TERMS OF REFERENCE
for
Training services for Data Protection Officers and raising awareness for civil servants in accordance with General Data Protection Regulation (GDPR), Law on Personal Data Protection and Information Security Law of the Republic of Serbia

Enabling Digital Governance in Serbia (P164824)

a. Background Information

Digitalization is increasingly becoming the backbone of any and all functional restructuring in the public sector, an objective driver of change management and a precondition for transformative development. Going digital, being a horizontal measure, is also accelerating the attainment of Sustainable Development Goals, in further text, SDG. While it directly falls under SDG 16, e-governance is contributing to building stronger institutions – effective, accountable and transparent – at all levels.

The Government of Serbia, elected in June 2017, has heavily prioritized digital transformation of the national economy and state administration. The Prime Minister's Keynote Address before the Parliament stressed digitalization and education as the most important catalysts of innovations, competitiveness and growth for Serbia in the coming years. It also stressed the need for a rapid digitalization of public administration and provision of integrated, secure and citizen-focused electronic services. This political support has materialized in August 2017, when the new Government formed the OITeG and appointed the Prime Minister as head of the Council for Innovative Entrepreneurship and Information Technologies (IT Council).

In addition, the Government of Serbia has requested assistance of the World Bank in supporting the reform efforts, through a loan. To this effect, the World Bank has initiated the Enabling Digital Governance Project (EDGE). The project, expected to be launched in April 2019, aims at contributing to development of the digitalization in Serbia, through implementation of the following components:

Component 1: Foundations for Digital Service Delivery[1]
The objective of this component is to establish the necessary cross-cutting foundations to support the use of ICTs in the provision of public services to citizens, and businesses, including inter alia, regulations, standards, and digital infrastructure.

Component 2. Transforming Services for Citizens, Business and Government
The objective of this component is to support re-engineering, digitalization, and piloting of selected administrative e-services. It will support improvements in back-office processes to reduce administrative burdens and increase efficiency of administrative service delivery to citizens and businesses.

Component 3. Digital Skills Development, Institutional Strengthening and Change Management
Activities under this component will focus on transforming the provision of administrative services to citizens and businesses, which will result in the change of the way public servants do their work as well as the way citizens and businesses interact with the administration. The key result of this component is enhanced capacity for project management and institutional coordination to achieve project results. This component will include strategic frameworks to help all stakeholders to understand, commit and

[1] Under subcomponent 1.4 in Project Appraisal Document of the Project is emphasized the importance to implement the activities, which will ensure compliance with the General Data Protection Regulation (GDPR) and Law on Personal Data Protection, as well as Cybersecurity activities, which will ensure compliance with Law on Information Security

successfully develop digital skills, implement change and, by promoting digital skills and changes, contribute to further institutional strengthening which will bring major benefits to citizens and business.

For the purposes of effectively managing and coordinating EDGe and future projects with IFI financing, the Project Implementation Unit (PIU) has been founded at the OITeG. PIU will have a dedicated staff to coordinate and supervise implementation of here requested activity.

b. Objective

General Data Protection Regulation (GDPR) lays down the rules relating to the protection of the individuals with regard to the processing of personal data and rules relating to the free movement of personal data. The GDPR was adopted on 14 April 2016 and became enforceable beginning 25 May 2018, superseding the Data Protection Directive 95/46/EC.

The Serbian Law on Data Protection (ZZPL), which largely represents the translated and adapted GDPR regulation, was adopted in November 2018 (entered into force in August 2019), and therefore it can be reliably considered that the principles of the GDPR have been implemented in Serbia. ZZPL states that every public authority or body (public institutions) must designate a Data Protection Officer (DPO) and publish his or her contact data, as well as submit them to the Commissioner. The DPO is determined on the basis of his or her professional qualifications, and especially professional knowledge and experience in the field of personal data protection.

The Law on Information Security (ZIB) ("Official Gazette of RS", No. 6/16) was adopted in June 2016, and changed in 2017 and 2019, regulating an information security posture, defining processes and reporting about information security, including information security incidents, affecting not only critical infrastructure, but also public sector and government. The law is defining principle of information security awareness for all employees in organization and awareness of risk related to the information security in the process of governing and managing information systems.

Information Society and Information Security Development Strategy 2021-2026 with the Action Plan for the period 2021-2023, has the following specific goals to be achieved:

- Improving the digital knowledge and skills of citizens, raising the capacity of employees in the public and private sector to use new technologies and improving the digital infrastructure in educational institutions.
- Improving the Information Security skills of citizens, public administration and the economy through raising awareness and knowledge.

Along with the digitization and transfer of large volume of personal data from analogue to digital form, there is increasing misuse of personal data and a high risk of endangering the privacy of individuals. Therefore, it is necessary to provide the most effective legal means to protect the privacy of individuals, both at the global international level and at the level of individual countries. The low awareness of the requirements needed for protecting privacy points out that great challenges for implementing personal data privacy and complying with GDPR, ZZPL and ZIB still lie ahead for public institutions, state bodies and private sector.

This assignment should support activities aimed at ensuring compliance with the GDPR, ZZPL and ZIB including the Rulebook on the techniques, practices and controls for personal data protection in the Office for Information Technology and E-Government in accordance with skills development and government institutions' strengthening, through enabling government officials to act in accordance with relevant legal framework in the field of personal data protection and overall information security.

Having in mind the abovementioned, this assignment aims towards systemic introduction of qualified DPOs, as well as raising the awareness of employees in the state administration about the importance of compliance with all legislations that define these areas.

Implementation of this assignment should fully institutionalize information security and personal data protection mechanisms within overall e-Government framework and, as such, increase safety and security of operations and users.

c. Scope of Work

In order to raise the level of protection of personal data of citizens, the Consultant firm will be required to conduct trainings for DPOs, as well as awareness raising trainings in the area of ZZPL (GDPR) and ZIB for employees in the state administration within the GoS (Government, Ministries, Agencies, Administrations on the state level).

Apart from GDPR, ZZPL and ZIB, DPO trainings must include in depth analysis of the Rulebook which was communicated with the Commissioner for information of public importance and personal data protection. The Consultant firm which will implement this Assignment will receive the Rulebook upon signing the Contract.

For the purposes of effectively managing and coordinating this assignment, PIU shall dedicate its employees (GDPR and CyberSecurity specialists) responsible for coordinating and supporting the implementation of this Assignment and will be point of contact to the Consultant firm, as well as to the relevant stakeholders within the GoS.

The assignment should consist of 3 phases as described below.

Implementation time should be 18 months.

Phase I – Examination and assessment of the current state of personal data protection and information Security – Inception Report with a training needs analysis

Keeping in mind the importance of personal data protection and information security, it is critical that the consultancy conduct a GAP analysis of the current state of personal data protection in Serbia against the requirements set out in ZZPL/GDPR which should include a training needs analysis based on which curriculum will be adapted

The Consultant should advise the Activity board on the inquiry to be made towards the respective institutions on the current state of appointed and/or unappointed DPOs within their organizations. The output of this phase – inception report should include this analysis as well. It is of crucial importance for the assignment that the list of 150 DPOs is fully established by the end of the Phase II.

Consultant firm shall include Information security Gap analysis based on previous reports and current state, with attention on knowledge and awareness of public servants regarding Information security, which should include a training needs analysis based on which curriculum will be adapted.

Phase II – Developing the curriculum for Data protection officer trainings and awareness raising trainings

Based on the results of the Phase I, a detailed curriculum for DPO trainings and awareness raising trainings will be developed, which should encompass rules, guidelines and knowledge on personal data protection, ensuring complete understanding of ZZPL/GDPR of all employees.

The curriculum must contain two parts:

a) Part 1 refers to the trainings of DPOs, which should be conducted in person.
b) Part 2 refers to online awareness raising trainings for civil servants which should be conducted via online learning platform in order to:
    a. Inform and educate civil servants about ZZPL/GDPR
    b. Inform and educate civil servants about ZIB

Phase III – Conducting Data protection officer training and awareness raising

Once the curricula are developed and approved, the next phase is conducting (deployment) both DPO trainings and awareness raising trainings.

Trainings will be conducted in two steps:

1. DPO trainings should be conducted in person with delegated 150 employees from the governmental institutions.
2. Online awareness raising trainings for 5.000 civil servants which should be conducted via online learning platform in order to:
    a. Inform and educate civil servants about personal data protection
    b. Inform and educate civil servants about top information security risks and countermeasures
    c. Analyse and/or adjust curricula based on the feedback provided by the trainees, at the midpoint of the phase

The Consultant firm is responsible to organize and bear the cost of complete training logistics.

Progress Reporting

In addition to activities covered under the three phases as described above, the Consultant firm must also submit quarterly progress reports (once every three months) detailing activities completed in the quarter being reported on with respect to activities planned in the Inception Report. Reasons for delay or slippage, if any, must also be presented along with explanation why the delay occurred and description which actions should be taken so the total timeframe of the project remains the same.

On completion of all activities envisaged under the assignment, the consultant firm shall submit a Final Report that should contain a summarized description of activities the Consultant firm carried out over the assignment period and the results achieved during the development and implementation of the Data protection officer trainings and awareness raising trainings.

The Final Report and the quarterly progress reports must be submitted to the PIU within OITeG. The Final Report must be submitted one month prior to the completion of the contract.

d. Deliverables, Timelines and Payment Schedule

No.	***Deliverable***	***Deadline***	***Payment Schedule (in % of professional fee)***
1	Inception Report with a training needs analysis	2 months after contract signing	10
2	Curricula for Data protection officer trainings and Awareness raising trainings – final versions	4 months after contract signing	20
3	Conducting Data protection officer training (150 Data protection officers	8 months after contract signing	15
4	Online awareness raising trainings (5000 civil servants)	16 months after contract signing	45
5	Final Report	18 months after contract signing	10

All deliverables must be submitted in English and Serbian. The report(s) should be submitted, in hardcopy (2 exemplars) and in electronic format.

The OITEG is obliged to provide feedback to draft report within 2 weeks from delivery of draft report and/or documents.

All deliverables will be quality reviewed and approved by PIU within OITeG in consultation with the World Bank.

All deliverables developed under the contract belong to OITeG and OITeG has the right to transfer the ownership to national partners.

e. Qualifications

In order to be selected, the Consultant firm must possess, at the minimum, the following qualifications:

Part I: Requirements:
a) The Consultant firm must be a legal entity;
b) The Consultant firm must prove its capability by listing its experience in the last five (5) years (2016-2020) related to:

- Conducting of the training needs assessment – minimum 3 assignments
- Curricula development - minimum 3 projects
- Provision of minimum five (5) public DPO courses approved by a Personnel and Training Courses certification body. The certification body must be accredited, against ISO/IEC 17024 "Conformity assessment — General requirements for bodies operating certification of persons", by an Accreditation body who is a member of International Accreditation Forum (IAF) and is a full-time member of IPC (International Personnel Certification Association)
- Minimum five (5) certification and/or recertification audits the Consultant firm has conducted in accordance with ISO 27701 or ISO 27001 along with recommendations for personal data protection. Experience in the region is an advantage.
- Minimum two (2) projects which include employee awareness raising trainings in the field of GDPR (ZZPL) and ZIB, out of which minimum one (1) must be implemented in an organization with more than 500 employees

c) General Data Protection Regulations: With EU General Data Protection Regulation (EU 2016/679, approved on 14.04.2016 by European Parliament and enforced on 25.05.2018 – in further text GDPR), the most important basic principles of personal data processing are defined. This Part specifies privacy-related requirements for data Controllers and data Processors holding the responsibility and accountability of personal data processing.
To that effect, the Consultant firm, as a legal entity, must fulfill three (3) criteria to prove compliance with the GDPR requirements:

1. To provide written evidence of the fulfillment of all criteria laid down in GDPR Chapter 3 "Rights of the data subject", in all Articles, starting with Article 12 and finishing with Article 23 (including Article 23)
2. To provide written evidence of the fulfillment of all criteria laid down in GDPR Chapter 4 "Controller and Processor", Section 1, in Article 30 "Records of processing activities"
3. As evidence of compliance with the criteria set out in GDPR Chapter 4 "Controller and Processor", Section 2, in Article 32 "Security of processing", the Consultant firm must provide an accredited certification for "ISO 27001:2013 along with recommendations for personal data protection."

d) The Consultant firm must provide training for DPO which is approved by a Personnel and Training Courses certification body. The certification body must be accredited, against ISO/IEC 17024 "Conformity assessment — General requirements for bodies operating certification of persons", by an Accreditation body who is a member of IAF, and is a full-time member of IPC (International Personnel Certification Association)

Part II: Team requirements

The Consultant firm must fulfill at least the following capacity:

Team requirements:

The Consulting firm must ensure that the key staff, that will perform the listed assignments possess the following qualifications:

Key expert 1: Team Leader

- Minimum fifteen (15) years of general working experience
- Minimum Bachelor's degree in the field of organizational sciences, IT or similar
- At least ten (10) years of professional experience on leadership positions;
- Proven record of leading capacity building project in the public sector;
- Participation on Team Leader position (or in any other leadership role) on at least 1 project financed by IFIs, Donors and/or respective governments
- Certified as a Lead auditor or Lead implementer for ISO 27001 – Information Security Management System – the certificate must be issued from the side of EU Certification body
- Certificate for DPO issued from the side of EU certification body
- Excellent communication, organization, and teamwork skills
- Excellent English written and presentation skills.

Key expert 2: Personal Data Protection Expert

- Minimum fifteen (15) years of general working experience
- Minimum Bachelor's degree in the field of Legal, Organizational sciences, IT or similar
- Minimum ten (10) years of experience in personal data protection
- Certified as a Lead auditor for ISO 27001-Information Security Management System – the certificate must be issued from the side of EU Certification body
- Certificate for DPO issued from the side of EU Certification body
- Approved as a lecturer from the side of educational institutions and/or certification body in the field of personal data protection
- Proven track record in leading the development and/or delivering training programs– minimum 1 project in last 3 years;
- Knowledge, experience and exposure to legal framework in the area of data protection, specifically in Serbia, will be a distinct advantage
- Excellent communication, organization and teamwork skills

Key expert 3: Information Security expert

- Minimum fifteen (15) years of general working experience
- Minimum Bachelor's degree in the field of organizational sciences, IT or similar
- Minimum ten (10) years of working experience on position IT Manager or Information Security Manager
- Minimum of three (3) projects organized or funded by the EU related to the certification or implementation of the Information Security Management System - ISO 27001 in state institutions or public administration
- Proven track record in leading the development and/or delivering online training programs
- Certified as a Lead auditor for ISO 27001- Information Security Management Systems – the training course must be recognized by IRCA
- Certified as a Lead auditor for ISO 20000 Information Technology - Information Technology - Service Management System – the training course must be recognized by IRCA
- Completed BS 10012 Personal Information Management System training

- Excellent communication, organization and teamwork skills

Key expert 4: Project Coordinator

- Minimum fifteen (15) years of general working experience
- Minimum Bachelor's degree in the field of organizational sciences, IT or similar
- Minimum ten (10) years of working experience on leadership and/or Project Coordinator positions
- Participation on Project Coordinator positions on at least 1 project financed by IFIs, Donors and/or respective governments
- Certified as a Lead auditor or Lead implementer for ISO 27001 – Information Security Management System – the certificate must be issued from the side of EU Certification body, would be considered as an advantage
- Certificate for DPO issued from the side of EU certification body, would be considered as an advantage
- Excellent English speaking, written and presentation skills

Non-key experts:
The Consultant firm must provide at least:

- three (3) non-key experts who possess a DPO certificate issued by a recognized institution. The certificate must be issued by a state approved institution or by a certification body who's DPO course is approved by a Personnel and Training Courses certification body accredited against ISO/IEC 17024 "Conformity assessment — General requirements for bodies operating certification of persons", by an Accreditation body who is a member of IAF. and is a full-time member of IPC (International Personnel Certification Association)
- one (1) non-key expert who possess Auditor or Implementer certificate for ISO 27001 – Information Security Management System – the certificate must be issued from the side of EU Certification body

CVs for non-key experts should not be submitted in the technical proposal, but the firm will have to demonstrate that they have access to these non-key experts with the required profiles in their proposal. The Consultant may select and hire additional non-key experts as per their needs.

Required general professional experience for non-key experts is at least 3 years in the fields relevant for this service contract. Non-key experts will have to be fluent in spoken and written English and have excellent communication, team working and representation skills.
The costs for backstopping and support staff, as needed, are considered to be included in the firm's financial offer.

The time-input of all Key Experts should not exceed 850 man/days, in total. The time-input of all Non-Key Experts should not exceed 550 man/days, in total.

Part III: Technology, Methodology and Work Plan

1) The Consultant firm is to ensure use of online learning platform/tool, own solution or solution provided by the third party. Training curricula provided through an online platform should be compatible and/or adjusted for the application over NAPA (National Academy for Public Administration)
2) Cybersecurity Regulations: As a part of government information system online learning platform/tool must meet cyber security requirement and appropriate industry security level.
    1. Online learning platform/tool, must have implemented cyber security protection measures to ensure confidentiality, integrity and availability of online learning platform/tool
    2. Prove cybersecurity capacity and measures implemented in online learning platform/tool.

3) The Consultant firm must provide detailed training plan, curriculum created especially for this project.

f. Selection of the Consultant firm

The Consultant firm will be selected in accordance with QCBS (Quality-and Cost-Based Selection) method set out in the World Bank's Procurement Regulations for IPF Borrowers (July 2016, revised November 2017, and August 2018).

Evaluation of the Proposals will be done in accordance with following criteria:

#	**Criteria**	**Weight**
1	Experience of the Consultant firm relevant to the assignment	5
2	Key Experts' qualifications and competence for the assignment a) Key Expert: Team leader [points 10] b) Key Expert: Personal Data Protection Expert [points 10] c) Key Expert: Information Security Expert [points 10] d) Key Expert: Project Coordinator [points 5]	35
3	Adequacy and quality of the proposed Technology, Methodology and Work Plan in responding to the Terms of Reference	45
4	Transfer of knowledge (training) program (relevance of approach and methodology)	5
5	Participation by nationals among proposed Key Experts	10
The Key Experts' qualifications shall be evaluated according to the following sub-criteria and their belonging weights:		
a)	General qualifications (general education and experience)	20
b)	Specific relevant experience required	80

The minimum passing score is 75 points.

The score per each of the criteria and sub-criteria is calculated in the following manner: score = (0-100 points) *weight.
QCBS uses a competitive process among short-listed firms that takes into account the quality of the proposal and the cost of the services in the selection of the successful firm.
The OITeG will publish Request for Expression of Interest and upon evaluation of received EoI, five to eight best evaluated firms will receive Request for Proposal. Those firms will be called to submit technical-and financial proposals.

g. Timeframe and duration

Contract duration: 18 months

h. Terms of Payment

The Contract will be the Standard World Bank Lump Sum Contract. The payments for services will be based on the deliverables / reports approved by the Project Coordinator. The Contract costs will include remuneration and reimbursable costs referring to the assignment.

i. Conflict of Interest

The engaged Consultant must not be involved in any other related activity to this Project.