# Terms of Reference with specification of inputs for short-term expert assignment

giz Deutsche Gesellschaft
für Internationale
Zusammenarbeit (GIZ) GmbH

## Procurement of the McAfee Data Loss Prevention Solution

## 1. Brief information on the project

Stand-alone measure: "Support of the German-Georgian pilot project for the introduction of the Automatic Exchange of Information in Tax Matters (AEoI) in Georgia", PN: 2005.3506.2-049.00

This stand-alone measure, within the scope of German development cooperation, is implemented by the GIZ "Study and Experts Fund" and it builds on the results, achieved in frames of the predecessor project “Combating Tax Evasion through Piloting the Automatic Exchange of Information in Georgia", implemented under the "Eastern Partnership Regional Fund for Public Administration Reform" in 2018 - 2020.

The objective of the current stand-alone measure is to provide further support to the Georgian Revenue Service (GRS) in the advancing the implementation of automated exchange of information (AEoI). This will support the fulfilling of Georgia’s official commitment to begin exchanging information with multilateral partners through the AEoI in 2024.

In particular, GIZ support covers two main components in frames of the stand-alone measure:

- The first component is concerned with information technology and administrative infrastructure. In particular, GRS requires the support of external expertise to produce a technical document - a Terms of Reference - that is to be used by IT developers to develop the AEoI platform. The platform will allow GRS i) to receive Common Reporting Standard (CRS)1 data from financial institutions, ii) to validate CRS data, sort it according to the CRS XML Schema, and transmit it to exchange partners, and iii) to receive CRS data from exchange partners (i.e. to match these data sets to the existing GRS data environment and use them for high level risk assessments).

* *This particular component is already accomplished successfully*

- The second component is concerned with implementation of confidentiality and data safeguarding standards. Specifically, GRS requires the procurement of a subscription/license for the GRS Data Loss Prevention (DLP) solution. One of the more critical needs pertaining to the effective implementation of the information security management system (ISMS) within the Georgia Revenue Service is the current lack of an adequate technical solution that would provide visibility into data usage and movement across the organization. Such a technical solution would allow the application of policy-based restrictions on the content and context at time of operation (in other words, allowing the identification and flagging of improper use of taxpayer data by unauthorised officials).

## 2. Context

Common Reporting Standard (CRS) is the the standard for the Automatic Exchange of Information (AEoI), thus the automatic exchange of financial account information in tax matters. CRS is developed by OECD based on the decision of G20 Finance Ministers and Central Bank Governors, in order to enhance co-

[1] The *Common Reporting Standard (CRS)* was developed by the OECD and represents the international consensus on the automatic exchange of financial account information for tax purposes on a reciprocal basis.

operation between tax administrations in the fight against tax evasion and in protecting the integrity of tax systems. CRS requires jurisdictions to collect data from their financial institutions and to automatically exchange it with other jurisdictions on an annual basis. It lays forth the financial account information that must be communicated, the financial institutions that must report, the various types of accounts and taxpayers that must be covered, and the common due diligence procedures that financial institutions must follow.

Confidentiality, data safeguards and proper use of the information is a critical pre-condition for the AEOI implementation. Therefore, at GRS, as a potential administrator/competent authority receiving and sending the data should fully meet OECD Global Forum standards on data safeguards and confidentiality. GRS has to implement information security management system entity-wide, including effective implementation of system controls to prevent data loss, in order to comply with the standards.

At the moment GRS applies a significant number of security controls in order to mitigate the threat of taxpayer data being misused. These controls are applied across all of the main security control 'domains' that are most relevant for a tax administration. However, at the same time there are some specific areas of weakness that need to be addressed. As a first step, before actual exchange of the data takes place, Georgia has to develop and follow an action plan on ensuring confidentiality and data protection. Among other important milestones of the abovementioned action plan, GRS has prepared, approved and implemented major security policies within the information security framework implementation and is currently in the process of working on some necessary system controls.  Among the identified crucially important controls is data loss prevention centralized solution for the monitoring, tracking and reporting data in motion, including protection of removable media, to be implemented as a high priority.  Acquisition and implementation of the subject solution will ensure protection of employee personal privacy data and taxpayer data, including the exchanged data.

**Georgia Revenue Service has outsourced its physical and virtual infrastructure to the Ministry of Finance LEPL Financial-Analytical Service (FAS), including management of its security solutions and products. Therefore, FAS serves as the key provider of the mentioned services and responds to relevant service requests from the Georgian Revenue Service pertaining to the infrastructure management, utilization, and maintenance.  As such, FAS will be the primary recipient of the Solution and all related licenses, specific training and support services associated with the full-scale deployment of the subject Solution.**

The focus of the subject Terms of Reference (TOR) is description and requirements for the specific Data Loss Prevention solution, including necessary licenses for operational capability to be provided by the potential vendors.

## 3. GIZ shall hire the contractor from 01/11/2023 until 31/12/2023

## 4. The contractor shall provide the following work/deliverables:

The overall objective of the assignment is **to select security solutions provider (thereafter „Bidder") for supply, implementation, maintenance and support of McAfee Data Loss Prevention solution (thereafter "Solution"), for a period of one year with the installation at the Financial-Analytical Service (FAS) of the Ministry of Finance to service Georgia Revenue Service (GRS) data loss prevention needs.**

## 5. Scope of the assignment

The scope of work will include but not be limited to the following:

5.1 The Bidder should offer a comprehensive Data Loss Solution for Data Protection for the Ministry of Finance LEPL Financial-Analytical Service to provide data loss prevention services to the Ministry of Finance LEPL Georgia Revenue Service.

**Available net budget for aforementioned solution equals to the 45000 EUR (equivalent in GEL).**

**5.2 The Solution specific requirements:**

5.2.1 Advanced protection capabilities, to provide comprehensive protection for multiple channels, including removable storage devices, the cloud, instant messaging, web, printing, clipboard, file-sharing applications, screen capture, etc. Among others, these capabilities shall include user-initiated scan and remediation, tagging technology to identify documents according to their origin, manual classification of documents.

5.2.2 Centralized management capabilities, including multiple policies and rule sets to define DLP policies across the organization and customize them considering different departments, role, regulation, and more.

5.2.3 Role-based access control capabilities to ensure separation of duties for policy management as well as incident management.

5.2.4 Security policies implementation capability, to create and enforce policies for information leaving the organization via email, IM, portals FTP transfers, etc.

5.2.5 Ability to intercept and monitor email for compliance and to protect managed and unmanaged mobile devices.

5.2.6 Built-in polities to classify and protect different content types over any port and any application, to ensure protection for known and unknown sensitive information

5.2.7 Object-classification mechanisms (fixed-format and variable data) to classify and block sensitive information and identify risks. The Solution shall cover content and contextual information, detect grammar or syntax of multiple objects, including text documents, source code and other, as well as identify content types regardless of the extension.

5.2.8 Ability to monitor, track, and Report on Data in Motion across the network in real time and provide its full visibility.

5.2.9 Pre-built rules to perform real-time network traffic scanning and analysis to detect anomalies. Apart from real-time monitoring rules, the Solution shall leverage historical network traffic behavior to identify sensitive data and its usage scope.

5.2.10 Ability to set up pre-built and customizable policies and automatically distribute policies and rules to specific appliances.

5.2.11 Ability to have a centralized view of all identified incidents, to detect and centralize correlated incidents into an incident dashboard.

5.2.12 Comprehensive user management capability to differentiate roles and assign permissions accordingly.

5.2.13 Integration with LDAP and Microsoft Active Directory for authentication

5.2.14 Comprehensive reporting capabilities at both high and very granular level, exportable in PDF and CSV formats.

5.2.15 Single user-friendly and intuitive management console to provide centralized system management to determine the type of information that is sensitive and manage its access, transfer, storage, and use.

5.2.16 Fully compatible and unified with McAfee MVISION and ePOlicy Orchestrator software.

5.2.17 The Solution should be able to keep logs for a duration of 1-3 months on the server and 1 year online.

## 5.3 Requirements for solution implementation

The Bidder is required to:

5.3.1 Provide comprehensive DLP solution as described in 5.2 of the subject TOR

5.3.2 Deploy the Solution in the FAS infrastructure fully

5.3.3 Set-up and activate pre-built set of policies and up to 10 customized policies in the Solution

5.3.4 Provide hands-on technical training for up to 7 (seven) assigned staff of the Ministry of Finance and Georgia Revenue Service on the full functionality of the Solution. The training should include setting up the solution, activating basic and advanced functionalities, activating pre-built policies and setting up new policies, generating default and customized reports, case management, incident management dashboard utilization, complex data classification techniques and mechanisms, user/role management, etc.

5.3.5 Supply, implement and provide technical and other related support of the Solution for the duration of the contract/service.

5.3.6 Provide comprehensive set of manuals for all components of the proposed Solution.

5.3.7 Inform of any additional storage or other infrastructure-related requirements to make the Solution fully operational prior the actual deployment.

5.3.8 Provide the license (end-user) expansion capability without the need to change the Solution or its individual modules/components.

5.3.9 Provide any and all functional and security updates as they become available to keep the Solution secure and up to date.

5.3.10 Advise of best practices for implementing various policies or policy sets within the Solution as per best accumulated knowledge of the manufacturer/solution provider.

5.3.11 Inform of any vulnerabilities in the Solution immediately upon discovery.

## 6. Proposal Structure

The Bidder shall provide the proposal in response to the subject TOR to include the following components in the strict order provided below:

1. Short narrative on the Bidder and its relevant work;
2. Scope of works, technical specifications and functionality detailed description of the solution, implementation plan and timeline;
3. Vendor qualifications and references (from completed projects);
4. **Number of licences to be provided (incl. in this ToR described services for full implementation, maintenance and support) for one year period, for the given maximum budget of net 126500 GEL.**

## 7. Eligibility Criteria

The assessment criteria for selecting potential Bidder:

- The Bidder shall be a company registered and operating in Georgia (Republic of) for at least two years*;
- The Bidder should have a demonstrated experience integrating security solutions in Georgia for private and public sector*;
- The Bidder should have at least 2 (two) successful deployments of the McAfee DLP Solution or similar solutions at organizations in Georgia*;
- The Bidder (its shareholders, management, employees) should not be blacklisted by any bank/institution in Georgia or be under investigation;
- The Bidder shall have an experienced technical engineer onsite to assist in Solution deployment and implementation FAS on-premises (CV has to be submitted together with the offer). If necessary, the Bidder should be able to involve regional/global representative of the Solution Vendor to ensure full and frictionless deployment and implementation of the Solution*;
- The Bidder should hold any all licenses necessary to deploy, implement, maintain and support the proposed Solution*.
-

** Corresponding information (reg. company experience, project references, licenses etc.) should be included and described in the offer, submitted by the bidder.*

## 8. Assessment Criteria

Number of licences offered by the bidder (incl. in this ToR described services for full implementation, maintenance and support) for one year period, for the given maximum budget of net **126500 GEL.**