Prevention and Fight against Corruption

TERMS OF REFERENCE

Contract No:	2017/386-597, PREVENTION AND FIGHT AGAINST CORRUPTION
Objective (s)	2) Strengthened capacities for prevention of corruption in line with the strategy and action plan and the recommendations of the action plan for chapter 23 (Chapter 2. Fight against corruption)
Expert Category:	Senior Non-Key Expert (2 positions)
Position:	Senior Prevention of Corruption Expert – Information /Cyber/ Security and Whistleblowing
Result (s):	Result 2 – Prevention of Corruption
Activity No:	2.2.6: 8 x 1day training on WB protection (legislative framework – best practice – problems) overall 200 participants – max 25 participants x 8 trainings
Days allocated:	10 w/d for each Senior-NKE (Total of 20 w/d)
Location:	Serbia
Start/End of the tasks	September - November 2020

Background

1. Beneficiary country

Republic of Serbia

1.1 Contracting authority

European Union Delegation in the Republic of Serbia.

1.2 Relevant Project Background

1.2.1 Overall Objective

Improve overall efficiency in fight against corruption and reduce all form of corruption

1.2.2 Project Purpose

To strengthen national mechanisms for prevention and fight against corruption in accordance with the National Anti-Corruption Strategy and Action Plan for the Action Plan for Chapter 23.

II. Scope and content of the assignment

The Internet (and Internet services) is an integral part of the everyday life in modern society communications, business, education, healthcare and social interactions. Modern correspondence and workflows rely heavily on digital means of communications and data storage. Subsequently, these workflows produce huge amounts of data, which could be susceptible to abuse or breaches. With increasing dependence on technology, information security has emerged as a critical issue for citizens, businesses and government regulators.

The Republic of Serbia has adopted the Law on Information Security, regulating measures against security risks in information and communications systems, as well as setting out the responsibilities of legal entities in the management and use of information and communication systems. Knowledge of the basics of information security can help protecting personal and organization data. It is important that raise awareness of the security risks and what can be done to avoid those risks, and thus protect the obtained information.

The topic of *information security* has been identified as topic of great interest amongst the participants of the Project's trainings for whistle-blowers and last webinar on personal data protection (August 2020) for the authorised persons in terms of the Law on the Protection of Whistleblowers.

Since the information security is essentially tied with the effective implementation of the protections for whistleblowers, it is necessary for authorised persons, who receive the information and to conduct proceedings in respect of whistleblowing, to gain basic knowledge on the topic. It would enable them to understand a so-called "bigger picture" – the systemic needs and preconditions that are necessary for safe and effective whistleblowing.

The Law on the Protection of Whistleblowers started with implementation in 2015, providing the safe channels for staff or certain other categories to report fraud, corruption or serious wrongdoings in organisations. The Law applies to both public and private sector, provides three channels for blowing the whistle, and envisions court protection against retaliation. When disclosing information, a whistleblower may disclose numerous pieces of information that need to stay secure within the organization's information system. The authorised persons in the ministries and other public institutions and companies often come from the HR and legal/compliance departments, with no IT-background in most cases, where whistleblowing is being just one in already long list of duties. It is necessary that organizations do undertake measure to protect identity of possible whistleblowers and accused persons, and their personal data, from leaking them to the unauthorised persons and public.

Having said that, the participants in the webinar on information security would benefit from learning more about: (i) what is information and how to assess its value and need for protection; (ii) identify and estimate some key risks related to information security in the organization; (iii) understand legislation and standards through examples.

The contribution of the engaged Senior Non-Key Experts would be to:
(1) conduct assessment of relevant legislative framework;
(2) review relevant best practices and standards;
(3) develop tailor-made training curriculum for the needs of public servants;
(4) develop training program;
(5) verify content of the training once it is adapted into e-learning course;
(6) prepare transcript of the training so it can be used as additional training material in the future. Developed training materials will cover necessary basic concepts on management of information security.

The experts will be responsible to produce the e-learning course and enable its transfer/upload to the designated platform (National Academy for Public Administration). The engaged NKEs would work under the overall supervision of the Team Leader; and receive additional input from the already engaged Senior Non-Key Experts.

Tasks	Deliverables
1. Hold meeting with Project Team and other NKEs already engaged in complementary activities to discuss main issues, goals, methodology for the requested e-learning course, and timeline.	1.Brief summary of the meeting, including relevant proposals.

2. The SNKEs will develop training curriculum and program that would cover necessary basic concepts on management of information security including: • Modules, video(s), PowerPoint presentations, tests, reference lists, etc.	2.Training curriculum and program
3. Deliver 1 webinar on the topics in detail described above	3.Presentation and Attendance list
4. When tasks concluded, the NKEs will deliver Mission Report.	4.Mission Report
5. The Project TAT will coordinate the activities and arrangements needed to fulfil the assignment under the present ToR.	

IV. Qualification and skills:

__Senior Non-Key Expert__

General professional experience

- University degree in the Law, Political or Social Sciences, Computer Sciences, or related fields;
- At least 7 years in general professional experience relevant for the assignment;
- Experience in conducting assessments/research / analyses;
- Experience in preparation and delivering of the e-learning courses.

Specific professional experience

- Have hands-on experience in analysing laws and bylaws, and other pieces of legislation;
- Have hands-on experience in preparation of e-learning courses;
- Have hand-on experience in information security challenges and risks in ICT systems of organizations;
- Have thorough understanding of existing legal frameworks for information security;
- Have experience in report writing and presenting findings;
- Teamwork and good communication skills;
- Fluency in Serbian and English is required.

V. Annexes

- Project ToR
- Project PowerPoint template
- NKE Mission Report template

Application

* apply via e-mail to stevan.stepanovic@pwc.com
**apply only with CVs in EU or Europass form (include supporting documents for relevant experience stated in your CV) and specify for which concrete position you are applying for
***Please note that only short-listed candidates will be contacted