.

## ***2. Glossary of terms and abbreviations***

The abbreviations used in this Manual have the following meaning:

1. **Beneficiary** – for the needs of the Manual, this term covers both lead beneficiaries and project partners;
2. **TCD** – Territorial Cooperation Department at the Ministry of Economic Development of the Republic of Poland;
3. **AA** – the Audit Authority referred to in Article 28 of the Implementing Regulation, whose function in the Programme is performed by the Department for Protection of EU Financial Interests at the Ministry of Finance of the Republic of Poland;
4. **NA** – National Authority of the Programme;
5. **MA** – Managing Authority of the Programme whose function is performed by the TCD;
6. **EC** – European Commission;
7. **Independent auditor** – the auditor referred to in Article 32 of the Implementing Regulation;
8. **OLAF** – European Anti-Fraud Office;
9. **Programme** – Cross-border Cooperation Programme Poland-Belarus-Ukraine 2014-2020;
10. **ICT system** – the system referred to in Article 26(2)(d) of the Implementing Regulation;
11. **JTS** – the Joint Technical Secretariat referred to in Article 27) of the Implementing Regulation;
12. **CCPs – the Control** Contact Points referred to in Article 20(6)(b);

The terms used in this Manual have the following meaning:

1. **Irregularity** – pursuant to Article 2(m) of the Implementing Regulation, “any infringement of a financing agreement, a contract or of applicable law resulting from an act or omission by an economic operator involved in the implementation of the programme, which has, or would have,

the effect of prejudicing the budget of the Union by charging an unjustified item of expenditure to the budget of the Union”;

2. **Fraud** – pursuant to Article 1 of the Convention on the Protection of the European Communities’ Financial Interests:

(a) in respect of expenditure, any intentional act or omission relating to:

- i. the use or presentation of false, incorrect or incomplete statements or documents, which has as its effect the misappropriation or wrongful retention of funds from the general budget of the European Communities or budgets managed by, or on behalf of, the European Communities,
- ii. non-disclosure of information in violation of a specific obligation, with the same effect,
- iii. the misapplication of such funds for purposes other than those for which they were originally granted;

(b) in respect of revenue, any intentional act or omission relating to:

- i. the use or presentation of false, incorrect or incomplete statements or documents, which has as its effect the illegal diminution of the resources of the general budget of the European Communities or budgets managed by, or on behalf of, the European Communities,
- ii. non-disclosure of information in violation of a specific obligation, with the same effect,
- iii. misapplication of a legally obtained benefit, with the same effect.

3. **Collusive bidding** – an arrangement whose objective or effect lies in elimination, restriction, or breach of competition on a relevant market in any other way;

4. **Conflict of interests** – pursuant to Article 57(2) of the Financial Regulation, “a conflict of interests exists where the impartial and objective exercise of the functions of a financial actor or other person (...) is compromised for reasons involving family, emotional life, political or national affinity, economic interest or any other shared interest with a recipient.” In addition, pursuant to Article 24 of the Public Procurement Directive, the concept of conflicts of interest shall at least cover any situation where staff members of the contracting authority or of a procurement service provider acting on behalf of the contracting authority who are involved in the conduct of the procurement procedure or may influence the outcome of that procedure have, directly or indirectly, a financial, economic or other personal interest which might be perceived to compromise their impartiality and independence in the context of the procurement procedure.

5. **Corruption** – as there is no single definition of corruption in EU regulations, for the needs of this Manual the definition from the EC Guidance was adopted:

A broad definition of corruption used by the Commission is the abuse of (public) position for private gain. Corrupt payments facilitate many other types of fraud, such as false invoicing, phantom expenditure or failure to meet contract specifications. The most common form of corruption is corrupt payments or other advantages; a receiver (passive corruption) accepts a bribe from a giver (active corruption) in exchange for a favour.

6. **Document forgery** – consists in counterfeiting, altering or use of a forged document or official attestation of untruth as to a circumstance of legal significance by a public official or other person authorised to issue a document.
7. **Law enforcement authorities** – bodies sanctioned by national governments to enforce laws acting in accordance with detecting or investigation procedures and apprehend those who break them. Law enforcement authorities in Poland are:
  - Prosecutor's Office
  - Police
  - Military Police
  - Central Anticorruption Bureau
  - Internal Security Agency
  - Border Guard
  - National Revenue Administration.

### ***3. Scope and purpose of the Manual***

Pursuant to Article 26(5)(c) of the Implementing Regulation, MA shall put in place effective and proportionate anti-fraud measures taking into account the risks identified. In addition, Article 30(1)(g) of the Implementing Regulation stipulates that the management and control systems shall provide for prevention, detection and correction of irregularities, including fraud, and the recovery of amounts unduly paid, together with any interest. In the light of the above, this Manual presents tips and recommendations as to actions to prevent, identify, and respond to suspicions of fraud in Programme and project implementation. The four most common types of fraud that affect absorption of EU funds to the greatest extent are: collusive bidding, conflict of interests, corruption, and document forgery. This is not an exhaustive list of fraud types as new practices and offences may emerge that fit the definition of a fraud.

This Manual is addressed at all institutions involved in Programme and project implementation, i.e. MA, other bodies responsible for establishing first level control system, JTS, CCPs and beneficiary institutions. The presented tips and recommendations do not impose new obligations on the institutions, they only highlight common tasks resulting from the law that must be performed by all national institutions. Without prejudice to this Manual, institutions may draft more detailed documents concerning risk analysis and assessment as well as corruption threat monitoring in the ENI project implementation process. Existing solutions can be supplemented with appointment of internal teams responsible for effective corruption risk management.

The main idea behind the Manual is to communicate that **no types of fraud will be tolerated** within and outside the implementation system. Therefore, particular emphasis is placed on the first part of the Manual that concerns fraud prevention, including creation of an adequate culture of ethics in institutions and operation of the internal control system. Subsequent parts of the Manual are devoted to fraud detection, correction, and prosecution.

This Manual is available at Programme websites and is valid throughout the Programme implementation period.

## 4. Anti-fraud cycle

EC Guidance recommends implementation of actions that serve fraud prevention that comply with the **anti-fraud cycle**. There are four key elements in the anti-fraud cycle: prevention, detection, correction and prosecution. Proportionate implementation of all the above elements could significantly reduce the fraud risk as well as provide adequate deterrence against fraud.

Fig. 1. Anti-fraud cycle.



Source: Own study on the basis of EC Guidance.

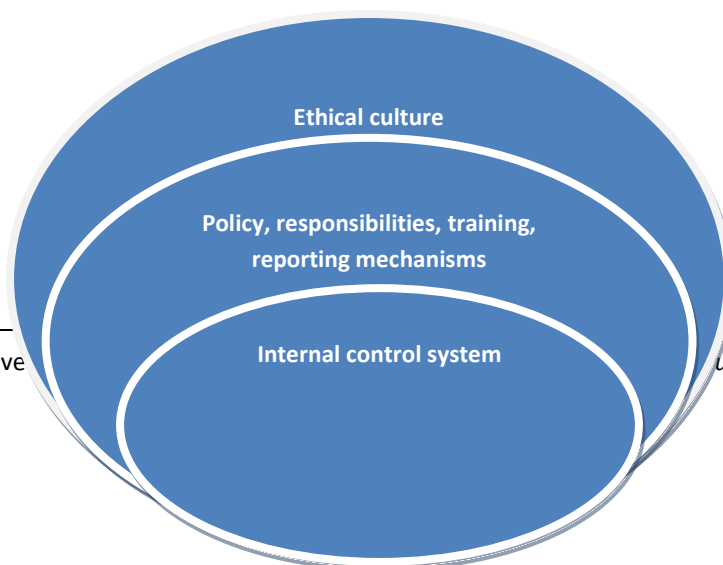
### 4.1. Prevention

The first cycle element is **prevention**. It consists in creating a clear and strong message from a given institution on inadmissibility of fraud that may happen during project implementation under the Programme. Particular role is played by the management of individual institutions in line with the rule that example must come ‘from the above.’ The example can be verbal, for instance in direct contacts or meetings within institutions, or more formalised, in the form of e-mails or information to institution staff on internal communication systems, such as the intranet.

The role of prevention is significant as it is easier to prevent negative phenomena than to take actions to mend undermined reputation afterwards. This is the only element in the entire cycle that does not start to run after fraud actually takes place, but before. Therefore it is a barrier against fraud and allows to avoid involvement of institution resources in subsequent cycle elements. To be noticeable, effective, and acceptable, preventive actions should be taken primarily in the sphere of shaping social awareness of the harmfulness of corruption.<sup>1</sup>

EC Guidance defines four types of prevention actions that are the most effective in combating fraud: **ethical culture**, **internal control system**, **fraud risks analysis**, and **policy, responsibilities, training, reporting mechanisms**. Their significance and structure are presented in Fig. 2. The EC emphasises that comprehensive implementation of all these actions brings about optimum effects.

Fig. 2. Prevention structure.



<sup>1</sup> In Poland preve

ruption Plan for 2014-2019.



Source: Own study on the basis of EC Guidance.

#### 4.1.1. Ethical culture

Ethical culture is a very board term at the foundations of all fraud type risk mitigation. While it is not measurable and shaping the desired attitudes is a long-term and multifaceted process, rooted in the institutions, among the employees and, where possible, the beneficiaries, ethical culture brings about measurable and long-term effects.

Ethical culture can be created through actions from the second circle on Fig. 2, i.e. policy, responsibilities, training and reporting mechanisms. There are also more general mechanisms that can considerably contribute to ethical culture development, such as **mission statement**, **tone from the top**, and **code of conduct**. They are characterised below.

##### MISSION STATEMENT

A clear expression that the **MA is striving to achieve the highest legal, ethical, and moral standards and that all participants involved in their implementation should comply with principles such as integrity, objectivity, accountability and honesty**. To the greatest extent possible, the MA will communicate its mission statement in its documents, during Programme meetings, and through direct messages communicated to individuals involved in work on Programme and project implementation.

##### TONE FROM THE TOP

Oral and/or written communication from the highest level, i.e. management of individual institutions, that the highest standard of ethical and moral behaviour is expected from the individuals involved in Programme and project implementation. This message should be communicated in ongoing contacts and actions, and stem from the code of conduct. The management of individual institutions should respond to warning signals that may suggest negative corruption-encouraging phenomena during Programme and project implementation.

##### CODE OF CONDUCT

Code of conduct (code of ethics) that all employees of institutions involved in Programme and project implementation must routinely declare adherence to. The **code of conduct** defines desirable patterns of behaviour of institution staff and is based on the following principles:

- **Principle of the rule of law** – stands for performance of duties with due diligence, in compliance with the EU and national law,



- **Principle of accuracy** – stands for diligent performance of duties to the best of one's knowledge and skills, based on correct findings, and using information solely for professional purposes and in line with its purpose,
- **Principle of impartiality** – stands for treatment of all applicants, beneficiaries, and other inquirers in a non-discriminatory manner, without prejudice on grounds of colour, sex, marital status, ethnic background, language, religion, sexual orientation, disability, reputation, or social rank,
- **Principle of avoiding conflicts of interest** - this means that no obligations arising from a family relationship, acquaintance or membership should be entered into, and no work or occupations which may be in contradiction with the public duties they should be undertaken. In the case of a conflict of interest between private matters and official business the employee has to withdraw from the activities that may raise suspicion of partiality or pursuit of self-interest,
- **Principle of professionalism** - this means concern for systematic improvement of skills, full knowledge of EU and national legislation, ability of substantive and legal justification of the decisions taken and procedures adopted as well as for professional cooperation inside and outside the institution,
- **Principle of transparency** - this means that the tasks are to be executed based on the procedures adopted while the stakeholder are informed about the procedure, subject to the protection of legally protected information,
- **Principle of responsibility** - this means that the difficult solutions and responsibility for his/her conduct cannot be avoided, the experience and knowledge must be shared, and reliability of the institutions involved in the Programme implementation must be striven after.

The particular institutions may have more detailed Codes of Conduct and principles associated with corruption and fraud combatting. For example in the Ministry of Economic Development where the Programme MA has its seat, *Anticorruption Policy in the Ministry of Infrastructure and Development* was adopted by way of the regulation of the Director General of the Ministry of Infrastructure and Development of 21 September 2015. The document describes in particular how to prevent a conflict of interests, a procedure to be taken in the case of personal or financial benefit or gifts are offered, how to inform about the opportunities for corruption and what to do in the case of external reports of corruption, and defines the scope of staff responsibility. The document also defines the employee conduct in particular situations.

#### ***4.1.2. Policy, responsibilities, training, reporting mechanisms***

Another important element of prevention consists of adequately allocating the responsibilities in the institutions involved in Programme and project implementation, organising training in and raising awareness of prevention and combatting the corruption and fraud.

### ***Allocation of responsibilities***

EC recommends to allocate the responsibilities precisely so as to avoid any doubts as to the responsibility for certain tasks, including those associated with fraud combatting. The staff should be aware of their responsibilities to be able to articulate them inside and outside.

The Management and control system should ensure that the functions and tasks carried out by the institutions are precisely determined as, similarly, the tasks implemented within, and the principle of function separation is met.

Allocation of tasks was laid down in the following documents:

1. Agreements on financing and implementation of the Poland-Belarus-Ukraine 2014-2020 Cross Border Cooperation Programme (Financing Agreement) - signed by the European Commission separately with Belarus and Ukraine.. They concern i.a. the institutional structure of the Programme, control system, personal data processing, prevention of irregularities, fraud and corruption, controls and audits, recovery of funds, financial adjustments, risk management, complaints or operation durability..
2. In accordance with Article 27(1) of Implementing Regulation, the participating countries may decide to set up a JTS and for this reason an Agreement on conferring the implementation of European Neighbourhood Instrument Programmes 2014–2020 to the Centre of European Projects was signed in order to establish and ensure functioning of the JTS. One agreement for all ENI Programmes has been drawn up and signed.

Additionally, each participating country shall appoint a control contact point to support the Managing Authority in its control of the programme obligations pursuant to Article 20(6)(b) of Implementing Regulation. The following institutions play the role of the CCPs: EU ITA Centre in Belarus, Ministry of Finance of Ukraine, Centre of European Projects in Poland.

Transparent conferring of the activities to the institutions lets them identify specific tasks at the level of the staff. In accordance with Article 26(8) where the institution hosting the MA is also a beneficiary under the programme, it is also necessary to ensure suitable segregation of functions.

At the institution level the staff who are involved, e.g. who participate in the call for proposals, should not combine this function with control tasks.

At the level of beneficiary the transparent allocation of tasks among the organisation personnel formally involved in the project work is an important aspect. A part-time employee should dedicate the time referred to in the employment contract to the work on the project. Time dedicated to the project work should be adequately registered and documented, while specifying the time devoted to the tasks within the framework of different budget lines.

### ***Training and awareness-raising***

Training is another important element of the ethical and moral structure building in the Programme institutions. All staff should be trained in both theoretical and practical matters of corruption and fraud prevention. Training of this kind helps build ethical awareness of the staff and prevents narrowing the definition of corruption to the bribery notion.

The scope of training should generally include the methods of detecting the irregularities and frauds, reporting mechanisms and corruption addressing proceedings. The required training subjects may be updated where the risk self-assessment results show the emergence of new negative phenomena or corruption threats. Thus, they will comply with the current needs of the Programme.

The institutions should attempt to train as large number of employees as possible. As far as the use of the EU funds is concerned the corruption may practically occur at any stage ranging from the call for projects and selection through the implementation up to the control. Therefore, it is recommended to ensure that each member of the staff involved in the Programme and project implementation participate in the training. It is also recommended to adapt the training subjects to the current needs of the staff member and tasks allocated to the specific post. The institution's staff should also have access to the available documents issued by the bodies set up to detect corruption, e.g. in Poland, the such documents and guides are available on the Central Anti-corruption Bureau (CBA) website.

Apart from the training, the current internal communication concerning ethics and corruption prevention also contributes to awareness-raising among the staff. It should be multi-level and multi-directional. It may be provided by means of any intranet systems, internal info portals, e-mail, discussion forums, electronic bulletins etc. It is recommended to use as many channels as possible to promote the desired attitudes and to educate the staff.

#### ***4.1.3. Internal control system***

The internal control is of key importance for the prevention of irregularities. Besides, it is the only prevention measure that may minimise the chance for an opportunity for a fraud to emerge. Hence, it may contribute both to the protection of the system correctness and good reputation of the employee or beneficiary. This subsection describes the process of identification of the sensitive posts and procedures set up in this respect.

##### ***Aim and scope of internal control***

According to the EC guidance the internal control system is the most efficient method to prevent potential fraud. 3 main elements may be mentioned as a reason for fraud, which are defined as "fraud triangle". These include: **opportunity** (the motive alone is not sufficient, i.e. there must be an opportunity for a fraud), **rationalization** (justification of the fraud by rationalising it), **motive/financial pressure** (greed, human weaknesses). In the EC opinion breaking up this triangle is of key importance for prevention of fraud. Among the cited factors the institutions have the greatest impact on the occurrence or lack of an opportunity for fraud. This is why it is so important to have the internal control system in place to exclude any emergence of such opportunity. The examples of the system weaknesses which may give rise to such an opportunity include omissions associated with supervision and reviews, allocation of responsibilities, approval by the management, system controls. It must be also stressed that a person who finds an opportunity and is tempted is supposedly in inconvenient and unpleasant situation<sup>2</sup>. The internal control system addresses such situations and, therefore, it protects the employee against embarrassing situations and any suspicion.

---

<sup>2</sup>International Anti-corruption Conference, Warsaw, 9 December 2010. Conference follow-up materials, Central Anti-corruption Bureau, Warsaw 2011, p. 110



In order to prevent such situations from occurring the internal control system of the MA includes the following:

1. Control inside the institution on an ongoing basis (verification of task implementation by the superiors, verification of the documentation on “four eye” principle basis),
2. Controls of projects, including technical assistance projects (both administrative and on-the-spot checks),
3. Cross-checks,
4. Ongoing analysis of data collected in the IT system,
5. Identification of so-called sensitive posts and putting in place the control mechanisms in order to eliminate the inherent risks.

### ***Sensitive posts***

When designing the management and control system for the Programme an analysis was carried out which identified the tasks in case of which the employees may be particularly sensitive to the factors with negative impact on the system operation. The factors include the risk of corrupt conduct and conflict of interests that may ultimately lead to financial fraud. The tasks involve in particular the employees who are direct contact with the beneficiaries as well as the employees whose improper performance of their duties may have adverse impact on the integrity and functioning of the Programme.

The identified sensitive tasks include the following:

1. Selection of projects for funding,
2. The process of concluding Subsidy Contracts, their modifications and termination thereof,
3. Verification of incurred expenditure,
4. On-the-spot check,
5. Recovery of funds from the beneficiary,
6. Certification of expenditure for EC,,
7. IT system administration.

The posts which include some the a.m. tasks within the scope of all the allocated tasks should be considered sensitive.

Therefore, taking into account the risk of improper performance of the duties that may adversely affect the integrity and functioning of the Programme, appropriate control mechanisms will be in place at such posts, i.e.:

1. Signing of the relevant declarations of impartiality (if the process requires so),

2. Application of “four eyes” principle,
3. Verification and approval of the tasks and work results by the direct superior,
4. Suitable distribution of tasks,
5. Appropriate training to raise staff awareness in this area,

All programme institutions are recommended to identify the sensitive posts based on the a.m. criteria and to apply the suggested safeguards.

Thus, the risk of fraud associated with the sensitive will be reduced to a minimum and the task which contribute to such risk will be subject to a strengthened control.

#### ***4.1.4. Fraud risks analysis***

The preventive measures set up to protect against the potential fraud may reduce the risk of its occurrence but they will not eliminate it entirely. Therefore, the EC recommends a **risk analysis** to be carried out in order to identify the areas and activities that may subject to an increased risk. In order to make this process easier EC provided a **fraud risk assessment tool** which is enclosed with the EC Guidance as Annex 1. It should be stressed that this tool is intended to assess the probability of corrupt practices rather than to detect them, and, therefore, to make the Programme institutions prepared for their occurrence.

It has been assumed that the tool will be used by the **self-assessment team** set up by the MA.

#### ***Fraud risk assessment tool***

Based on the previous financial perspectives EC elaborated a tool which encompasses specific fraud risks which may occur at 3 main stages of Programme implementation, e.g.:

1. Call for proposals,
2. Implementation of the projects by the beneficiaries, especially including the public procurement and labour costs,
3. Certification and payments

The a.m. list may be completed with the risks that are specific for the Programme based of the analysis of risks notified to MA by the institutions involved in the Programme implementation and committed to undertake risk analysis at their level.

In general, a full analysis will be carried out on annual basis. In justified cases when the risk level is very low and no case of financial fraud attempt was identified in the previous year, the MA may decide to carry out the fraud risk assessment every second year. When in the Programme circumstances arise that may bring about new risks and threats the self-assessment team may carry out and additional analysis in this respect.

The document created so will be used as a contribution to preparation of the MA Annual Control Plan for the subsequent financial year. It will include the identified risks, especially significant and critical risks, if any.

The methodology of risk analysis is based on 5 main steps:

1. Quantification of the risk of occurrence that a given fraud type would occur by assessing impact and likelihood (gross risk);
2. Assessment of the effectiveness of the current controls in place to mitigate the gross risk;
3. Assessment of the net risk after taking into account the effect of any current controls and their effectiveness i.e. the situation as it is at the current time (residual risk);
4. Assessment of the effect of the planned mitigating controls on the net (residual) risk;
5. Defining the target risk, i.e. the risk level which MA considers tolerable after all controls are in place and effective.

The responsibility for analysis preparation is borne by the self-assessment team. During the analysis process the team takes into account the audit and control reports (if drawn up in the period of time subject to the analysis), reported fraud and own control assessments. Besides, the team will be able to use the documents prepared for the purpose of, for example, management verifications, or other documents which may be helpful in analysis preparation. It is up to the self-assessment team members to identify the processes which need fraud risk assessment. At the same time, with the setting up of the a.m. team the mechanism has been put in place which potentially prevents arbitrary choices and fraud risk assessments in particular departments and institutions responsible for Programme implementation. JTS will also contribute to the document. Involvement of the a.m. institution is intended to prevent risk from being underestimated and omitting the risk areas, in particular in the light of modifications introduced along the Programme implementation process and particular project execution. The point is that the self-assessment team is to assess the risk associated with corruption while analysing the whole process that includes the particular activities. The analysis process will be documented so as to allow an overview of the analysis conclusions. In this context the team safeguards a reasonable and realistic risk cataloguing so that they are not too numerous and unspecified. The final version of the document will be submitted for approval to the TCD direction.

### ***Self-assessment team***

The task of self-assessment team consists in preparing the risk analysis in accordance with the EC Guidance. Composition of the team is of key importance for the execution of the a.m. task.

The risk analysis includes 3 main processes within the framework of the Programme implementation, i.e. call for proposals, execution of the projects, certification and payments, therefore, it is recommended that the scope of responsibilities of the members of the team includes the tasks associated with these processes. Thus, the team composition will provide for the broadest possible identification of risks which may emerge at the particular stages.

The team will be set up by the MA which also lays down the Rules for its operation and for the election of the team chairman. The team will be composed of at least 3 members. The team members are not entitled to additional remuneration for participation in the team work.

If necessary, the team may be extended to include a JTS employee or a controller. Representatives of services that combat fraud or of other specialised bodies that have useful knowledge in this area can be invited to team meetings.

Working meetings of the team will be called by the chairperson within at least 5 days prior to the planned meeting. Before the meeting each member provides the chairperson with proposals on selected types of fraud risk if some risks were identified that have not been covered by the previous analysis and the member believes they should be covered by self-assessment and there are other issues that the team should work on.

The main task of the self-assessment team is to assess fraud risk on a periodical or ongoing basis. Self-assessment cannot be performed by external entities as it requires familiarity with the management and control system and knowledge of applicants and Programme beneficiaries.

The tasks of the self-assessment team also include:

1. Running a database of detected/notified cases fraud,
2. Identifying areas that should be covered by systemic control in individual institutions if such a need results from analyses,
3. Analysis of mechanisms for notifying fraud under the Programme and processes described in this Manual,
4. Preparing recommendations as to the subject and scope of training and other information actions,
5. Informing and assisting to institutional staff as to interpretation of Manual's provisions.

#### ***4.1.5. Preventing conflict of interests***

##### ***General information and definitions***

Conflict of interests is highlighted by EC in the framework of the financial perspective 2014-2020 in Articles 52(2), 57(1)(c), Annex point 3(i)(d) of Implementing Regulation. A conflict of interests exists where the impartial and objective conducting the activities associated with the procedure of selecting the contractor by the project partner and persons authorised to incur liabilities on behalf of the project partner or persons performing actions connected with preparing and conducting the contractor selection procedure on behalf of the project partner is compromised for reasons involving family, emotional life, political or national affinity, economic interest or any other interest shared with the contractors.

Capital or personal ties are understood as mutual ties between the project partner and persons authorised to incur liabilities on behalf of the project partner or persons performing actions connected with preparing and conducting the contractor selection procedure on behalf of the project partner and the contractor which consist in particular of:

- a) acting as a partner in a civil partnership or a partnership,
  - b) holding at least 10% of stocks or shares,
  - c) acting as a member of the supervisory or management board, proxy, plenipotentiary,
  - d) being a spouse, relative by lineal consanguinity or affinity, secondary relative in the second degree of consanguinity or the second degree of affinity, in a relationship of adoption, care or guardianship.
- It should be noted, however, that conflict of interests itself does not constitute a violation, but failure to notify responsible persons and to remove those persons affected by the conflict of interests from performing their duties is considered a violation. Organisation for Economic Co-operation and

Development (OECD) suggests the following definition<sup>3</sup>: “A ‘conflict of interest’ involves a conflict between the public duty and private interests of a public official, in which the public official has private-capacity interests which could improperly influence the performance of their official duties and responsibilities.”

The MA aims at making decisions connected with Programme implementation objectively and impartially. Yet there may be situations where impartiality and objectivity of an employee could be compromised by some circumstances. Article 57(2) of the Financial Regulation stipulates that these circumstances include reasons involving family, emotional life, political or national affinity, economic interest or any other shared interest with a recipient.

When an employee making a decision in a specific Programme implementation sphere or participating in preparing the decision has or may have private interest in the way in which a matter is handled, a conflict of interests takes place. A conflict of interests occurs not only when an employee is driven by his/her private interest, but also when it is theoretically possible that personal interest would prevail over public interest.

A conflict of interests should not be identified with corruption. Corruption usually requires a deal between at least two partners which comprises kind of a bribe, payment, or profit. A conflict of interests arises when a person has an opportunity to prefer private interest to official duties.

### ***Counteracting conflict of interests***

Programme and project implementation may lead to various situations where a conflict of interests may occur, for instance during a call for proposals, recruitment of staff and experts, public procurement. Therefore it is recommended for institutions to counteract conflict of interests, in particular by discovering it.

It consists *inter alia* in:

1. Application of the ‘four eyes’ principle, which means that tasks are performed by at least two people,
2. Committing employees to immediately notify their superiors of:
  - a) Potential conflict of interests,
  - b) Suspicions or becoming aware of irregularities connected with spending funds under the Programme,
3. Submission of declarations on absence of a conflict of interests when performing their duties by institution personnel, if required by a process,
4. Submission of other declarations resulting from national law, for instance on the Polish side, submission of the declarations referred to in Article 17 of the Act – Public Procurement Law and exclusion from a public procurement procedure pursuant to the Act in the case of such circumstances,

---

<sup>3</sup> OECD guidelines *Managing Conflict of Interest in the Public Service*, pp. 24-25.



5. Participation in trainings, meetings, conferences, working groups and reading documents or other materials to expand staff awareness of preventing conflict of interests and corruption,
6. Issuing a code of conduct that would apply to all aspects of staff work, of which considerable part consists in contacts with the public, funds or areas where it is essential to treat all entities equitably.

Counteracting conflict of interests is of particular importance to following the principles of transparency, equal treatment and non-discrimination in public procurement.

If the risk of a conflict of interests is identified or if a conflict of interests has been notified or detected before or during a procedure, adequate measures must be taken to secure a contract award procedure on the basis of relevant national legislation. Depending on the existence of a declaration on absence of a conflict of interests, the nature of the conflict of interests and procedure stage, the following steps should be considered:

- Discussion of factual circumstances with the interested person to explain the situation, where applicable,
- Exclusion of the interested person from the contract award procedure regardless if he/she is an employee or an external expert,
- A change in the division of tasks and scope of responsibility of the personnel,
- Contract award procedure annulment.

Exclusion of an employee or expert from a procedure should be considered not only in case of an actual conflict of interests, but also in every case where there are grounds to doubt their impartiality. In exceptional cases exclusion of an official or an expert can be impossible due to budgetary shortages or absence of experts in specific fields. The contracting authority should then make sure its decision is fully transparent, specify the limits of this staff member's/expert's input in the procedure, and ensure that the final decision is based on transparent and honest evidence.

A declaration on absence of a conflict of interests should be signed when a given person accedes the procedure. It is an obligation that must be fulfilled immediately to protect the procedure and the individual.

A declaration on absence of a conflict of interests should include a definition of a conflict of interests and all requirements of the code of conduct or ethics applicable to a given procedure and connected with a conflict of interests, and reference to disciplinary, administrative, or penal sanctions for a false declaration.

The declaration should say:

- Whether the person undersigned is in apparent, potential, or actual conflict of interests connected with the contract award procedure in question,
- Whether there are any circumstances that may put the person in apparent, potential, or actual conflict of interests in the near future,
- That the person undersigned commits to immediately notify any potential conflict of interests in case of any circumstances that may lead to such a conclusion.

The existence of a conflict of interests in itself does not necessarily violate the law. It is against the law to participate in a given procedure if a conflict of interests occurs. It is thus essential to reveal any potential conflict of interests before a given procedure starts and decisions are issued, and to take adequate precautions.

## ***5. Fraud detection***

Prevention techniques are a kind of barrier to fraud and corruption, but they cannot ensure absolute certainty there will be none. Therefore it is necessary to set up a management and control system as well as adequate mechanisms to support it in detecting fraud. Independent auditors should be sensitive to any symptoms of potential fraud. To obtain sufficient assurance, control team members should remain sceptical throughout the control and take into account the findings of controls by institutions from outside the implementation area, such as the Supreme Audit Office, Tax Offices, the domestic institution responsible for public procurement control or corruption detection. If during a risk assessment, control planning, or substantive analysis the independent auditor concludes that the circumstances indicate fraud, adequate steps should be taken to safeguard financial interests of the EU and a participating countries from unjustified expenditure.

### ***5.1. Control system***

According to EU regulations, the control system envisages independent and complementary processes of control by institutions in the framework of the Programme implementation system and by AA audits, supported by a Group of Auditors.

Pursuant to Article 31(3) of the Implementing Regulation, carrying out verifications in the Programme is the responsibility of individual participating countries. They delegate authority to conduct the verifications, especially to the extent set out in Article 26(5)(a) of the Implementing Regulation, to selected control contact points. They nonetheless remain responsible for performance of these tasks.

The control system referred to above has been set up in a way that allows detection and identification of irregularities at various project implementation stages. The main role belongs to the independent auditor who verifies expenditure of beneficiaries. Verification consists in examining whether the costs of the project declared by the beneficiary are real, accurately recorded and eligible in accordance with the contract. During control, the independent auditor also takes into account the findings of controls by other authorised institutions. The MA recommends to conduct controls in compliance with the ‘four eyes’ principle, i.e. by at least two people. In addition an independent auditor must sign a declaration which says he/she is impartial towards the project and he/she will not disclose any information connected with the project that he/she acquires during the control.

The Programme follows joint control and audit rules set in Guidance on expenditure verification that cover general procedures for controls under Article 32 of the Implementing Regulation. The procedures define how to report irregularities detected in projects. The rules are binding for independent auditors involved in the Programme. This way the MA remains in control of processes throughout the Programme. Creation of a joint framework of conduct and accompanying procedures also reduces the risk of irregularities.

Due to the fact that participating countries are responsible for expenditure control in their territories, they verify correctness of the tasks they entrust to third parties. On the Polish side of support, systemic controls are carried out in this respect, in the auditors' headquarters and in the JTS. These controls serve verification of correctness and efficiency of designed control mechanisms and risk analysis. During systemic controls also potential problems concerning the staff of the institutions responsible for Programme implementation are identified, such as staff turnover and insufficient training, especially of new employees, which increases the risk of corruption. Both auditors and the JTS describe the process of reporting irregularities, taking corruption into account, in their internal procedures. Employees of the above-mentioned institutions must be familiar with these procedures and any possible amendments thereto.

The AA is located on the Polish side of support and conducts annual operation audits on the basis of which it estimates the error level in the operational Programme and assesses the management and control system in place. The AA passes the results of audits on to EC.

In addition, the MA and the NA share information on existence or suspicion of irregularities in a given participating country and on suspected fraud by a beneficiary with a registered seat in a given state, together with a proposal for remedial or corrective measures, on an ongoing basis. Also notifications from law enforcement bodies, press reports, and notifications from private entities (also anonymous tip-offs) can serve as sources of information on irregularities.

The above system ensures that irregularities, which may occur at any implementation stage, are effectively detected. Thanks to expedient identification, remedial actions can be taken in due time.

The control process is thus transparent and minimises the risk that fraud remains undetected.

## ***5.2. Control system supporting mechanisms***

The management and control system that allows detecting irregularities at every Programme implementation stage is described in Section 5.1. Yet the institutional framework of the system should be complemented by additional control mechanisms to support the process. In particular, it is adequate attitude and knowledge of people who perform control tasks on potential fraud.

All people involved in Programme and project implementation may see potential signs of fraudulent activity and are obliged to take appropriate steps in response. **Critical thinking** is a desirable quality in this respect, especially on the part of the people who perform control tasks. It means that when performing tasks, including control preparation and conduct, one needs to have a **healthy level of scepticism** and take into account the risk that information obtained in relation to these tasks may be misleading or false. Fraud is intentional, which makes it more difficult to detect than other irregularities. Fraudsters do whatever they can to make sure they remain undetected. Therefore employees should be informed where to look for fraud indicators on an ongoing basis.

***Fraud indicators (or red flags)*** are signs that fraudulent activity is taking place, when an immediate response is required to verify whether further action is required. The EC Guidance states that fraud indicators can also be specific to those activities frequently taking place in public procurement and labour costs. The non-exhaustive list of fraud indicators has been presented in annex 1 to this document.

If any red flags emerge during Programme implementation, it is recommended to disseminate information on that fact among the employees, for instance by e-mail. It can help other staff members see potential signs of fraud. It is important as fraud can take on various forms and it is necessary to be aware of its manifestations, e.g. vertical and horizontal collusive bidding and document falsification and forgery, as well as the methods of detecting fraud.

EC drafted and published documents that can help employees, especially those who control beneficiaries, in this respect, and recommends reading them:

1. *Identifying conflicts of interests in public procurement procedures for structural actions. A practical guide for managers* elaborated by a group of Member States' experts coordinated by OLAF's unit D2 – Fraud Prevention,
2. *Detection of forged documents in the field of structural actions. A practical guide for managing authorities* elaborated by a group of Member States' experts coordinated by OLAF's unit D2 – Fraud Prevention,
3. *Contract and public procurement fraud* – Annex to this document.

Red flags from a given year will be taken into account during a fraud risk analysis.

### **5.3. Analysis of available data**

EC believes that more and more advanced methods of collecting, keeping, and analysing data provide new opportunities in the area of combating fraud. At this stage, within the limits of applicable legislation of individual participating countries and taking these limits into account, data analysis can significantly enrich the risk assessment process as data can be verified with the data of other organisations from the public or private sector (for instance tax authorities, government departments, creditworthiness evaluation bodies) and potentially high risk situations can be detected even before funding is granted.

In the light of the above, it is recommended to Programme institutions to use publicly available data collected in various IT systems of individual participating countries (for example the National Court Register or commercial information databases in Poland) to detect fraud.

Taking personal data protection into account, it is possible to consider using data analysis to enrich the risk assessment process, verify data with other public and private sector organisations, and to detect potential high risk situations at every project implementation stage, even before the co-financing agreement is signed.

In addition, pursuant to Article 26(2)(d) of the Implementing Regulation an ICT system has been set up in the Programme. It ensures electronic communication between the beneficiaries and the institutions. Information on co-financing agreements, verified requests for payment, and changes during project implementation will be fed to the system. The system has many functionalities, of which the most important element from the point of view of fraud detection is the SRHD reporting tool. It allows generating reports from information in the system. Depending on the needs, it will be possible to generate information required to be verified if potential fraud is detected.

Analysis of tender data in public contract award procedures in the context of collusive bidding identification is of particular importance. The minimum scope of data for assessment of potential collusive bidding risk should include:

1. Basic information about the project,
2. Tender data,
3. Details of the contractor,
4. Data concerning bids (successful bid, rejected and withdrawn bids),
5. Details of sub-contractor(s).

The above-mentioned analyses and verifications should take into account risk factors with corresponding indicators (with specific values), such as:

1. The price is similar to the estimated cost of the contract (for instance all bidders submit expensive bids or 'atypical' bids are submitted),
2. The number and coordination of bids,
3. Possibility of geographical market division,
4. Withdrawn and rejected bids, especially former competitors becoming sub-contractors, links and 'obvious connections' between the contracting authorities and contractors or bidders.

If the results of analysis give rise to red flag suspicions and the contract award procedure has not been investigated by competent bodies or services, these should be notified (prosecutor's office, police, or other bodies).

## **6. Correction**

### ***Notification of the EC about suspected fraud***

In the light of Article 31 (3) participating countries shall notify irregularities without delay to the MA and the Commission and keep them informed of the progress of related administrative and legal proceedings. Thus MAs and their fraud self-assessment team will be aware of emerging risks and thus they will be able to respond and update relevant preventive measures on an ongoing basis.

Irregularities should be monitored by participating countries until resolution. Detection of irregularities (i.e. so-called preliminary administrative or court finding) entails a need to take corrective measures that consist in reduction of eligible expenditure in the application.

The MA introduced measures to prevent undue payment of funds into the management and control system. The measures envisage:

1. Exclusion of incorrect expenditure covered by explanatory proceedings at a given moment which may be however considered eligible in the future from the payment claim,
2. Possibility of suspending funding on the basis of the provisions of the Subsidy Contract.

### ***Recovery of funds***

If EU funds under the Programme are spent in a dishonest way, the MA will require beneficiaries to return undue payments. Pursuant to Article 74 of the Implementing Regulation, the MA shall be responsible for pursuing the recovery of amounts unduly paid. This provision also concerns fraud. The beneficiaries must repay the funds with interest. Detailed procedures in this respect are set out in Programme documents.

## ***7. Prosecution***

The control system and accompanying mechanisms serve effective detection of irregularities, including fraud. Information on fraud can appear within the system and come from other sources, such as other institutions, the press, or so-called whistle blowers. This chapter describes all identified sources from which Programme institutions can derive information on emerging negative phenomena. It also sets out a procedure to be followed should such information surface.

### ***7.1. Sources of information on fraud***

Information on fraud can come from a number of sources that can be divided into three groups as follows:

1. **Employees.** Information from institution employees obtained during performance of official duties and controls, in particular administrative verifications and on-the-spot checks.
2. **Institution or external body.** Information can come from an institution or body, both participating and not participating in Programme implementation, such as:
  1. EC,
  2. OLAF,
  3. European Court of Auditors,
  4. Audit Authority,
  5. National control institutions (for example on the Polish side of support: Supreme Audit Office, Office for Competition and Consumer Protection, Public Procurement Office, Regional Chamber of Audit),
  6. Competent EU and national law enforcement bodies,
  7. Other control institutions (for example on the Polish side of support: Tax Services, Voivodeship Inspectorate of Building Control/Poviat Inspectorate of Building Control).
3. **Other sources.** Information on fraud suspicion can be obtained from any entity anonymously, from a press report, or as another unconfirmed information. Information can come from so-called whistle blowers. It can also be derived from mass media by employees.

## ***7.2. Procedure in the case of information on fraud suspicion from particular sources***

According to Section 7.1, information on fraud can reach the institutions involved in Programme implementation from various sources. In the case of fraud suspicion and after its correct notification a participating country must transfer the case to a competent participating country's body for prosecution. Information about suspected fraud must be submitted to the AA, NA and MA. In the framework of this procedure it is important to ensure that the people who report fraud, so-called whistle blowers, are safe, i.e. they suffer no negative effects.

### ***7.2.1. Information from employees***

Due to the fact that fraud can occur at any project implementation stage, all employees should be sensitive to various kinds of signs of potential fraud during performance of their everyday duties.

Each time they learn something important that may prove fraud has taken place, all Programme institution employees must notify competent law enforcement authorities of that fact.

If an employee suspects fraud, he/she can notify competent national law enforcement bodies of suspicion of an offence in one of the following ways:

***Anonymous report (by phone with no personal data provided, for instance via a helpline or emergency line, in writing: without a signature or with an illegible signature)***

This form is intended for people who have information on an offence or have knowledge that can contribute to detection of a forbidden act or its perpetrators, but wish to remain anonymous.

***Letter sent or submitted to a competent body***

Notification of an offence can be e-mailed, mailed, faxed, or submitted to a police unit (or another competent law enforcement body) in person.

***Verbal report on offence***

The person reporting an offence must visit a police unit (or another competent law enforcement body) in person. This form involves interrogation of the person making the report in the capacity of a witness.

***Direct report to OLAF***

In addition to notifying domestic law enforcement bodies, every citizen can directly **inform OLAF** of suspected fraud or another serious irregularity that may have potentially negative impact on financial interests of the European Union. Information should be as precise as possible and OLAF should also receive relevant documents.

In this context, the key role is played by liaison officers from national investigation services cooperating with OLAF in the Member States.

OLAF services can be contacted in all official languages of the European Union:

1. Via the electronic Fraud Notification System (FNS) available at: <https://fns.olaf.europa.eu/>;

2. By mail to: OLAF – European Anti-Fraud Office, European Commission, Rue de la Loi, 200, 1049 Bruxelles/Brussel, Belgique/België;
3. By e-mail to [OLAF-FMB-SPE@ec.europa.eu](mailto:OLAF-FMB-SPE@ec.europa.eu).

Detailed information in this respect is available at:  
[http://ec.europa.eu/anti\\_fraud/investigations/report-fraud/index\\_pl.htm](http://ec.europa.eu/anti_fraud/investigations/report-fraud/index_pl.htm).

### ***7.2.2. Information from law enforcement bodies***

All institutions within the Programme implementation system should actively seek information on all potential instances of fraud when using any available tools, they are also obliged to share information they may have on proceedings conducted by national law enforcement bodies.

Not all pieces of information provided by the above-mentioned institutions constitute suspicion of fraud. Therefore they should be analysed in detail for fraud.

In the case of suspicion of fraud, each institution should make sure it has all the information necessary to at least determine the potential impact of fraud on the project and take adequate steps to address the matter comprehensively.

In situations that require it, the MA must withhold certification and report fraud suspicion to EC.

All institutions in the Programme implementation system are obliged to provide the MA with information on pending proceedings immediately. MA management will use the information to set adequate 'tone from the top' signalling potential areas at risk of fraud. The information will also be important for the fraud risk self-assessment team when preparing subsequent risk analyses.

### ***7.2.3. Information obtained from other sources***

When becoming aware of a possibility of irregularities in a project implemented under the Programme (i.e. information from a third person or directly from the beneficiary), one must always analyse whether a given event may give rise to suspicions of fraud.

If there are grounds to believe an offence has been perpetrated, employees must notify law enforcement bodies.

If information has been submitted to the police as well, a competent body must be contacted to inquire about actions taken on the case.

If information on proceedings of law enforcement bodies is derived from the press, one must always request a competent body to confirm the data and possibly supplement them.

If press is the source of information on irregularities that may prove an instance of fraud, the competent institution must take the necessary steps in this regard.

### ***Whistle blowers***

When information from other sources is concerned, there is information provided by so-called whistle blowers. Whistle blowers are people who, acting in good faith and driven by care for public



good, reveal irregularities such as potential fraud.<sup>4</sup> Under the Programme, it may concern irregularities on the part of representatives of Programme institutions and entities involved in project implementation, for example beneficiaries.

To facilitate contact with the MAs and to protect the people who report irregularities, a mailbox has been set up where any reservations can be e-mailed: [nieprawidlowosci.EWT@mr.gov.pl](mailto:nieprawidlowosci.EWT@mr.gov.pl). Information can be sent in Polish or English.

The MA will examine every notification in accordance with Programme procedures and with the law.

Every notification sent to the mailbox will be protected against unauthorised disclosure. Information in the notification that may reveal the identity of the person who sent the report will be protected at the stage of examination, during possible preventive measures, and in the future. It will be disclosed only to authorised officials and officers of competent services.

If the person who e-mails the notification wishes to remain anonymous, the report will be fully anonymised (personal details of the sender will be deleted from the notification, as well as other elements that could allow his/her identification) before passing it on for examination.

In the case of notifications (mainly anonymous) that are incomplete and it is impossible to supplement information, there is a risk that such a report will not be examined for formal reasons.

Literature:

1. *Detection of forged documents in the field of structural actions. A practical guide for managing authorities* elaborated by a group of Member States' experts coordinated by OLAF's unit D2 – Fraud Prevention,
2. *Identifying conflicts of interests in public procurement procedures for structural actions. A practical guide for managers* elaborated by a group of Member States' experts coordinated by OLAF's unit D2 – Fraud Prevention,
3. Report from the Commission to the European Parliament and the Council. *Protection of the European Union's financial interests – Fight against fraud*,
4. *Public procurement guidance for practitioners – on the avoidance of the most common errors in projects funded by the European Structural and Investment Funds*.

On the Polish side:

1. *Anti-Corruption Tips for Officials*, a document developed by the Central Anti-Corruption Bureau,
2. *Anti-Corruption Manual for Officials*, a document developed by the Central Anti-Corruption Bureau.

---

<sup>4</sup> *Support for and Protection of Whistle Blowers* [accessed on 5 November 2015], available on-line at: [http://www.batory.org.pl/programy\\_operacyjne/przeciw\\_korupcji/wsparcie\\_i\\_ochrona\\_sygnalistow](http://www.batory.org.pl/programy_operacyjne/przeciw_korupcji/wsparcie_i_ochrona_sygnalistow).

## Annex 1

### Fraud indicators (or red flags) for Cross-border Cooperation Programme Poland-Belarus-Ukraine 2014-2020 2014-2020

All people involved in Cross-border Cooperation Programme Poland-Belarus-Ukraine 2014-2020 and project implementation may see potential signs of fraudulent activity and are obliged to take appropriate steps in response. **Critical thinking** is a desirable quality in this respect, especially on the part of the people who perform control tasks.

In order to enhance above-mentioned critical thinking and to facilitate the detection of fraud, the Managing Authority prepared the list of the most important fraud indicators, which can be used for identification of fraudulent behaviour. If any red flags emerge during Programme implementation, immediate response is required to verify whether further actions are required.

The list is divided into 2 parts: **public procurement** and **labour charges and consultancy services**. It is connected with European Commission Guidance *Fraud Risk Assessment and Effective and Proportionate Anti-Fraud Measures* where it is indicated that 2 above-mentioned fields are especially exposed to potential fraudulent behaviour. Each part is divided into types of possible fraud, which has their own fraud indicators.

The list of fraud, which is non-exhaustive and can be **extended** by adding new indicators, which might appear during Programme implementation, e.g. types of detected fraud within the Programme, which are currently not listed.

#### **Public procurement:**

##### **1. CORRUPTION – BRIBES AND KICKBACKS**

- unexplained favourable treatment of a contractor by a contracting employee over a period of time,
- close socialisation between a contracting employee and service or product provider,
- unexplained or sudden increase in wealth by the contracting employee,
- contracting employee has an undisclosed outside business,
- contractor has a reputation in the industry for paying kickbacks,
- undocumented or frequent changes to contracts increasing the value of the contract,
- contracting employee declines promotion to a non-procurement position,
- contracting employee fails to file or complete conflict of interest declaration;

##### **2. UNDISCLOSED CONFLICT OF INTEREST**

- unexplained or unusual favouritism of a particular contractor or seller,
- continued acceptance of high priced, low quality work etc,
- contracting employee fails to file or complete conflict of interest declaration,
- contracting employee declines promotion to a non-procurement position,

- contracting employee appears to conduct side business;

### **3. COLLUSIVE BIDDING**

- winning bid is too high compared to cost estimates, published price lists, similar works or services or industry averages and fair market prices,
- persistent high prices by all bidders,
- bid prices drop when new bidder enters the competition,
- rotation of winning bidders by region, job, type of work,
- losing bidders hired as subcontractors,
- unusual bid patterns (e.g. the bids are exact percentage apart, winning bid just under threshold of acceptable prices, exactly at budget price, too high, too close, too far apart, round numbers, incomplete, etc),
- apparent connections between bidders, e.g. common addresses, personnel, phone numbers etc,
- contractor includes subcontractors in its bid which are competing for the main contract,
- qualified contractors fail to bid and become subcontractors or low bidder withdraws and becomes a subcontractor,
- certain companies always bid against each other, others never do;
- losing bidders cannot be located in the Internet, business directories, have no address etc (in other words they are fictive),
- correspondence or other indications that contractors exchange pricing information, divide territories, or otherwise enter informal agreements,
- collusive bidding has been found in the following sectors and is also relevant for structural funds: asphalt paving, building construction, dredging, electrical equipment, roofing, waste disposal;

### **4. UNBALANCED BIDDING**

- particular line item bids appear to be unreasonably low,
- changes are issued soon after contract awards to delete or modify line item requirements,
- line items for bids are different than the actual contract,
- bidder close to procurement personnel or participated in drafting specifications,

### **5. RIGGED SPECIFICATIONS**

- only one or a few bidders respond to request for bids,

- similarity between specifications and winning contractor's product or services,
- complaints from other bidders,
- specifications are significantly narrower or broader than similar previous requests for bids,
- unusual or unreasonable specifications,
- high number of competitive awards to one supplier,
- socialisation or personal contacts between contracting personnel and bidders during the bidding process,
- the buyer defines an item using brand name rather than generic description.

#### **6. LEAKING BIG DATA**

- poor controls on bidding procedures, e.g. failure to enforce deadlines,
- winning bid just under the next lowest bid,
- some bids opened early,
- acceptance of late bids,
- late bidder is the winning low bidder,
- all bids are rejected and contract is re-bid,
- winning bidder communicates privately with contracting personnel by e-mail or otherwise during bidding period;

#### **7. MANIPULATION OF BIDS**

- complaints from bidders,
- poor controls and inadequate bidding procedures,
- indications of changes to bids after reception,
- bids voided for errors,
- a qualified bidder disqualified for questionable reasons,
- job not re-bid even though fewer than the minimum number of bids were received;

#### **8. UNJUSTIFIED SINGLE SOURCE AWARDS**

- single source awards above or just below competitive bidding thresholds,
- previously competitive procurements become non-competitive,
- split purchases to avoid competitive bidding threshold,
- request for bid mailed only to one service provider;

#### **9. SPLIT PURCHASES**

- two or more consecutive, related procurements from the same contractor just under competitive bidding or upper level review thresholds,
- unjustified separation of purchases, e.g. separate contracts for labour and materials, each of which is below bidding thresholds,
- sequential purchases just under the thresholds;

#### **10. CO-MINGLING OF CONTRACTS**

- similar invoices presented under different jobs or contracts,
- the contractor invoices for more than one job for the same time period;

#### **11. COST MISCARGING**

- excessive or unusual labour charges,
- labour charges inconsistent with contract progress,
- apparent changes to time sheets,
- time sheets cannot be found,
- the same material costs charged to more than one contract,
- charging indirect costs as direct costs;

#### **12. DEFECTIVE PRICING**

- contractor refuses, delays or is unable to provide supporting documents for costs,
- contractor provides inadequate or incomplete documentation,
- out-of-date pricing information,
- apparent high prices compared to similar contracts, price lists or industry averages;

#### **13. FAILURE TO MEET CONTRACT SPECIFICATIONS**

- discrepancy between test and inspection results and contract claims and specifications,
- absence of test or inspection document or certificates,
- low quality, poor performance and high number of complaints,
- indications from the contractor's expense records that the contractor did not e.g. purchase materials necessary for the works, does not own or did not lease equipment necessary for the work or did not have the necessary labour on the site (NB: this type of cross-checking can be valuable);

#### **14. FALSE, INFLATED OR DUPLICATE INVOICES**

- invoiced goods or services cannot be located in inventory or accounted for,
- no acknowledgment of receipt for invoiced goods or services,

- questionable or no purchase order for invoiced goods or services,
- contractor's records do not reflect that the work was done or that the necessary costs were incurred,
- invoice prices, amounts, item descriptions or terms exceed or do not match contract items, purchase order, receiving records, inventory or usage records,
- multiple invoices with the same amount, invoice number, date etc,
- sub-contracts in cascade,
- cash payments,
- payments to off-shore companies;

#### **15. PHANTOM SERVICE PROVIDERS**

- service provider can not be found in any directories, the Internet, Google and other search engines etc,
- service providers address can not be found,
- the service provider lists incorrect street address or phone number,
- off-shore company used;

#### **16. PRODUCT SUBSTITUTION**

- unusual or generic packaging: packaging, colours or design different than the norm,
- discrepancy between expected appearance and actual appearance,
- product identification numbers differ from published or catalogue numbers or numbering system,
- above average number of test or operation failures, early replacements, or high maintenance or repair costs,
- compliance certificates signed by unqualified or non-certified person,
- significant difference between estimated and actual costs for materials,
- contractor is behind schedule but quickly catches up,
- unusual or obliterated serial numbers; serial numbers are not consistent with legitimate manufacturer's numbering system,
- invoice or inventory item numbers or descriptions do not match purchase order terms;

### **Labour charges and consultancy services fraud:**

#### **1. INCURRED LABOUR COST**

- distinctive charging patterns,

- sudden, significant shifts in charging,
- decrease in charges to projects/contracts in overrun or near ceilings,
- a disproportionate percentage of employees charging indirect,
- large number of employees reclassified from direct to indirect or vice versa,
- same employees constantly reclassified from direct to indirect or vice versa,
- weak internal controls over labour charging, such as employee time cards signed in advance, employee time cards filled in by the supervisor, time cards filled in with pencil or time cards filled in at the end of the pay period,
- actual hours and euros consistently at or near budgeted amounts,
- use of adjusting journal entries to shift costs between contracts, R&D, commercial work,
- significant increases or decreases in charging to sensitive accounts,
- employee's time charged differently than associated travel costs;

## **2. UNCOMPENSATED OVERTIME**

- professional staff required to work a significant amount of unpaid overtime on a variety of projects-both direct and indirect,
- salaried employees only charging the regular hours worked during any day for an extended period,
- a pattern of management directed unpaid overtime with employee bonus based on the extra hours worked,
- overrun contracts/projects worked on only during unpaid hours;

## **3. CONSULTING/PROFESSIONAL SERVICE**

- no formal signed agreements or contracts; however, large sums paid for "services rendered" based on invoices with few specifics,
- formal agreements or contracts exist but are vague as to services to be rendered, and no other documented support, such as detailed invoices, trip reports or studies, exists to justify the expenses,
- services paid for were used to improperly obtain, distribute or use information or data protected by law or regulation,
- services paid for were intended to improperly influence the content of a solicitation, the evaluation of a proposal or quotation, the selection of sources for contract award or the negotiation of a contract, modification or claim. It does not matter whether the

award is by the prime contractor or any tier subcontractor,

- services paid for were obtained or performed in some way that violated a statute or regulation prohibiting improper business practices or conflict of interest;

#### **4. LABOUR CATEGORIES**

- significant differences between proposed and actual unit costs or quantities with no corresponding changes in work scope or job requirements,
- task-by-task invoicing consistently at the ceiling level established in the contract. An exception would be if the contract/work order specifies how many hours to bill,
- specific individuals proposed as "key employees" not working on the contract,
- proposed labour not based on existing work force. Massive new hires needed. New hire labour rates significantly lower than proposed,
- employees' skills do not match the skill requirements as specified for their labour category or the contract requirements,
- employees typically charged indirect by the company being charged direct to the contract,
- partners', officers', supervisors' and other employees' time being charged in noncompliance with the contract terms or with the company's established accounting policies and procedures.