REGIONAL ANTI-CORRUPTION INITIATIVE

ASSESSMENT OF THE LEGAL FRAMEWORK AND TECHNICAL CAPACITIES FOR COLLECTION, VERIFICATION AND EXCHANGE OF ASSET DECLARATION DATA IN THE SOUTHEAST EUROPE - REPORT

In partnership with
UNODC
United Nations Office on Drugs and Crime

With funding from
Austrian Development Cooperation

Assessment of the legal framework and technical capacities for collection, verification and exchange of asset declaration data in the Southeast Europe - REPORT

REGIONAL ANTI-CORRUPTION INITIATIVE

January 2024

Publisher

Regional Anti-corruption Initiative

Editor

Nikola Naumovski, RAI Senior Anti-corruption Advisor

Authors

Irena Brzanova, Legal Expert
Esmin Berhamović, IT Expert

Proofreader

Profis d.o.o., Sarajevo

Design and print

UrbanGRAF, Sarajevo

The views expressed in this document are solely those of the authors and do not necessarily reflect the views of the Regional Anti-Corruption Initiative or its member States, or of the Austrian Development Cooperation.

TABLE OF CONTENTS

* This designation is without prejudice to positions on status, and is in line with UNSCR 1244 and the ICJ Opinion on the Kosovo Declaration of Independence

ACKNOWLEDGEMENTS

The Regional Anti-Corruption Initiative (RAI) Secretariat wishes to acknowledge and thank the experts and specialists from the competent institutions who participated in the preparation and development of the Assessment of the legal framework and technical capacities for collection, verification and exchange of asset declaration data with other jurisdictions for Albania, Bosnia and Herzegovina, Kosovo*, Moldova, Montenegro, North Macedonia and Serbia (the Blueprint). In particular to the High Inspectorate of Declaration and Audit of Assets and Conflicts of Interest (HIDAACI) from the Republic of Albania, Agency for the Prevention of Corruption and Coordination of the Fight against Corruption of Bosnia and Herzegovina, the Agency for Prevention of Corruption of Kosovo*, National Integrity Authority (ANI) of the Republic of Moldova, the Agency for Prevention of Corruption of Montenegro, the State Commission for Prevention of Corruption of the North Macedonia and the Agency for Prevention of Corruption of the Republic of Serbia.

This document was developed under auspices of the Regional Programme Southeast Europe-Together against Corruption (SEE-TAC), implanted in partnership with the United Nations Office on Drugs and Crime (UNODC) with the financial support of the Austrian Development Cooperation (ADC).

1. EXECUTIVE SUMMARY

Legal and technical options and future challenges in effective implementation of the International Treaty on Exchange of Data for the Verification of Asset Declarations in the legislation and practice of beneficiary jurisdictions

In the era marked by global interconnectedness and greater focus on transparency and accountability, the ratification and implementation of the International Treaty on Exchange of Data for the Verification of Asset Declarations represents a key step forward. This Treaty underscores the commitment of the international community to combat corruption, promote financial integrity and ensure accountability of public officials by facilitating the exchange of data related to asset declarations. To effectively integrate the provisions of the Treaty into the legal framework in each beneficiary country, a precise approach to identification and implementation of the best legal and technical solutions is of vital importance.

Implementation of the International Treaty holds substantial significance in the fight against corruption and promotion of good governance. By harmonizing the process of verification of asset declarations across beneficiary countries the Treaty fosters a collaborative approach to addressing illicit wealth and ensures that public officials' financial activities are subject to monitoring.

Successful integration of the Treaty into national laws requires comprehensive legal solutions. Analysis of the existing legal frameworks in beneficiary countries will identify potential gaps and inconsistencies. Amendments to laws related to asset declaration, data protection and international cooperation should be considered with the aim to create a balance between facilitating data exchange and protecting the rights of individuals, thus ensuring compliance with both the Treaty and the international human rights standards.

Data exchange established by the Treaty requires implementation of efficient and secure technical solutions. Establishing secure and standardized data sharing protocols and infrastructure is imperative for ensuring the accuracy and confidentiality of exchanged data. Beneficiary countries should take all necessary measures to protect such data from unauthorized access.

The International Treaty on Exchange of Data for the Verification of Asset Declarations presents a historic opportunity to reinforce transparency, accountability and the rule of law in beneficiary countries. With joint efforts and commitment, the international community can break down the barriers that protect corruption.

2. BACKGOUND INFORMATION

The Regional Anti-Corruption Initiative (hereinafter: *RAI*) is an intergovernmental regional organization comprising nine member countries in South East Europe (SEE): Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Moldova, Montenegro, North Macedonia, Romania and Serbia; along with five observers: Poland, Georgia, Greece, Ukraine and Slovenia.

RAI's mission is to lead regional cooperation in support of anticorruption efforts by providing a common platform for discussion through exchange of knowledge and best practices. RAI acts as a regional hub where the governments of the region can combine their efforts to curb corruption in the SEE.

The RAI Secretariat is based in Sarajevo and is the executive body of the Initiative. It facilitates regional cooperation and efforts to curb corruption in SEE by building on existing actions through better coordination of all efforts and by relying on high-level political commitment.

RAI and the United Nations Office on Drugs and Crime (UNODC) are jointly implementing the 3-year Regional Programme "Southeast Europe - Together Against Corruption" (hereinafter: SEE-TAC) funded by the Austrian Development Cooperation (hereinafter: *ADC*). SEE-TAC focuses on Albania, Bosnia and Herzegovina, Kosovo*, Moldova, Montenegro, North Macedonia and Serbia as beneficiary jurisdictions.

The overall goal of the Programme is to contribute to strengthened resilience to corruption in SEE societies, harmonized by strengthening the capacity of governments, civil society organizations (hereinafter: *CSOs*), the private sector and the media to prevent and combat corruption.

To achieve the Programme goal, the Programme is designed to deliver six results (outcomes). By the end of the Programme, it is expected that the targeted jurisdictions will have strengthened their corruption risk assessment (1) and corruption proofing of legislative mechanisms (2); that the regional framework for cooperation on data exchange in asset disclosure is fully operational (3); that the general public in the region is better informed about prevention of corruption and the work of relevant entities (4); that CSOs and other relevant stakeholders have increased and furthered their capacities, knowledge and engagement on UNCAC implementation (5); and that CSOs, SMEs, chambers of commerce have enhanced their knowledge and cooperation in the area of collective action and compliance (6).

Direct beneficiaries of the Programme are the representatives of national ministries and anticorruption agencies, civil society, private sector and relevant partner umbrella organizations, such as the SELDI Network and the United Nations Convention against Corruption (hereinafter: *UNCAC*) Coalition. This assignment is directly linked to Outcome 3: Regional framework for cooperation on data exchange in asset disclosure is fully operational, with

- Output 3.1: A regional mechanism for data exchange in asset disclosure is introduced into national practice;
- Output 3.2: A regional network of perspective Focal Points for asset disclosure is established and maintained;

- Output 3.3 Baseline capacities, inclusive of IT infrastructure, for regional exchange in the verification of asset declarations have been determined;
- Output 3.4 International Treaty is promoted at the regional level.

In Phase 1 of the Regional Programme (2015-2020)[1], RAI developed the text and facilitated the process of technical and political negotiation of the International Treaty on Exchange of Data for the Verification of Asset Declarations (hereafter Treaty)[2] as a legal instrument for better cooperation between integrity bodies in the civil and administrative exchange of data for verification of asset declarations in line with the UNCAC (Article 43). The Treaty signing ceremony by the initial three beneficiary jurisdictions: Montenegro, North Macedonia and Serbia, with the Government of Serbia as the depositary, was held on 19 March 2021[3].

Following the initial signing by three countries, the Treaty needs to be operationalized and transposed into national legal frameworks. Transposition of the Treaty into domestic legal frameworks will streamline formal communication and simplify the presently time-consuming process of verification of public officials' asset declarations through data exchange[4].

[1] Final External Evaluation of the Southeast Europe (SEE) Regional Programme on Strengthening the Capacity of Anti-corruption Authorities and Civil Society to Combat Corruption and Contribute to the United Nations Convention against Corruption (UNCAC) Review Process https://www.rai-see.org/php_sets/uploads/2020/05/FINAL-External-Evaluation-Report-APRIL-2020.pdf
[2] https://rai-see.org/what-we-do/regional-data-exchange-on-asset-disclosure-and-conflict-of-interest/
[3] https://rai-see.org/the-regional-treaty-on-exchange-of-data-for-the-verification-of-asset-declarations-signed-today/
[4] https://rai-see.org/php_sets/uploads/2021/12/Integrating-the-Treaty-into-National-Laws.pdf

3. ASSESSMENT OBJECTIVES

The first objective of the assignment is to produce an assessment of the legal framework and technical capacities for collection, verification and exchange of asset declaration data with other jurisdictions. The assessment covers the following jurisdictions: Albania, Bosnia and Herzegovina, Kosovo*, Moldova, Montenegro, North Macedonia and Serbia.

The second objective of the assignment is to develop the long-term implementation plan – the Blueprint.

The Legal Expert will provide a comprehensive assessment of the legal framework for collection and verification of asset declarations in each jurisdiction, in respect of their capacity for data exchange with other jurisdictions. The Legal Expert will develop conclusions and recommendations for strengthening and alignment of existing frameworks.

The Technical Expert will examine the technical capacities, including the available infrastructure and IT solutions, for data collection, verification and exchange at the regional level. The outcomes of the assessment will form the base for development of the Blueprint. The Blueprint will serve as the guide for implementation of the Treaty.

The Technical Expert and the Legal Expert will closely coordinate with the RAI Secretariat in performing their activities and will jointly produce the Assessment Report & Blueprint. Recommendations in the Assessment Report & Blueprint document will be aligned with the relevant international standards and the GRECO recommendations stemming from the fourth round and fifth round evaluations of asset declarations in beneficiary states.

The main beneficiaries of the Assessment Report & Blueprint are the RAI Secretariat and the Programme beneficiary jurisdictions.

4. DATA COLLECTION METHODS

4.1 DESK RESEARCH

4.1.1 LEGAL

The Legal Expert will examine the legal framework for collection, verification and exchange of data in the region through the following activities:

- Determining the scope of the legal framework in each beneficiary jurisdiction in order to create an outline for the Assessment Report & Blueprint;
- Analysis of the legislation in beneficiary jurisdictions (laws and by-laws);
- Comparative analysis of laws, by-laws and the form and content of asset declarations.

The Legal Expert will use information and documentation provided by the RAI team and that available on the websites of national ministries or anticorruption agencies in charge of asset declaration collection, verification, disclosure and exchange of data.

4.1.2 TECHNICAL

In the inception phase, the Technical Expert examined and analysed the information and documentation provided by the RAI team and that available on the websites of national ministries or anticorruption agencies in charge of asset declaration collection, verification, disclosure and data exchange related to technical aspects of this process. The Technical Expert has also analysed the availability of horizontal building blocks such as the interoperability platform (Government Service Bus), eID provider and emailbox service in each beneficiary jurisdiction. These building blocks, where available, should be treated as primary implementation mechanisms for electronic exchange of data between asset declaration information systems and national electronic registries used in the asset verification process. Special attention was paid to up-to-date information on the availability of registers commonly used to verify the data stated in asset declarations (real estate, tax administrations, business register, register of securities, register of bank accounts, etc.) for the purposes of data exchange with national anti corruption agencies or national interoperability platforms of the Parties of the Treaty.

4.1.3 DOCUMENTS PROVIDED BY THE RAI SECRETARIAT

The RAI Secretariat has shared the following documents in July 2023:

- International Treaty on Exchange of Data for the Verification of Asset Declarations
- Explanatory Notes to the International Treaty on Exchange of Data for the Verification of Asset Declarations
- SEE-TAC Project Document
- ReSPA Feasibility Study on the international instrument on data exchange for income and asset declarations, including a draft Model Memorandum of Understanding on Data Exchange
- Agendas, conclusions and participant lists for meetings held during the development of the Treaty.

4.2 QUESTIONNAIRES

4.2.1 LEGAL

The Legal Expert prepared a detailed legal questionnaire foreseen as the primary data collection method regarding the legal competences of the competent authority, as well as the process of implementation of the Laws and by-laws governing asset declaration data collection, verification and exchange at the national and regional level.

The content of the questionnaire includes:

- General information about the institution
- Contact persons
- Employees in the Legal or other relevant department/unit
- Competences related to asset declaration
- Information concerning the relevant legislation (laws and by-laws) on asset declaration data collection, verification and exchange at both the national and regional level
- Details about the format and content of asset declarations
- Information about publication of asset declaration information/data according to the law
- Additional information or comments.

The questionnaire is included in Annex 1 to the Inception Report. It will be shared with contact persons in Focal Points - competent authorities in the beneficiary jurisdictions. These bodies will be kindly asked to complete the questionnaire or provide any legal acts (by-laws/forms) relevant for successful completion of this assignment.

4.2.2 TECHNICAL

The Technical Expert prepared the detailed technical questionnaire foreseen as the primary method of data collection on technical and IT governance capacities for asset declaration data collection, verification and exchange at both the national and regional level.

The questionnaire covers the following aspects of technical and IT governance:

- General information on the Focal Point institution
- Contact persons
- Human resources responsible for ICT management and support
- ICT infrastructure, including networks, data centre and system infrastructure
- Asset declaration information system, including general information, key software components/features supported and data exchange interfaces with external systems
- ICT governance
- Annual budget for supply and maintenance of ICT equipment and software
- Information security
- E-government status in beneficiary states

The questionnaire is enclosed in Annex 1 to the Inception Report. Questionnaires were shared with contact persons in Focal Points - competent bodies in beneficiary jurisdictions and, if feasible, with national bodies competent for E-Government or the national registers relevant for

asset verification. These bodies were kindly asked to complete the questionnaire or provide any technical documentation relevant for successful completion of this assignment.

The following institutions returned the completed questionnaires:

- High Inspectorate of Declaration and Publication of Assets and Conflicts of Interests of Albania
- Agency for Prevention of Corruption of Kosovo*
- Agency for Prevention of Corruption of Montenegro
- State Commission for Prevention of Corruption of North Macedonia

The Agency for Prevention of Corruption of the Republic of Serbia did not complete the questionnaire, but it provided the most of relevant information to the Technical Expert during the semi-structured interview held at the Agency on 31 October 2023.

4.3 FIELD MISSIONS/ONLINE MEETINGS – SEMI-STRUCTURED INTERVIEWS

The Legal Expert, the Technical Expert and the representatives from the RAI Secretariat conducted on-site[5] or online[6] meetings with the representatives of institutions competent for collection, verification, disclosure and exchange of asset declaration data, as well as representatives of institutions in charge of maintenance of national registers used in the asset verification process. The primary objectives of these meetings were:

- to get a clear picture of the whole process, regarding implementation of laws and bylaws, technical capacities and the available legal options for implementation of the Treaty.
- to cross-check information provided in the technical and legal questionnaire, or to complete the questionnaire during the semi-structured interview if the competent body did not return the completed questionnaire prior to the field mission.
- to verify the existence of legal, semantic and technical interoperability infrastructure in the country and of electronic registries that can be reused for the asset verification process at the regional level.

In online interviews or field missions the experts insisted on meetings with high-ranking officials in order to establish their readiness to support and sponsor the activities required to achieve the objectives of the Regional Programme.

In these meetings and while leveraging other data collection methods, the experts paid special attention to the following aspects of the process of collection, verification, disclosure and exchange of asset declaration data at the regional level:

- Project sponsorship (ability of the competent body's management to drive the change management process needed to implement specific actions)
- IT infrastructure readiness

[5] On-site meetings were held in Bosnia and Herzegovina, Montenegro, North Macedonia, Albania and Serbia.
[6] Online meetings were held with the representatives of competent institutions in Kosovo* and Moldova.

- Architecture of the existing information systems for asset declaration and verification and their capability to exchange data with the relevant national registries or competent bodies in other beneficiary jurisdictions
- Existence of an interoperability platform (Government Service Bus) and identity providers at the national E-Government level, including accessibility of the relevant electronic registries on the Government Service Bus. Publication of electronic registries on the Government Service Bus can make technical implementation of the data exchange process (especially asset verification) between beneficiary jurisdictions much easier.
- Applied technical and organizational personal data protection measures in the relevant information systems.
- Sustainability (competent body's ability to provide human resources to manage both the information system and the data exchange infrastructure and the funds for system maintenance in the post implementation phases)

Information gathered, analysed and structured in the Desk research and Interim phase served as a sound basis for preparation of a draft Assessment with Blueprint.

5. REGIONAL OUTLOOK

5.1 eIDAS

eIDAS stands for electronic Identification, Authentication and Trust Services. This European regulation established a single framework for electronic identification (eID) and trust services, making it more straightforward to deliver services across the European Union.

eIDAS promoted interoperability across the 27 EU Member States, ensuring that countries mutually recognise each other's notified electronic identification schemes. It also ensures that the trust services provided by service providers compliant with the Regulation can be accepted as evidence in legal proceedings.

"Digital identity" and "electronic identity" (eID) are used as synonymous. An eID is a means for a person to prove who they are and on this basis gain access to online services. An eID can be associated with one of three contexts

- Natural person (physical person, a citizen in public-sector terminology)
- Legal person (owner or representing an organization)
- Natural person representing a legal person (normally an employee in an organization acting in a specific role)

Identity proofing is the process of verifying the identity of a natural or legal person. Once the natural or legal person passes identity proofing at the requested assurance level[7], the selected identification means must be bound to the person that is the subject of identity proofing.

Authentication is required when a user, via an eID, requests access to Service Provider resources requiring authentication of a certain level of assurance.

eID access to services is nearly always of a synchronous character, where validation of the eID takes place at a specific point in time.

Authentication proves that the user possesses the required identification means, at a point in time, in order to reach a requested assurance level. The identification means was associated to the user during the identity proofing and enrolment process.

Typical identification means are the password, hardware token (e.g. OTP or FIDO tokens), mobile app or a smartcard. Identification means are used on their own or in combination with other identification means. The assurance level obtained by the authentication process depends on the strength of the identification means and the enrolment process. Identification means constitute one or more of the three authentication factors: Possession, Knowledge and Inherence.

[7] eIDAS defines three assurance levels: Low: for instance, enrolment is performed by self-registration in a web-page, without any identity verification; Substantial: for instance, enrolment is performed by providing and verifying identity information, and authentication using a user name and a password and a one-time password sent to your mobile phone; High: for instance, enrolment is performed by registering in person in an office, and authentication by using a smartcard, like a National ID Card.

Trust services under the eIDAS Regulation are:

- Electronic signature (eSignature): the expression in an electronic format of a person's agreement to the content of a document or set of data. Qualified eSignatures have the same legal effect as handwritten signatures.
- Electronic seal (eSeal): similar in its function to the traditional stamp. It can be applied to an electronic document to guarantee the origin and integrity of a document.
- Electronic Timestamp (eTimestamp): links an electronic document to a particular time, providing evidence that the document existed at that time.
- Website Authentication Certificates (WACs): electronic certificates that prove to users that the website is trustworthy and reliable. They ensure that the website is linked to the person to whom the certificate is issued. They also help to avoid data phishing.
- Electronic Registered Delivery Service (eDelivery): allows the user to send data electronically. It provides proof of sending and delivery of the document and protects organizations against the risk of loss, theft, damage or unauthorised alteration.ž

5.2 GDPR

The General Data Protection Regulation (GDPR) (EU) 2016/679 Regulation of the European Union was adopted in March 2016 (entered into force in May 2018) to regulate the protection of personal data and privacy of persons within the European Union, as well as transfer of data to third countries in new circumstances conditioned by technological development and the emergence of new methods of processing personal data. The GDPR regulation defines the scope, harmonizes regulations and establishes bodies and mechanisms for monitoring the implementation of the Directive, promotes accountability and transparency in personal data processing, prescribes a framework for further strengthening and enforcing of technical and organizational measures for personal data protection and very severe sanctions for violators.

According to the GDPR, personal data is any information that relates to an individual who can be directly or indirectly identified. Data processing is any action performed on data, such as collecting, recording, organizing, structuring, storing, using, erasing, whether automated or manual. Data subject is the person whose data is processed. Data controller is the person who decides why and how personal data will be processed. Data processor is a third party that processes personal data on behalf of a data controller.

The regulation applies if the data controller or processor, or the data subject, is based in the EU. Under certain circumstances, the regulation also applies to organisations based outside the EU if they collect or process personal data of individuals located inside the EU. The regulation does not apply to the processing of data by a person for a "purely personal or household activity and thus with no connection to a professional or commercial activity."

GDPR proclaims the following data protection principles:

- Lawfulness, fairness and transparency — Processing must be lawful, fair and transparent to the data subject.

- Purpose limitation — Personal data must be processed for the legitimate purposes specified explicitly to the data subject when it is collected.
- Data minimization — Organization should collect and process only as much data as absolutely necessary for the purposes specified.
- Accuracy — Personal data must be kept accurate and up to date.
- Storage limitation —Personally identifying may only be stored for as long as necessary for the specified purpose.
- Integrity and confidentiality — Processing must be done in such a way as to ensure appropriate security, integrity and confidentiality (e.g. by using encryption).
- Accountability — the data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

Data subjects' privacy rights, according to the GDPR, are

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Chapter V of the GDPR forbids the transfer of personal data of EU data subjects to countries outside the EEA — known as third countries — unless appropriate safeguards are imposed, or if the third country's data protection regulations are formally considered adequate by the European Commission (Article 45). Binding corporate rules, standard data protection contractual clauses issued by a Data Processing Agreement (DPA), or a scheme of binding and enforceable commitments by the data controller or processor situated in a third country, are some of the examples.

Not every data controller or processor needs to appoint a Data Protection Officer (DPO). There are three conditions under which you are required to appoint a DPO:

- The organization is a public authority other than a court acting in a judicial capacity.
- Organization's core activities require systematic and regular monitoring of people on a large scale.
- Organization's core activities are large-scale processing of special categories of data listed under Article 9 of the GDPR or data relating to criminal convictions and offenses from the same Article.

5.3 NIS2

The Network and Information Security Directive introduced in 2016 was the first legislative framework of the European Union that regulates specific aspects of protection against cyber attacks, such as:

- Establishment of one or more national competent authorities and CSIRTs and designation of a single national contact point;
- Adoption of national strategies for cyber security of network and information systems;
- Identifying key service providers in key sectors (energy, transport, finance, banking, health, water and digital infrastructure, where a cyber attack would disrupt a key service;
- Promoting a culture of risk management in accordance with information security standards;
- Determining reporting obligations in case of incidents or cyber attacks;
- Improving cooperation at the EU level through the establishment of a cooperation group and a network of CSIRTs;
- Imposing the obligation to sanction in order to ensure the effectiveness of the measures envisaged in the NIS Directive.

EU cybersecurity rules introduced by the NIS Directive in 2016 were updated by the Directive on measures for a high common level of cybersecurity across the Union (hereinafter: *NIS2 Directive*), which came into force in 2023. It modernised the existing legal framework to keep abreast of increased digitisation and an evolving cybersecurity threat landscape. By expanding the scope of cybersecurity rules to cover new sectors and entities, it further improves the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole. The NIS2 Directive provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:

- Member States' preparedness, by requiring them to be appropriately equipped. For example, with a Computer Security Incident Response Team (CSIRT) and a competent national Network and Information Systems (NIS) authority,
- cooperation between all Member States, by means of setting up a Cooperation Group to support and facilitate strategic cooperation and exchange of information among Member States.
- a culture of security across sectors that are vital for our economy and society and that rely heavily on ICT, such as energy, transport, water, banking, financial market infrastructure, healthcare and digital infrastructure.

Businesses identified by the Member States as operators of essential services in the above sectors will have to take appropriate security measures and notify relevant national authorities of any serious incidents. Key digital service providers, such as search engines, cloud computing services and online marketplaces, will have to comply with the security and notification requirements under the Directive.

6. ANALYSIS OF THE CURRENT SITUATION PER JURISDICTION

6.1 Albania

6.1.1 Legal

6.1.1.1 Competent authority

The High Inspectorate for the Declaration and Audit of Assets and Conflicts of Interest (HIDAACI) is an independent institution, established by law, under parliamentary control. It started to operate in 2003, pursuant to the Law no. 9049 of 10.04.2003 "On the Declaration and Audit of Assets, Financial Obligations of the Elected Persons and Certain Public Officials" (Law no. 9049/2003).

HIDAACI, pursuant to Article 16 of this Law, is a public juridical person which, under the responsibility of the Inspector General, administers the declaration of assets, financial liabilities and conducts audits of such declarations according to the specifications provided in Law no. 9049/2003, as amended, the Law on Prevention of Conflict of Interest in the Exercise of Public Functions and the Code of Administrative Procedure.

Competences

The High Inspectorate has the following competences:

- conduct direct audits of declarations in its designation;
- collect data, conduct administrative audit and investigation of declarations of persons under obligation to declare according to Law no. 9049/2003, in conformity with the Code of Administrative Procedure. Data collection is carried out in accordance with the legislation applicable to the protection of personal data, as well as legislation applicable to classified information.
- cooperate with state institutions' authorities responsible for implementation of Law no. 9049/2003, Law on Prevention of Conflict of Interest in the Exercise of Public Functions and the Law on Whistle-Blowing and Protection of Whistle-Blowers.
- cooperate with audit bodies and other structures responsible for the fight against corruption and economic crime;
- cooperate with other institutions according to the provisions of applicable legislation.

6.1.1.2 Legal framework

- Law no. 9049 of 10.4.2003, "On the Declaration and Audit of Assets, Financial Obligations of Elected Persons and Certain Public Officials", as amended by the following laws: no. 9367 of 7.4.2005; no. 9475 of 9.2.2006; no. 9529 of 11.5.2006; no. 9530 of 11.5.2006; no. 9584 of 17.7.2006; no. 85/2012 of 18.9.2012; no. 45/2014 of 24.4.2014; no. 42/2017 of 6.4.2017; no. 105/2018 of 13.12.2018.

The purpose of this law is to determine the rules for declaration and auditing of assets, legitimacy of their sources of origin, financial obligations for elected officials, civil servants, their families and related persons.

According to this law, HIDAACI has the competence to: collect data, carry out administrative inquiries and investigations of declarations of persons under obligation to declare, in conformity with the Code of Administrative Procedure. Data collection is carried out in accordance with the legislation applicable to the protection of personal data, as well as with the legislation applicable to classified information.

Declarants

Article 3 of this Law stipulates the persons under the obligation to declare.

The obligation to periodically file a declaration with the High Inspectorate for the Declaration and Audit of Assets and Conflict of Interest shall be borne by:

a) The President of the Republic, members of Parliament, Prime Minister, Deputy Prime Minister, ministers and deputy ministers;
b) Judge of the Constitutional Court, Chairman of High State Control, Prosecutor General, Peoples' Advocate, members of the Central Election Commission, member of the High Judicial Council, member of the High Prosecutorial Council, High Justice Inspector and inspectors of the High Justice Inspectorate, Inspector General of the High Inspectorate for the Declaration and Audit of Assets and Conflict of Interest;
c) High and middle level management officials according to the civil servants' legislation in force, excluding the local self-government bodies;
ç) Prefects, heads of regional councils and mayors;
d) Directors and commanders of Armed Forces at the Ministry of Defence and the National Intelligence Service;
dh) Prosecutors, judges and the General Director of the Judicial Bailiff Service and directors of the bailiff offices within the jurisdiction of every district court of first instance;
e) Directors of independent public institutions and members of regulatory bodies;
ë) The General Director and Deputy Director of the State Police, directors general of the State Police, directors of departments at the General Directorate of State Police, directors at the local directorates of the State Police, head and officers of the judicial police of the National Investigation Bureau, judicial civil servants at anti-corruption and organized crime courts, as well as administrative personnel at the Special Prosecution Office.
f) The General Director, Deputy General Directors, directors of departments at the central and regional level in the General Tax Directorate, General Customs Directorate and the General Directorate for Prevention of Money Laundering;
g) Directors at all levels in the property restitution and compensation, privatization and property registration structures;
gj) Officials, elected and appointed by the Assembly, the President of the Republic, Prime Minister, ministers or equivalent persons;
h) Governor of the Bank of Albania, the deputy and the members of its Supervisory Board;
i) Directors of public institutions under the central institutions at the regional level;

j) Administrators of joint stock companies with state capital share greater than 50 percent and more than 50 workers.

2. The obligation to declare shall be borne even by persons who, under Article 9 of this Law, have the obligation to make a declaration upon request.

2/1. The obligation to declare shall be borne even by subjects set out in Articles 26 and 27 of the Law no. 84/2016 "On transitory re-evaluation of the judges and prosecutors in the Republic of Albania".

3. The Assembly, by its own decision and upon proposal of the Inspector General, imposes the obligation to declare assets to other functions not provided for in this Law.

Declarants	
President of the Republic, members of Parliament, Prime Minister, Deputy Prime Minister, ministers and deputy ministers	Judge of the Constitutional Court, Chairman of High State Control, Prosecutor General, Peoples' Advocate, members of the Central Election Commission, member of the High Judicial Council, member of the High Prosecutorial Council, High Justice Inspector and inspectors of the High Justice Inspectorate, Inspector General of the High Inspectorate for the Declaration and Audit of Assets and Conflict of Interest
High and middle level management officials according to the civil servants' legislation in force, excluding the local self-governing bodies	Prefects, heads of regional councils and mayors
Directors and commanders of Armed Forces in the Ministry of Defence and the National Intelligence Service	Prosecutors, judges and the General Director of the Judicial Bailiff Service and directors of the bailiff offices in the jurisdiction of each district court of first instance
Directors of independent public institutions and members of regulatory bodies	General Director and Deputy Director of the State Police, directors general of the State Police, directors of departments at the General Directorate of State Police, Directors of the local directorate of the State Police, head and officers of judicial police of the National Investigation Bureau, judicial civil servants in anti-corruption and organized crime courts, as well as administrative personnel in the Special Prosecution Office
General Director, deputy general directors, directors of departments at the central and regional level in the General Tax Directorate, General Customs Directorate and the General Directorate for Prevention of Money Laundering	Directors at all levels in property restitution and compensation, privatization and property registration structures
Officials, elected and appointed by the Assembly, the President of the Republic, Prime Minister, ministers or equivalent persons	Governor of the Bank of Albania, the deputy and the members of its Supervisory Board
Directors of public institutions under the central institutions at the regional level	Administrators of joint stock companies with state capital share greater than 50 percent and with more than 50 workers

Additionally, Article 3/1 of the Law 9049 of 10.4.2003, was added as follows:

Article 3/1
Declaration of assets for the candidates for different positions in the institutions of the justice system

1. The obligation to declare private assets and interests shall be borne by:
a) candidates who express interest in the vacancies in the Constitutional Court, according to the provisions of the legislation regulating the governance of the justice system;
b) candidates who express interest in the position of High Justice Inspector and non-magistrate candidates for the position of inspector attached to the Office of High Justice Inspector according to the provisions of the legislation regulating the governance of the justice system;
c) candidates to be admitted to the initial training of the SoM, as well as the graduates applying for appointment as magistrates, according to the provisions of the legislation regulating the status of judges and prosecutors;
ç) candidates for the position of judges and judicial civil servants in specialized anticorruption and organised crime courts, including their close family members, according to the legislation regulating the organization and functioning of institutions for the combat against corruption and organized crime;
d) candidates for the position of prosecutor, investigation officer, administrative staff of the Special Prosecution Office, Special Investigation Unit, including their close family members, according to the legislation regulating the organization and functioning of institutions for the combat against corruption and organized crime;
dh) candidates who, according to the legislation regulating the status of judges and prosecutors, request promotion to higher or specialized levels;
e) candidates for members of the High Court coming from the ranks of distinguished lawyers, according to the provisions of the legislation regulating the status of judges and prosecutors;
ë) candidates for the position of chairperson of courts or other prosecution offices, according to the provisions of the legislation regulating the status of judges and prosecutors;
f) any other person subject to the obligation to declare prior to candidacy, in accordance with the legislation in force.

2. Candidates for the positions mentioned in paragraph 1 of this Article, who are under the obligation to declare private interests according to the provisions of Article 3 of this Law, shall not submit a new declaration but shall undergo a full asset audit. If, within 180 days prior to his/her submission of the application, the candidate underwent an audit by the High Inspectorate for the Declaration and Control of Assets and Conflict of Interest that has not resulted in adverse findings, then the control shall be considered as conducted.

3. The High Inspectorate shall conduct a full audit to verify the accuracy and authenticity of the data in the declaration of persons from point 1 of this Article within 2 months from the submission of the declaration, unless otherwise provided in the law. Upon completion of the verification, the Inspector General shall immediately send the verification report to all relevant institutions.

Asset declaration – forms and content

The official document "Declaration of Private Interests" was approved by Order no. 926 of 29.10.2021 “On the approval of the forms of the declarations of private interests”. [8]

The declaration of assets, their sources and financial liabilities is made according to the requirements specified in the Law and in the form determined by the Inspector General.

The declaration includes assets of the public official and their family (husband/wife, cohabitant and adult children), sources of origin and financial liabilities of the person. The declaration must also indicate whether the declarant has any other related persons or not.

The declaration should be completed only electronically, by the public official and signed by him/her, as well as by the person related to him/her (spouse, cohabitant and/or adult children) when assets are separately owned and registered to their name.

For that purpose, HIDAACI has established the Electronic Asset Declarations and Conflict of Interest System (EACIDS). [9]

There are 5 (five) types of declarations of private interests provided by the Law no. 9049/2003 *“On the declaration and control of assets and financial obligations of elected persons and certain public officials”,* as amended and the Order of the Inspector General no. 223 of 9.5.2017 “*On the approval of private interest declaration forms*” and the Order of the Inspector General no. 284 of 9.5.2017 “*On the approval of asset and private interest declaration forms for the candidates for different positions in the justice system”*, as follows:

- *Declaration of Private Interests Prior to Start of Employment*[10]

After taking up public office, within 30 days from the start date of employment, all persons under the obligation to declare private interests and their related persons should complete the Declaration of Private Interests Prior to Start of Employment.


REPUBLIKA E SHQIPËRISË
INSPEKTORATI I LARTË I DEKLARIMIT DHE KONTROLLIT TË PASURIVE DHE KONFLIKTIT TË INTERESAVE

DEKLARATË E INTERESAVE PRIVATË PARA FILLIMIT TË DETYRËS

AUTORIZIM
PËR KONTROLLIN E DEKLARATËS SË INTERESAVE PRIVATË

This form of declaration includes the declarant’s assets as well as those of his/her family (spouse, cohabitant and adult children), sources of acquisition and financial liabilities. This declaration also indicates if the declarant has any related persons or not. Article 22 of the Law no. 9049/2003 sets out the asset declaration procedure for declarant’s family members.

According to Article 4 of the Law no. 9049/2003, all persons identified in Article 3 shall declare, by the 31st of March every year and for as long as they hold their office, the status of their private interests inside

[8] https://www.ildkpki.al/gloolsys/2021/11/Urdher-Nr.926-date-29.10.2021.pdf
[9] https://www.ildkpki.al/
[10] https://www.ildkpki.al/deklarata-para-fillimit-te-detyres-new/

and outside the country, sources of origin and their financial obligations as at 31st of December of the previous year:

Declaration of Private Interests – content	
Immovable assets and all any related rights according to the Civil Code	Movable assets that must be registered in public registers and any related rights according to the Civil Code
Valuables with a value of more than 300.000 ALL	Value of shares, securities and capital shares in their possession
Value of liquid assets, amounts of cash outside the banking system, in bank accounts, deposits, money lent out, treasury bills, held in ALL or foreign currency	Financial obligations towards legal or natural persons, in ALL or foreign currency
Annual personal income, from salary or participation in boards, commissions or any other activity that generates personal income	Licenses and patents that generate income
Gifts and preferential treatment, including the identity of the legal or natural person that is the source of the gifts and/or preferential treatment. Gifts and preferential treatments valued at less than 10,000 ALL and multiple gifts or preferential treatments from the same person that do not exceed that amount in aggregate across the declaration period, are excluded	Engagement in private activities with the aim to generate profits or any other activity that generates income, as well as any income generated from said activity
Private interests of the person derived from, containing or merged with family or cohabitation relationships	All declarable expenses amounting to more than 300.000 ALL made in the year of declaration

- *Annual/Periodic Declaration of Private Interests*[11]

All officials and other related persons under the obligation to declare must submit the Annual/Periodic Declaration by the 31st of March each year.

The Periodic Declaration includes only changes in the previously declared assets, financial obligations and private interests that occurred in the declaration year and any earned income and declarable expenses for the entire year of the declaration.


REPUBLIKA E SHQIPËRISË
INSPEKTORATI I LARTË I DEKLARIMIT DHE KONTROLLIT TË PASURIVE DHE KONFLIKTIT TË INTERESAVE

DEKLARATË E INTERESAVE PRIVATË
PERIODIK / VJETOR

AUTORIZIM
PËR KONTROLLIN E DEKLARATËS SË INTERESAVE PRIVATË

[11] https://www.ildkpki.al/deklarata-periodike-vjetore-new/

- *Declaration of Private Interests After Leaving Public Office*[12]

In case of leaving or removal from office, not later than 15 days from the date of leaving or being removed from office the public official and other related persons are required to complete the Declaration of Private Interests After Leaving Public Office.

This declaration includes only the changes in assets, financial obligations and private interests that occurred in the period between the last declaration and the date of leaving the office/duty.


REPUBLIKA E SHQIPËRISË
INSPEKTORATI LARTË I DEKLARIMIT DHE KONTROLLIT TË PASURIVE
DHE KONFLIKTIT TË INTERESAVE

DEKLARATË E INTERESAVE PRIVATË
PAS LARGIMIT NGA FUNKSIONI

AUTORIZIM
PËR KONTROLLIN E DEKLARATËS SË INTERESAVE PRIVATË

- *Declaration of Private Interests Upon Request*[13]

This form of declaration is requested by the Inspector General. This declaration differs from other declarations of private interests submitted by officials and their related persons (spouse, cohabitant, adult children) in line with the terms provided by the law, as it is made only upon request from the Inspector General.


DEKLARATË E INTERESAVE PRIVATE
ME KËRKESË

AUTORIZIM
PËR KONTROLLIN E DEKLARATËS SË INTERESAVE PRIVATE

This request is addressed to individuals, natural or legal persons, who are not declarants under the law no. 9049/2003 when the verification of Declarations of Private Interest, i.e. a full audit or administrative investigation of the Declaration of Private Interests of an official and his/her related person, determines that a contribution from another individual, natural or legal person was stated as the source of origin for their private interests. Under these circumstances, the latter are deemed as related persons and are called, based on the order issued by the Inspector General, to complete and submit the *Declaration of Private Interests Upon Request*. This declaration shall be submitted according to the terms foreseen in the request and shall be further processed and audited for accuracy.

- *Declaration of Assets and Private Interests of Candidates for Different Positions in the Justice System*

[12] https://www.ildkpki.al/deklarata-pas-largimit-nga-funksioni-new/
[13] https://www.ildkpki.al/deklarate-me-kerkese/

Since 2016, HIDAACI is also involved in the re-evaluation (vetting) process for judges and prosecutors as provided by the Law on "*Transitional re-evaluation of judges and prosecutors*". This law, approved as part of the comprehensive justice reform in Albania, aims, *inter alia*, to ensure the proper functioning of the rule of law in Albania, the independence of the justice system as well as well as restoration of the public confidence in these institutions.

REPUBLIKA E SHQIPËRISË
INSPEKTORATI I LARTË I DEKLARIMIT DHE KONTROLLIT TË PASURIVE DHE KONFLIKTIT TË INTERESAVE

DEKLARATË E PASURISË DHE INTERESAVE PRIVATË
E kandidatit për pozicione të ndryshme në institucionet e sistemit të drejtësisë

AUTORIZIM
PËR KONTROLLIN E DEKLARATËS SË PASURISË DHE INTERESAVE PRIVATË

Emri | Atësia | Mbiemri

Kandidat për

Institucioni dhe adresa

Data e dorëzimit të deklaratës

Autorizoj:

Nënshkrimi i Kandidatit

This form of declaration includes the assets of the candidate for different positions in the justice system as well as those of his/her family (spouse, cohabitant and adult children), their sources of origin and the financial obligations of the candidate. This form of declaration includes the declaration of assets and private interests of any related persons.

All declarations shall be accompanied by the declarant's authorization in which they authorize HIDAACI to verify all their declarations by gathering information from any private or public organizations, either financial or non-financial.

Data publication

The information provided in the declarations is made public based on the Law no. 9049/2003 *"On the declaration and control of the assets and financial obligations of elected persons and certain public officials",* as amended, taking into consideration the legal provisions on the protection of personal and sensitive data, which shall be manually redacted prior to publication.

Currently, Declarations of Private Interests are published upon third party requests for information. Personal and sensitive information in declaration forms is manually redacted prior to disclosure, in accordance with the appropriate legislation in force.

HIDAACI follows an open and transparent policy towards citizens, the media and the civil society. In the period 2014-2022, a total of 66,204 declarations were published, of which 4271 Declarations of Private Interests for the year 2022.

Article 34 "*Publication*" of the Law no. 9049/2003 *"On the declaration and control of the assets and financial obligations of elected persons and certain public officials",* as amended, states:

"1. The data collected by the declaration, according to this law, shall be available to the public only in accordance with the legislation applicable to the right to information on official documents and protection of personal data.

2. Private interest declarations shall be official documents and shall be published on the official website of the High Inspectorate, with confidential, personal data edited in compliance with the effective legislation on the right to information and protection of personal data.

3. Data collected from public and/or private institutions during an audit, re-audit of private interest declarations or during an administrative investigation shall be used only for the purposes of this law and there must not be any unauthorized publication or dissemination of such data as

that would go against this law and the effective legislation on the publication and processing of personal data."

The Decision of the Albanian Constitutional Court no. 16 of 11.11.2004 states: "... *as a rule, it is made public, what constitutes the essence of the information on the assets and their sources declared by the relevant subject, without going into unnecessary details or elements of the declaration which could be used (with regard to verification and control) by the High Inspectorate of the Declaration and Audit of Assets or to other public authorities, but which in themselves do not represent public interest ….*"

The High Inspectorate for the Declaration and Audit of Assets and Conflict of Interest publishes only private interests' declaration data which are not confidential and are a matter of public interest.

The process of publication of declarations of private interests will be improved with the introduction of the electronic system. Pursuant to Article 42/1 point 5 of the Law no. 9049/2003, publication of declarations of private interests according to point 2 article 34 of the Law no. 9049/2003 shall be carried out after the preparation and commissioning of the necessary infrastructure by HIDAACI. Once the electronic system becomes functional, declarations of private interests will be published by default. To this end, HIDAACI has created a special menu on its website dedicated to the declaration platform and publication of declarations (https://www.ildkpki.al/publikimi-en/?lang=en).

Data verification

The audit process is initiated by order of the Inspector General and is conducted by HIDAACI inspectors and assistant inspectors. After the order is issued, inspectors and assistant inspectors initiate the process by dispatching requests for information regarding the subject's private interests to all relevant private and public institutions.

After gathering responses from the competent institutions, the inspector performs a full audit and financial analysis of the declarations of private interests by cross-checking the information. The entire audit process is based on the Code of Administrative Procedure which dictates that for any issues identified in the audit HIDAACI summons the subjects to the institution's premises and presents the identified issues that must be addressed, thus providing a lawful possibility to present explanations and evidence in relation to the findings of the full audit or evidence to support their declaration (article 27 of the Law no. 9049/2003). After this step, if the audit still ends with identified breaches of the Law, the Inspector General shall take appropriate measures, which may include administrative fines (article 40 of the Law no. 9049/2003), referral to the competent institution for potential breaches of other laws (for example breach of tax laws, as set out in Article 32 of the Law no. 9049/2003), as well as referral to the State Police or the Prosecution Office in case of suspected criminal offences. Article 25 of the Law no. 9049/2003 sets out types of controls performed by HIDAACI inspectors.

Preliminary control (formal control) consists mainly of verification of the jurisdiction and verification of all the data necessary for the declaration of private interests. In case of missing information or substantial errors, HIDAACI notifies the appropriate declarant to make the necessary corrections within the legal deadline of 15 days. (Article 24, Law no. 9049/2003).

Arithmetic and logic control is performed after the formal control. During this type of control HIDAAC inspectors inspect the substance of the declaration of private interest form. The main

aim is to verify the correctness of declared assets, accuracy of the declared legitimate financial sources, as well as whether the assets are adequately covered by the declared sources. This type of control is carried out by HIDAACI within the calendar year of submission of the declarations of private interests.

The full audit aims to verify the authenticity and accuracy of the data provided in the declaration of private interests.

After gathering the responses from the competent institutions, the inspector performs the full audit and financial analysis of declarations of private interests by cross-checking the information. (Please refer to point 7 above).

The complete audit consists not only in crosschecking the declared data with the responses of the competent institutions, but also in identifying private interests that have not been declared, or lack of financial sources for the declared assets, identification of conflicts of interests, etc.

With the initiation of a complete audit, a full practice of requests directed to various competent private and public institutions is sent out. These institutions include but are not limited to:

- The National Bank of Albania;
- All second-tier banks;
- Leasing, investment and other financial institutions;
- The General Directorate for Road Transport Services (which maintains the register of registered road vehicles);
- National Business Centre (which maintains the register of all commercial legal and natural persons);
- General Directorate of Taxes (which maintains all information relate to payment of taxes and tariffs, as well as profit statements of commercial entities);
- Electricity Distribution Operator (which maintains the register of household electricity supply contracts);
- General Maritime Directorate (which maintains the register of marine vehicles);
- State Cadastral Agency (which maintains ownership records for immovable assets and land).

For the purposes of verification of conflicts of interest, information may also be required from other institutions.

The obligation of these public and private institutions derives from the provisions of Article 26 of the Law no. 9049/2003, which states that for the purposes of audit and verification of declarations HIDAACI has the right to verify the data in the entire state and public apparatus, as well as data held by public and private legal persons. According to the same Article, all the above subjects have an obligation to provide the requested data in their possession within 15 days from the request issued by the Inspector General. If the public of private entities fail to provide the required information, the law provides for imposition of administrative fines.

One of the aims of HIDAACI activities is to increase international cooperation in order to obtain data for particular control cases where reasonable grounds exist to believe that a part of the hidden assets is outside Albania and has not been declared.

HIDAACI considers the Law on the Right to Information and the Law on Data Protection and its internal regulation. Moreover, the internal regulation of the High Inspectorate of the Declaration and Audit of Assets and Conflicts of Interest, provides the obligation of each employee to protect the confidentiality of the information under his/her possession. Breach of this obligation is considered a disciplinary measure.

Data Protection

- Law No 9887 of 10.03.2008 "On Protection of Personal Data", amended by Law no. 48/2012, date 26.04.2012, amended by Law no.120/2014

Law 9049/2003, in the first chapter "*General dispositions*", Article 2 "*Definitions*" point 9 refers to legislation on data protection - Law on "Data Protection" (Law no. 9887/2008) - and incorporates the same definitions of the terms "*personal data*" and "*data processing*".

Data collection, verification and exchange is carried out in accordance with the legislation applicable to the protection of personal data, as well as with the legislation applicable to classified information.

Additionally, cooperation agreements between HIDAACI and other institutions specifically provide for data protection and privacy of individuals' asset declaration information during the data collection, verification and exchange processes.

In relation to the above, the High Inspectorate's controller takes appropriate organizational and technical measures to protect personal data from unlawful, accidental destruction, accidental loss, access or dissemination by unauthorized persons, especially when the data processing is done in the network and from any other form of unlawful processing in accordance with the legislation on protection of personal data.

The applicable legislation in this field is fully approximated with the EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The entry into effect of Directive (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR) on 25 May 2018 repealed the previous Directive.

Because of the necessity to guarantee the same European personal data protection standards for Albanian citizens, the Commissioner's Office (Information and Data Protection Commissioner) intensified its efforts regarding approximation of the Albanian legislation with the GDPR through preparation of the draft Law "On Personal Data Protection", which has not been adopted yet.[14]

6.1.2 Technical

6.1.2.1 IT infrastructure

The information system for collection and verification of asset declaration data and supporting IT services are hosted in the High Inspectorate of Declaration and Publication of Assets and Conflicts of Interests (hereinafter: HIDAACI).

[14] https://www.idp.al/wp-content/uploads/2016/11/ENGLISH_Strategjia-Institucionale-2022-2025_revised.pdf

The HIDAACI data processing facility (hereinafter called data centre) is located on its premises. Equipment in the data centre is surge-protected by a central UPS device and a generator that provides backup power in case of a mains power outage. Cooling of the data centre equipment is performed by air-conditioning systems. Technical protection of the data centre is achieved by the video surveillance and electronic access control system. The data centre has a fire alarm system and a fire extinguishing system.

Hardware and network infrastructure in the main data centre consists of:

- Servers - virtualization hosts
- Storage systems connected with servers
- Top-of-the-rack access switches
- Core/aggregation switch
- Network and infrastructure security

Data centre processing capacity is optimized and consolidated to maximize the utilization of installed computing nodes in the server farm, reduce electricity consumption and maintenance costs through the use of a virtualization platform.

Top-of-the-rack access switches provide all LAN connections to virtualization hosts, storage systems and firewall LAN segments and management. Core switches perform intelligent routing and filtering of traffic between different IP subnets (VLANs).

The data centre has 100 Mbps access to the state-owned WAN network. Firewall devices with high availability terminate VPN tunnels between HIDAACI and other public authorities. Access rules have been defined on firewalls in accordance with network security policies and security requirements of the IT services and deployed information systems to restrict network access to specific IP addresses, protocols and ports. Firewalls also perform routing and NAT translation of traffic to the Internet and DMZ zones and protect inner HIDAACI network segments against unauthorized intrusions and threats coming from an Internet network.

Microsoft Windows Server-based Active Directory is used for centralized management of user, password, workstation and server operating system settings through the enforcement of so-called "group policies". Active Directory Domain Controllers have been installed as virtual machines on the physical server infrastructure to perform the aforementioned roles, as well as domain name to IP address (and vice versa) resolution – the Domain Name System (DNS).

HIDAACI hosts an email server installed as a virtual machine on the physical server infrastructure. The email server is used for internal and external email communication of its employees and sending/receiving notifications from/to its information systems.

Anti-malware protection is applied to workstations and servers, as well as real time scanning of messages and content stored in the email server database. HIDAACI is currently implementing the Endpoint Detection and Response (hereinafter called: EDR) solution. EDR technology will be leveraged to identify suspicious behaviour and advanced persistent threats on endpoints (workstations, laptops, servers, mobile devices) in an environment and alert administrators accordingly.

Windows Server Update Services role is deployed on servers to download Microsoft product security and other update packages from the Official Microsoft sites and update workstation/server operating systems and Microsoft-based services in accordance with patch management policies.

Specialized backup software is used for backing up virtual machines on the backup storage.

6.1.2.2 Electronic system for collection, verification and exchange of asset declaration data

HIDAACI, supported by the Council of Europe's Action Against Economic Crime in Albania[15] and USAID, has established the new electronic system for assets declarations - EACIDS. In 2021, in cooperation with HIDAACI the Action organised trainings for the public authorities on the use of the electronic system.

The electronic system is in operation since 1 January 2022. A total of 300 representatives of public authorities were trained by the Action (in two sets of trainings) and are ready to use the new electronic system. These public authorities will provide assistance and facilitate the process of asset declaration by elected representatives and public officials who are under the obligation to declare their assets and conflicts of interest. This system simplifies the process of asset declaration and submission and publication of asset declarations based on authentication via the e-Albania portal, while increasing the transparency and effectiveness of HIDAACI controls and administrative investigations. Standardization of data entry and processing in this electronic system facilitates rapid and complete investigation of cases related to HIDAACI reports or corruption and money laundering investigations.

Establishment of the system represents a fulfilment of legal obligations and commitments made in the implementation of the Cross-Cutting Strategy against Corruption, recommendations from the (EU) Progress Report and GRECO.

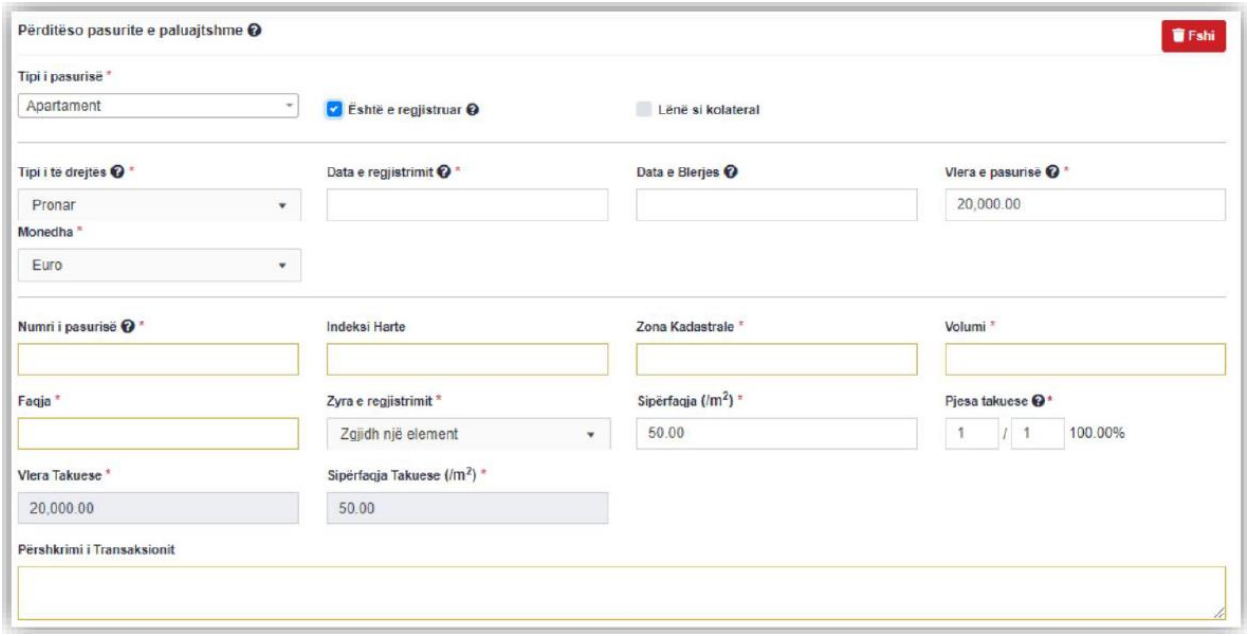
The EACIDS information system is composed of the following software components:

- Application software (EACIDS application servers, database servers, CORE, etc.)
- Online declaration module integrated into the web portal

The online declaration module allows Albanian officials who have the legal obligation to declare their assets to complete and submit the asset declaration electronically, quickly, securely, while minimizing possible errors. Candidates for judicial office positions can also attach documents, such as various certificates, to their electronic declaration.

The EACIDS system communicates electronically with the Civil Status Registry to retrieve and verify public officials' and their family members' personal data entered in the user registration process. The user needs to register in the system before he/she can authenticate, complete and submit the electronic asset declaration.

[15] The Action Against Economic Crime in Albania was part of the "Horizontal Facility for the Western Balkans and Turkey II", a joint programme of the European Union and Council of Europe which aimed to assist the beneficiaries in the Western Balkans region and Turkey to comply with the Council of Europe standards and European Union acquis in the framework of the enlargement process.



Add immovable asset screen in the EACIDS online asset declaration process

HIDAACI is responsible for management and administration of the EACIDS.

The EACIDS system was developed by an outsourced partner. Development technology is .Net Framework / PHP, while SQL Server / Mysql is used as Relational Database Management System (hereinafter: RDBMS). Load balancer performs load balancing of web traffic between multiple web servers.

EACIDS **supports** the following functionalities:

- Document management
- Workflow management
- Business processes are visualized as BPMN diagrams using the Visio application
- Email or in-application notification for new tasks or alarms received (during user creation, completion of asset declarations, etc.)
- Both the online declaration module and the internal system provide users directions for next steps in the procedure and the relevant deadlines (by displaying messages about declaration submission deadlines)
- Search (including full-text search) and/or filtering of the data
- Option to define, create and maintain templates which the users can use in their everyday life to generate specific content (template for sending email, template for generating statements, etc.)
- Capability to create documents in a visual online rich text editor capable of combining static text and metadata in a dynamic template.
- Personal cabinet/customization of user profile
- Electronic submission of asset declaration data and document attachments[16] using the web application accessible via the Internet.

[16] Only candidates for judicial office positions can attach electronic documents.

- Identifying, classifying, storing, securing, retrieving, tracking, labelling and reporting of collected content for the purposes of process logging (Every action in the system is logged, processed and reported, if necessary).
- Electronic archiving (classification and archiving of closed cases/records).
- Supporting roles and user profiles by granting access to resources (both functionality and data) to the specific profile, combining the role and the user.
- Multilingual support for menus and data fields in Albanian and English language
- Automated, semi-automated or purely human mechanisms are implemented for regular monitoring of data quality
- Remote (out-of-office) access enabled via the Internet, to authorized users only
- Ad hoc reports & statistics (tools for ad hoc analysis that can be used to create non-predefined reports or to drill deeper into a static report to obtain details about the case data, transactions or records).

EACIDS **does not support** the following functionalities:

- Users can manage documents in workgroups (multiple author participation) to facilitate document control, auditing, editing and timeline management.
- Scanning of incoming paper documents
- OCR of the scanned documents
- Capability to sign, seal, store and transfer selected electronic documents using a qualified electronic certificate and a qualified electronic time stamp.
- Capability to identify, accept and exchange signed messages with certification authorities (CA) registered in National Register of Qualified Trust Service Providers.
- Capability to automatically check the validity of electronic signatures and electronic seals.
- Data Pseudonymisation
- Data Encryption (there are plans to implement TDE (Transparent Data Encryption) using Azure key vault
- Compliance with WAI (Web Accessibility Initiative) level A1 – accessible to people with disabilities.
- Datawarehouse & Business Intelligence (Datasets included into DW/BI)

6.1.2.3 Interoperability infrastructure and data exchange with the relevant national registries and databases

The EACIDS system currently retrieves and verifies information through integration with the national GSB/ESB platform (Government Gateway) from the following national registers[17]:

- CITIZEN REGISTER (personal IDs, IDs for foreigners, passports, personal ID number, residence)
- CITIZEN PERSONAL STATUS REGISTER (birth, marriage, death)
- BUSINESS ENTITY REGISTERS

[17] These registers have already been integrated with the national GG.

Interoperability - questions	Interoperability - answer
Is the external system's data available in a machine-readable format	Yes ☒ No ☐
URL of the external information system, if publicly available	https://e-albania.gov.al/gg/submission
INSTITUTION RESPONSIBLE FOR MANAGEMENT/ADMINISTRATION OF THE EXTERNAL SYSTEM	AKSHI
External system DEVELOPED	Outsourcing ☒
Data exchange type	Other ☒ ____ GovTalk _____
Type of web service, if applicable	REST ☒
Web service architecture, if applicable	via GSB (ESB) ☒
Data format used	XML ☒
Communication protocol used	HTTPS ☒
Implemented security features	Authentication ☒ Authorization/access control ☒ SSL/TLS ☒
Authentication used	Username ☒
Data retrieval steps	1. HTTP Post to the URL https://e-albania.gov.al/gg/submission 2. XML request called GovTalk according to the template is posted. 3. Integration is done through ESB production.

For communications with third parties, HIDAACI uses an external system called DMZ which sends manual requests to the requested institution. Response that comes back to HIDAACI is either uploaded as a CSV file or entered manually in the system. So EACIDS doesn't have automatic integration in this case.

The EACIDS system will retrieve and verify information from other relevant external systems. This communication will be possible through integration via the GG platform.

Information on the availability of national registries mainly used in the asset declaration verification process on the GSB platform or in electronic form is presented in Table X.

Electronic registry	Available in electronic form	Published on the GSB and available to EACIDS
CITIZEN REGISTER (personal IDs, IDs for foreigners, passports, personal ID number, residence)	Yes	Yes
CITIZEN PERSONAL STATUS REGISTER (birth, marriage, death)	Yes	Yes
REGISTER OF MOTOR VEHICLES	Yes	No
REGISTER OF SHIPS/VESSELS	Yes	No
AIRCRAFT REGISTER	Unknown	No
REAL ESTATE REGISTER	Yes	No
REGISTER OF SECURITIES	Yes	No
TAX ADMINISTRATION REGISTERS	Yes	No
REGISTER OF BUSINESS ENTITIESS	Yes	Yes
CENTRAL BANK REGISTER OF COMMERCIAL BANK ACCOUNTS	Unknown	No
SOCIAL WELFARE REGISTER	Unknown	No
REGISTER OF INTELLECTUAL PROPERTY	Unknown	No

6.1.2.4 IT governance, information security, data protection

HIDAACI's IT Department is responsible for operational management and support of EACIDS and the underlying infrastructure. The IT Department has 3 staff, the Head and 2 IT specialists.

HIDAACI must coordinate with AKSHI its activities related to electronic data exchange with other national registries via the GG platform. AKSHI is responsible for operational management of Albanian digital services infrastructure, such as the e-Albania government portal, Government Gateway, Active Directory, Public Key Infrastructure that issues electronic certificates for public administration and the state data centre.

HIDAACI has established a working group for further development and improvement of the EACIDS system. It consists of representatives of different user roles and expertise. The institution possesses the source code for the EACIDS system. HIDAACI collects user feedback and new ideas for software improvements and development of new features.

The IT Department provides user support for EACIDS. However, Service Desk (Ticketing) software or call centre is not implemented to track all relevant information related to submission and resolution of support and change requests.

Additional training for the existing staff and EACIDS training for new staff is provided by the IT Department.

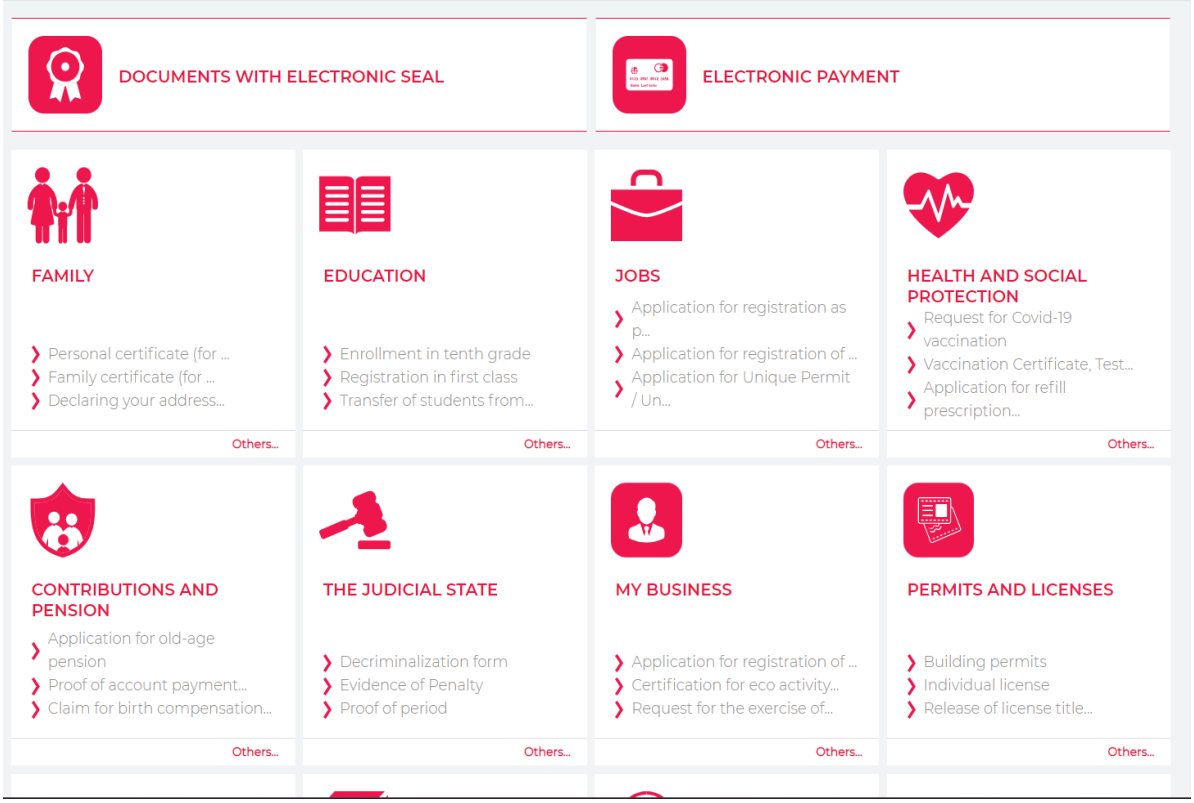
HIDAACI's annual budget includes an allocation of 18420 € for maintenance of the information system and IT infrastructure, while 23737 € is available for IT capital expenditures.

HIDAACI could not provide answers to questions related to Information Security in the submitted questionnaire, because this information is treated as confidential and not shared with third parties.

6.1.2.5 E-Government

Digital transformation is high on the Albanian government policy agenda. 1,225 or 95% of all services delivered by the public administration are now only provided online.

"e-Albania" is the central government portal of Albania that serves as a single point of contact for electronic services provided by Albanian public institutions via the Internet. This portal and other e-Government digital service infrastructure in Albania is administered and developed by the National Agency for Information Society (hereinafter: *AKSHI*). The e-Albania government portal is connected to the Government Interaction Platform – Government Gateway, which is the basic architecture for interactions with public institutions' electronic systems. The Government Gateway is a multifunctional central system, an Enterprise Service Bus solution with a service-oriented architecture that connects 48 information systems[18] and electronic registers that exchange data in real time and enable the provision of electronic services G2G[19], G2C[20], G2B[21]. The Government Gateway is one of the key technical layers of the Albanian Interoperability Framework, which was adopted in 2010 to enable the exchange of information between public administration institutions.



E-Albania portal – home screen with e-services categorized by life or business events

[18] According to the information provided on the e-Albania portal, https://e-albania.al/Pages/eAlbania.aspx
[19] Government to Government
[20] Government to Citizen
[21] Government to Business

The E-Albania portal provides:

- Electronic services level 3 and 4 (according to UNPAN 2014) use the latest technology standards, with options for online payment for these services using debit and credit cards. Payments for electronic services are made securely through the Government Electronic Payments Platform, which is connected to banking and non-banking institutions.
- Electronic services level 1 and 2 (according to UNPAN 2014), where anyone interested can find detailed information about services for the public (licenses, permits, authorizations, documents with a digital stamp, certificates or other similar services), the necessary documentation, the procedure that must be followed, operating hours and the location of administration offices, contacts and the address of the official website of the institution that offers the relevant service, where further details may be available.

Users of the portal include:

- all Albanian citizens;
- businesses registered in the Republic of Albania;
- public administration employees in the Active Directory – identification management system.

The registration process goes through the government portal and the details entered by users in the registration process are verified electronically with the data of the National Register of Civil Status for individuals and the National Commercial Register of Businesses (CKB). The authentication and identification process is based on the "Single-Sign-On" strategy. Citizens can authenticate using their Personal ID number and password or eID based on the qualified electronic certificate (connected to their personal computer via a smart card reader), business entities authenticate using their Business entity ID number and password, while government employees use their Active Directory accounts (gov.al domain) or PKI certificates for authentication on the e-Albania portal. Employees of the Prime Minister's Office, line ministries and dependent institutions are included in the "gov.al" domain based on the Microsoft Active Directory. AKSHI manages the Public Key Infrastructure which issues electronic certificates for public administration. Government employees are provided with a USB token they can use to identify and log into the portal, if using the electronic certificate option.

6.2 Bosnia and Herzegovina

6.2.1 Legal

Analysis of the regulations in Bosnia and Herzegovina indicates that the situation in the area of collection and verification of asset declarations is exceptionally complex. This is due to the fact that Bosnia and Herzegovina lacks a central institution with the authority to collect and verify asset declarations of public officials across the entire territory of the country. For this reason, the text below encompasses multiple institutions in Bosnia and Herzegovina that share this role, each according to its legal competences.

6.2.1.1 Competent authorities

- Central Election Commission

After the adoption of the Election Law of Bosnia and Herzegovina, which entered into force on 28 September 2001, the Provisional Election Commission (PIK) ceased to operate and the Election Commission of Bosnia and Herzegovina was established. In April 2006, the BiH Election Commission changed its name to the BiH Central Election Commission.[22]

The Central Election Commission of Bosnia and Herzegovina is an independent body that reports directly to the Parliamentary Assembly of Bosnia and Herzegovina. The Central Election Commission of Bosnia and Herzegovina is responsible for:

Competences

The competences of the Central Election Commission are determined by the Election Law, where, among other responsibilities, the Commission has the authority to maintain the electronic register of asset declarations of officials elected in local and general elections and their family members.

- Agency for Prevention of Corruption and Coordination of the Fight Against Corruption

This Agency was established under the Law on the Agency for Prevention of Corruption and Coordination of the Fight Against Corruption ("Official Gazette of BiH" no. 103 /09).[23]

The Agency is an independent and autonomous administrative organization that reports to the Parliamentary Assembly of Bosnia and Herzegovina.

Competences

Article 10 of the Law on the Agency for Prevention of Corruption and Coordination of the Fight Against Corruption outlines the responsibilities of the Agency. It is evident from the listed competences that the Agency lacks the authority for collection and verification of asset

[22] https://www.izbori.ba
[23] http://apik.ba

declarations of public officials. The only competence related to asset declarations is specified in Article 10, paragraph 1(e): "Prescribe a uniform methodology for collection of data about the financial status of civil servants".

- Anticorruption and Quality Management Office of the Sarajevo Canton

On 2 February 2018, the Government of the Sarajevo Canton adopted the Decree on Establishment of the Anticorruption and Quality Management Office of the Sarajevo Canton.[24]

Today, this Office is the legal successor of the Sarajevo Canton Quality Office and the earlier Office for the Introduction and Maintenance of ISO 9001:2000 Quality Systems in Administrative Bodies, Administrative Institutions and Professional Services of the Sarajevo Canton.

Competences

Among other competences, the Office is responsible for implementing the Law on Reporting and the Procedure for Data Validation of the Property of Public Position Holders in the Sarajevo Canton. The Office is competent and authorized for collection, verification and processing data related to public officials' assets and for establishment and maintenance of the Asset Data Register.

- Anticorruption and Quality Management Office of the Tuzla Canton

On 4 May 2021, the Government of the Tuzla Canton adopted the Decree on the Establishment of the Anticorruption and Quality Management Office of the Tuzla Canton.[25]

Competences

Among other competences, the Office has a responsibility to establish and maintain the Register of Asset Data for public officials, in accordance with Article 6 of the Law on Reporting, Origin and Control of Property of Elected Officials, Holders of Executive Functions and Advisors in the Tuzla Canton. The register is an electronic collection of data on the assets of public officials in the Tuzla Canton and is part of the unique anticorruption information system established and managed by the Office.

- Republic Commission for the Prevention of Conflicts of Interest in the Authorities of the Republika Srpska [26]

This Commission was formed according to the Law on Prevention of Conflicts of Interest in the Authorities of Republika Srpska ("Official Gazette of RS" 73/08).

[24] https://www.anticorrupiks.com
[25] https://anticorruptk.ba
[26] https://www.sukobinteresa-rs.org

Competences

The Commission has the following competences:

- Acts based on this law to ensure accountability and credibility of elected representatives, holders of executive functions and advisors, with the view to protect the integrity of the function rather than the individual performing that function;
- Issues instructions, regulations and rules, prescribes forms and organizes the registry for the implementation of this law;
- Makes decisions on whether certain actions or omissions constitute a violation of this law;
- Reports to the National Assembly of Republika Srpska and the public at least once a year; and
- Submits reports to the relevant prosecutor's office on any violations of this law that may have characteristics of a criminal offense.

In addition to the above competences, Article 12 of the Law prescribes that elected representatives, holders of executive functions and advisors must submit regular financial reports in accordance with the law and regulations of the Commission. The Commission will regulate, by a special act, the manner of controlling the financial report.

6.2.1.2 Legal framework

- Election Law of BiH ("Official Gazette of BiH" Nos. 23/01, 7/02, 9/02, 20/02, 25/02, 4/04 20/04, 25/05, 52/05, 65/05, 77/05, 11/06, 24/06, 32/07, 33/08, 37/08, 32/10, 18/13, 7/14, 31/16, 41/20, 38/22, 51/22 and 67/22)

According to Article 15.7 of this law, elected candidates at all levels of government (in both local and general elections) must submit to the Central Election Commission of BiH, on a specific form, a signed declaration which contains:

- Current income and sources of income, including all earnings, salaries, property income, contributions from Article 15.1 of this Law, payments and other earnings obtained in Bosnia and Herzegovina and abroad in the past calendar year;
- Property, including money, bank accounts, business documentation, stocks, securities, bonds, real estate, personal property, tenancy rights and other property and assets valued at more than 5,000 KM, in Bosnia and Herzegovina and abroad; and
- Expenditures and other liabilities, including all debts, obligations, promissory notes, loans and guarantees for such obligations in Bosnia and Herzegovina and abroad.

Declarants

From the above provision it follows that declarants are candidates elected at all levels of government in local and general elections.

Asset declaration – forms and content

According to Article 15.8 of the Law, candidates elected at all levels of government, within 30 days from the date of publication of their mandate in the Official Gazette of Bosnia and Herzegovina, must submit to the Central Election Commission a signed declaration on the asset status. The declaration should include data on the assets of the candidate and members of their immediate family; spouse, children and household members.

OIS-1

IZJAVA O IMOVINSKOM STANJU IZABRANOG ČLANA ORGANA VLASTI[1]

SVRHA[2] | DATUM PODNOŠENJA

OPĆE INFORMACIJE O IZABRANOM ZVANIČNIKU

IME | PREZIME

NIVO VLASTI
IZBORNA JEDINICA | ŠIFRA IZBORNE JEDINICE
POLITIČKI SUBJEKT | ŠIFRA POLITIČKOG SUBJEKTA

PODACI O BRAČNOM DRUGU

TRENUTNO STANJE (Oženjen/udata)

PODACI O DJECI

DJECA (Broj djece)

ČLANOVI DOMAĆINSTVA PREMA KOJIMA IZABRANI ZVANIČNIK IMA ZAKONSKU OBAVEZU IZDRŽAVANJA

ČLANOVI DOMAĆINSTVA (Broj članova)

SADAŠNJI PRIHODI I IZVORI PRIHODA IZABRANOG ZVANIČNIKA U BOSNI I HERCEGOVINI I INOSTRANSTVU U PROTEKLOJ KALENDARSKOJ GODINI

VRSTA PRIHODA	PERIOD (OD –DO)	IZNOS PRIHODA (KM)
1. PLATA		
2. PENZIJA		
3. NAKNADA		
4. KOMISIJA		
5. DOBIT OD IMOVINE		
6. HONORAR		
7. DRUGO		
	UKUPNA VRIJEDNOST	

[1] IZABRANI ČLAN ORGANA VLASTI – u daljnjem tekstu: IZABRANI ZVANIČNIK
[2] U slučaju Svrha upisuje se početak mandata ili prestanak odnosno istek mandata izabranog zvaničnika

Also, this Article prescribes that the elected official must report their assets to the Central Election Commission within 30 days from expiry of the mandate for which they were elected and also in case of termination of the mandate (cases specified by law), within 30 days from the date of termination of the mandate.

The Central Election Commission issues instructions that determine the form and manner of completing the form.

- Instruction on the Form and Manner of Completing the Asset declaration Form ("Official Gazette of BiH“ no. 56/17, 4/21)

This Instruction prescribes the form and contents of the asset declaration. With regard to this Instruction, the elected official should submit the asset declaration to the Central Election Commission electronically, through the application for asset records and the printed and signed copy should be submitted to the Central Election Commission of Bosnia and Herzegovina by mail.

The asset declaration should contain the following data:

- General information about the elected official, their family and household members they have a legal obligation to support and the elected official’s current income and sources of income in Bosnia and Herzegovina and abroad in the past calendar year,
- Assets of the elected official in the amount over 5,000.00 KM, their expenses and other liabilities in Bosnia and Herzegovina and abroad, with additional clarification of these items, and
- Assets of the elected official's spouse, children and household members.

The Central Election Commission of Bosnia and Herzegovina should record the submission of the declaration in the database.

Data publication

According to the Article 15.9 of this law, the Central Election Commission of BiH allows forms containing declarations of overall financial status to be accessible to the public.

The Commission is not responsible for the accuracy of data related to the information contained in the form.

Data verification

Specifically, this law does not contain provisions relating to verification of asset declarations, meaning that the Central Election Commission does not have such authority.

- Law on Reporting and the Procedure for Data Validation of the Property of Public Position Holders in The Sarajevo Canton ("Official Gazette of the Sarajevo Canton" no. 18/2019, 12/2022)

This law mandates the obligation of elected and appointed officials, holders of executive functions and advisors (public office holders) to report any acquired property and income, origin and changes in property and income, as well as any gifts received while in public office (property information). This obligation also applies to information about the property of close relatives and affiliated entities of public office holders.

Declarants

From the above provision it follows that declarants are public office holders: elected/appointed officials, holders of executive functions and advisors.

Article 4 of the Law precisely defines holders of public functions, as follows:

Declarants
a) Elected officials: - Representatives in the Assembly of the Sarajevo Canton and councillors in the City Council of the City of Sarajevo and municipal councils of municipalities within the territory of the Sarajevo Canton
b) Holders of executive functions: - Prime Minister of the Sarajevo Canton and members of the Government of the Sarajevo Canton, - Mayor of the City of Sarajevo and municipal mayors of municipalities on the territory of the Sarajevo Canton, - Directors and deputy directors of agencies, funds, public enterprises, public institutions and institutions founded by the Sarajevo Canton, - Members of assemblies, - Administrative and supervisory boards of directorates, institutes, public institutions, public enterprises and other institutions in the Sarajevo Canton that are elected and appointed, or whose election or appointment was approved by the legislative body of the Sarajevo Canton or the City and municipal councils or the Government of the Sarajevo Canton;
c) Advisors: - Advisors to elected officials and holders of executive functions appointed pursuant to lex specialis regulations.

Asset declaration – forms and content

According to Article 8, the Declaration includes detailed information about property and income, such as:

a) The right of ownership of real estate in the country/abroad;

b) The right of ownership of movable assets subject to registration with competent authorities in the country/abroad;

c) The right of ownership of movable assets valued at more than 5,000 KM in the country/abroad;

d) Shares, stocks, bonds and equity shares in legal entities and other securities in the country/abroad;
e) Deposits, dividends and interest in banks and other financial organizations, in the country/abroad;
f) Rights based on copyright, patent and similar intellectual property rights in the country/abroad;
g) Financial liabilities to individuals and legal entities in the country/abroad in excess of 5,000 KM;
h) Source and amount of annual monetary income in the country/abroad.

When the property of close relatives is separated, reporting is done separately for each member with assets registered to their name and is attached to the report of the declarant. In the income and financial liabilities report, the holder of the public function specifies the amount, type and source of each income, as well as the amount and type of financial liabilities.

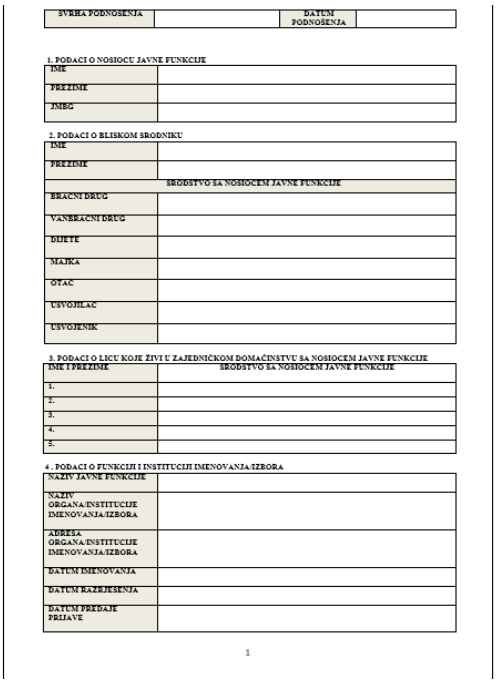
According to the law, there are 4 situations when a declaration of assets is required:

I. Declaration of assets upon assuming office (Article 9)
The holder of a public office must submit a declaration of assets within 30 days from the day of assuming public office.

II. Annual declaration of assets (Article 10)
The annual declaration of assets from Article 8 of this law must be made during the time of performing the function in the period from January 1 to January 31 of each calendar year.

III. Declaration of assets after the end of duty or dismissal (Article 11)
The holder of a public office must submit a declaration of assets, not later than 30 days from leaving the public office for any reason.
In addition to this obligation, the holder of a public office is required to declare that no activities have been initiated to acquire assets upon leaving the public office for any reason.

IV. Declaration upon request of the Office (Article 12)
At any time, the Office may request holders of public office to provide the requested information on assets from Article 8 of this law.



SVRHA PODNOŠENJA		DATUM PODNOŠENJA	

1. PODACI O NOSIOCU JAVNE FUNKCIJE

IME	
PREZIME	
JMBG	

2. PODACI O BLISKOM SRODNIKU

IME	
PREZIME	
SRODSTVO SA NOSIOCEM JAVNE FUNKCIJE	
BRAČNI DRUG	
VANBRAČNI DRUG	
DIJETE	
MAJKA	
OTAC	
USVOJILAC	
USVOJENIK	

3. PODACI O LICU KOJE ŽIVI U ZAJEDNIČKOM DOMAĆINSTVU SA NOSIOCEM JAVNE FUNKCIJE

IME I PREZIME	SRODSTVO SA NOSIOCEM JAVNE FUNKCIJE
1.	
2.	
3.	
4.	
5.	

4. PODACI O FUNKCIJI I INSTITUCIJI IMENOVANJA/IZBORA

NAZIV JAVNE FUNKCIJE	
NAZIV ORGANA/INSTITUCIJE IMENOVANJA/IZBORA	
ADRESA ORGANA/INSTITUCIJE IMENOVANJA/IZBORA	
DATUM IMENOVANJA	
DATUM RAZRJEŠENJA	
DATUM PREDAJE PRIJAVE	

1

The Law on Reporting and the Procedure for Data Validation of the Property of Public Position Holders in the Sarajevo Canton ("Official Gazette of the Sarajevo Canton“ no. 12/2022) stipulates that public officials in the Sarajevo Canton can declare property in two ways:

- on the Asset Declaration Form - after filling in the form, the public official should sign it and submit it to the Office by mail or by hand to the official premises of the Office;
- electronically.

The declaration form is an integral part and addendum to this Law.

In accordance with Article 17, the declaration form must contain the following data:

Asset declaration – content	
a) Full name and position of the public office holder submitting the declaration	b) Full names of close relatives submitting the declaration
c) Personal identification number, which will not be publicly disclosed	d) Name of the body or institution where the person is employed/appointed, institution address, date of appointment to the position
e) Declaration submission date	f) Immovable assets and type, municipality or city, country if located abroad, surface area, origin, acquisition value, ownership title, whether it is co-owned and in what shares, type and source of funds used to purchase the asset
g) Movable assets and type, year of production or purchase, acquisition value, ownership title, complete details about shares in companies or other institutions, securities, declarant's financial liabilities towards individuals and legal entities	h) Information about participation in supervisory boards, executive boards and the like, regardless of whether paid or unpaid
i) Total annual income divided by source of income	j) Personal statement confirming, under full moral, criminal and civil responsibility, the accuracy of the data in the declaration
k) Personal statement confirming, under full moral, criminal and civil responsibility, that no part of assets has been omitted from the declaration	l) Signature of the declarant

Data publication

Article 20 paragraphs 3 and 4 outline the publication of asset declaration data:

"Public availability of personal data concerning the entire property of the holder of a public office is ensured by providing information about where the property is located, in accordance with Articles 8 and 17 of this law. Data from Articles 8 and 17 of this law will be accessible and published on the website".

Data verification

Article 18 stipulates that the Office controls the reporting of assets and gifts by public office holders. Each declaration is examined to determine the presence or absence of substantive errors or incorrectly completed declarations. If substantive errors or errors in completing the declaration are found, or if the declaration is incomplete, the Office informs the declarant, who must amend or supplement the declaration within 15 days of receipt of such notification.

The Office is authorized to control the asset data and the data related to sources and types of income used to acquire the assets. In case of a mismatch between income and assets and in the presence of reasonable suspicion regarding the accuracy of the data and the legality of the way in which an asset was acquired, the Office must inform the competent prosecutor's office and

other competent authorities, including, but not limited to, tax authorities and the Financial Intelligence Unit of the SIPA (State Investigation and Protection Agency).
Regarding this issue, Article 19 paragraph 3 gives authority to the Office to request data from all relevant institutions, as well as legal and natural persons possessing information relevant for the verifications determined by the provisions of this law.

Data protection

In relation to the protection of personal data, Article 17 paragraph 3 specifies that every processing of personal data from the Register is carried out in accordance with the Law on Personal Data Protection of Bosnia and Herzegovina.

Additionally, in accordance with Article 19 paragraph 2 the Office has the authority to obtain and process personal data in accordance with the Law on Personal Data Protection of Bosnia and Herzegovina, exclusively for the purpose of verifying the accuracy or truthfulness of the information contained in the asset declaration.

The Office has the authority to obtain and process personal data in accordance with the Law on Protection of Personal Data of Bosnia and Herzegovina („Official Gazette of Bosnia and Herzegovina“ 49/06; 76/11; 89/11).

On the other hand, considering that the last amendment to the Law on Personal Data Protection of Bosnia and Herzegovina was made in 2011, it implies that this law is not in compliance with the European regulation for the protection of personal data.

- Law on Declaration, Origin and Control of Assets of Elected Officials, Holders of Executive Functions and Advisors in the Tuzla Canton (“Official Gazette of the Tuzla Canton“ no. 22/2021)

This law establishes the obligation of elected officials, holders of executive functions and advisors (public office holders), to report their existing assets and income, the origin and changes in property and income, as well as gifts received during the performance of public functions (asset information). This obligation also applies to providing information about the property of close relatives of public office holders.

The law also addresses the methods of data collection, processing, use, protection and storage, as well as the duties and responsibilities of the authorities responsible for implementing and supervising the enforcement of this law and other matters relevant for its implementation.

Declarants

Article 4 of the Law determines the meaning of the terms used in the law. This article, in relation with Article 1 of this law, defines declarants as follows:

Declarants
a) Elected officials: - Representatives in the Assembly of the Tuzla Canton and councillors in the city and municipal councils of cities and municipalities on the territory of the Tuzla Canton.
b) Holders of executive functions: - Prime Minister of the Tuzla Canton and members of the Government of the Tuzla Canton, - Mayor of the Tuzla Canton and municipal mayors of municipalities on the territory of the Tuzla Canton, - Cantonal prosecutor and city or municipal prosecutors, - Directors and deputy directors of agencies, funds, public enterprises, public institutions and institutions founded by the Tuzla Canton, - Members of assemblies, - Administrative and supervisory boards of directorates, institutes, public institutions, public enterprises and other institutions in the Tuzla Canton who are elected and appointed, or whose election or appointment has been approved by the legislative body of the Tuzla Canton or the City and municipal councils or the Government of the Tuzla Canton;
c) Advisors: - Advisors to elected officials and holders of executive functions appointed according to lex specialis regulations.

Asset declaration – forms and content

According to Article 10 of this law, the declaration includes detailed information about property and income, such as:

a) The right of ownership of real estate in the country/abroad;

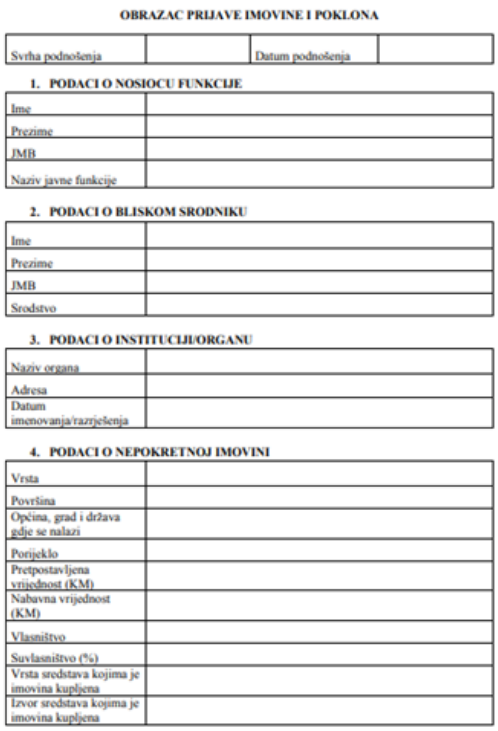
b) The right of ownership of movable property subject to registration with competent authorities in the country/abroad;

c) The right of ownership of movable property valued at more than 5,000 KM in the country/abroad;

d) Shares, stocks, bonds and shares in legal entities and other securities in the country/abroad;

e) Deposits, dividends and interest in banks and other financial organizations, in the country/abroad;

f) Rights based on copyright, patent and similar intellectual property rights in the country/abroad;



OBRAZAC PRIJAVE IMOVINE I POKLONA

Svrha podnošenja		Datum podnošenja	

1. PODACI O NOSIOCU FUNKCIJE

Ime	
Prezime	
JMB	
Naziv javne funkcije	

2. PODACI O BLISKOM SRODNIKU

Ime	
Prezime	
JMB	
Srodstvo	

3. PODACI O INSTITUCIJI/ORGANU

Naziv organa	
Adresa	
Datum imenovanja/razrješenja	

4. PODACI O NEPOKRETNOJ IMOVINI

Vrsta	
Površina	
Općina, grad i država gdje se nalazi	
Porijeklo	
Pretpostavljena vrijednost (KM)	
Nabavna vrijednost (KM)	
Vlasništvo	
Suvlasništvo (%)	
Vrsta sredstava kojima je imovina kupljena	
Izvor sredstava kojima je imovina kupljena	

g) Financial liabilities towards individuals and legal entities in the country/abroad in excess of 5,000 KM;

h) Source and amount of annual monetary income in the country/abroad;
i) Gifts with market value exceeding 200 KM; and
j) Protocol gifts.

When the property of close relatives is separated, reporting is done separately for each member with assets registered to their name and is attached to the report of the declarant. In the income and financial liabilities report, the holder of the public function specifies the amount, type and source of each income, as well as the amount and type of financial liabilities. When the property of close relatives is separated, reporting is done separately for each member with registered property in their name and it is attached to the report of the person obligated to report. In the report of income and financial obligations, the holder of the public function specifies the amount, type and source of each income, as well as the amount and type of financial obligations.

According to the law, there are 4 situations when a declaration of assets is submitted:

I. Declaration of assets upon assuming office (Article 11)
The holder of a public office must submit a declaration of assets within 30 days from the day of assuming public office.

II. Annual declaration of assets (Article 12)
The annual declaration of assets is required while in public office, between 1 January and 31 January of each calendar year.

III. Declaration of assets after leaving or dismissal from public office (Article 13)
The holder of a public office must submit a declaration of assets, not later than 30 days from leaving the public office for any reason.
In addition to this obligation, the holder of a public office is required to declare that no activities have been initiated to acquire assets upon leaving the public office for any reason.

IV. *Declaration upon request of the Office* (Article 14)
The Office may, at any time, request public office holders to provide the requested information on assets under this law.

The declaration form is an integral part of and an addendum to this Law.

In accordance with Article 20 of the law, the declaration form must necessarily contain the data as follows:

Asset declaration - content	
a) Full name and position of the public office holder submitting the declaration	b) Full names of close relatives submitting the declaration
c) Personal identification number, which will not be publicly disclosed	d) Name of the body or institution where the person is employed/appointed, institution address, date of appointment to the position
e) Declaration submission date	f) Immovable assets and type, municipality or city, country if located abroad, surface area, origin, acquisition value, ownership title, whether it is co-owned and in what shares, type and source of funds used to purchase the asset
g) Movable assets and type, year of production or purchase, acquisition value, ownership title, complete details about shares in companies or other institutions, securities, declarant's financial liabilities towards individuals and legal entities	h) Information about participation in supervisory boards, executive boards and the like, regardless of whether paid or unpaid
i) Total annual income divided by source of income	j) Personal statement confirming, under full moral, criminal and civil responsibility, the accuracy of the data in the declaration
k) Personal statement confirming, under full moral, criminal and civil responsibility, that no part of assets has been omitted from the declaration	l) Statement of consent for the Office to obtain and process personal data for the purpose of verifying the accuracy or truthfulness of the information contained in the declaration
m) Declarant's signature	

Data publication

Publication of the data from asset declaration is in accordance with Article 23 of the law.

Data verification

Article 21 of the Law prescribes that the Office controls the reporting of assets and gifts by the public office holder. Each declaration is examined to determine the presence or absence of substantive errors or incorrectly completed declarations. If substantive errors or errors in completing the declaration are found, or if the declaration is incomplete, the Office informs the declarant, who must amend or supplement the declaration within 15 days of receipt of such notification.

The Office is authorized to control the asset data and the data related to sources and types of income used to acquire the assets. In case of a mismatch between income and assets and in the presence of reasonable suspicion regarding the accuracy of the data and the legality of the way in which an asset was acquired, the Office must inform the competent prosecutor's office and other competent authorities, including, but not limited to, tax authorities and the Financial Intelligence Unit of the SIPA (State Investigation and Protection Agency).
Related to this issue, Article 22 paragraph 3 prescribes that the Office has the authority to request data from all relevant institutions, as well as legal and natural persons possessing information relevant for verifications determined by the provisions of this law.

Data protection

In relation to the protection of personal data, Article 19 paragraph 3 specifies that all processing of personal data from the Register must carried out in accordance with the Law on Personal Data Protection of Bosnia and Herzegovina.

Additionally, in accordance with Article 22 paragraph 2 the Office has the authority to obtain and process personal data in accordance with the Law on Personal Data Protection of Bosnia and Herzegovina, exclusively for the purpose of verifying the accuracy or truthfulness of the information contained in the asset declaration.

The Office has the authority to obtain and process personal data in accordance with the Law on Protection of Personal Data of Bosnia and Herzegovina („Official Gazette of Bosnia and Herzegovina“ 49/06; 76/11; 89/11).

On the other hand, considering that the last amendment to the Law on Personal Data Protection of Bosnia and Herzegovina was made in 2011, this implies that this law is not compliant with the European regulation for the protection of personal data.

- Law on Prevention of Conflict of Interest in the Government Bodies of Republika Srpska (“Official Gazette of RS” 73/08, 52/14)

This law regulates the special obligations of public officials in the authorities of Republika Srpska and local self-government units in the performance of public office and with the aim of preventing conflict of interest.

Declarants

According to this Law, public officials must submit financial reports, as provided by the law and regulations of the Commission.
Related to this, Article 4 of the Law precisely defines public office holders as follows:

a) Selected representatives: - Members of Parliament in the National Assembly of RS, - Delegates in the Council of RS, - Councilors in the assemblies of local self-government units
b) Holders of executive functions: - President and Vice President of RS; - Members of the Government of RS; - General Secretary of the President of RS; - General Secretary of the National Assembly of RS, - General Secretary of the Council of RS; - General Secretary of the Government; - Mayors and deputy mayors; - Municipal mayors and deputy municipal mayors

v) Advisors to selected representatives and executive office holders, namely advisors to:
- President and Vice President of RS;
- President and Vice President of the National Assembly of RS;
- President and Vice President of the Council of RS;
- Members of the Government of RS, and
- Mayors and municipal mayors.

Asset declaration – forms and content

Article 12 of the Law states that „Elected representatives, executive office holders and advisors shall submit regular financial reports as provided by the law and regulations of the Commission. The Commission will regulate, by a special act, how such financial reports will be controlled."

- Rules of the Republic Commission for Prevention of Conflict of Interest in the Authorities of Republika Srpska and the Manner of Control of Financial Statement

These rules closely regulate the work of the Republic Commission and prescribe the forms for financial reporting of assets by public officials and their close relatives.". [27]

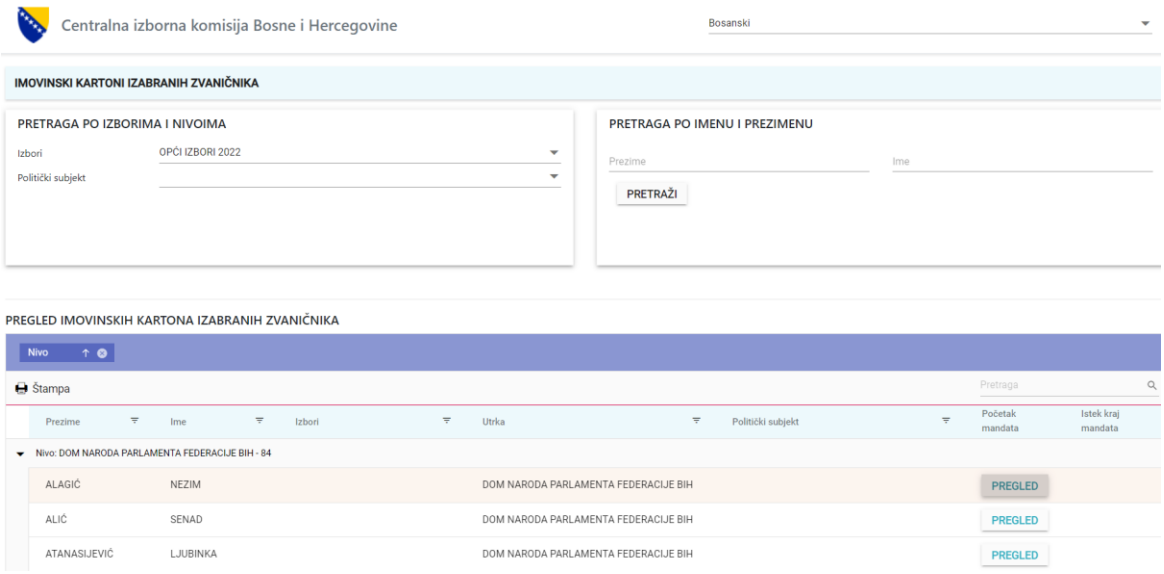
Law on Prevention of Conflict of Interest in the Government Bodies of the Republika Srpska does not contain provisions related to publication, verification and exchange of data. It also lacks specific provisions related to protection of personal data.

6.2.2 Technical

6.2.2.1 Electronic system for collection, verification and exchange of asset declaration data

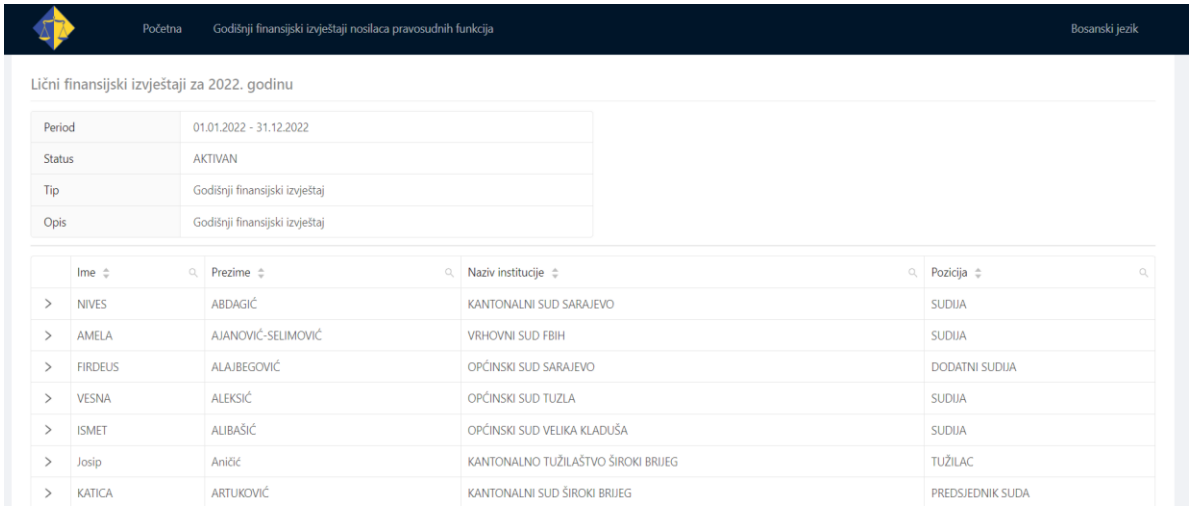
The Central Election Commission of Bosnia and Herzegovina (hereinafter: *CEC BiH*) maintains an electronic register of asset declarations for officials elected at the local and general elections and their eligible family members. Asset declarations are collected at the beginning and at the end of their mandate. Asset declarations without the elected officials' personal data are published on the CEC BiH website[28]. Elected officials can complete asset declarations electronically. However, they have to print the completed form, sign it and send it to CEC BiH by registered mail. Upon receipt of the signed asset declaration form, authorized employees of CEC BiH will cross-check the data on the printed copy with the data stored in the database and, in case of a full match, verify the asset declaration in the database. Elected officials need to register in the asset declaration system before they can log in. For authentication they can use their username and password as the simple, less secure method, or two-factor authentication (after successful password verification, the user receives an SMS code on his/her mobile phone number provided at registration and enters it when prompted by the system) as a more secure authentication method.

[27] https://www.sukobinteresa-rs.org/index.php?option=com_content&view=category&layout=blog&id=6&Itemid=29&lang=sr-YU
[28] https://eimovinskikartoni.izbori.ba/public/



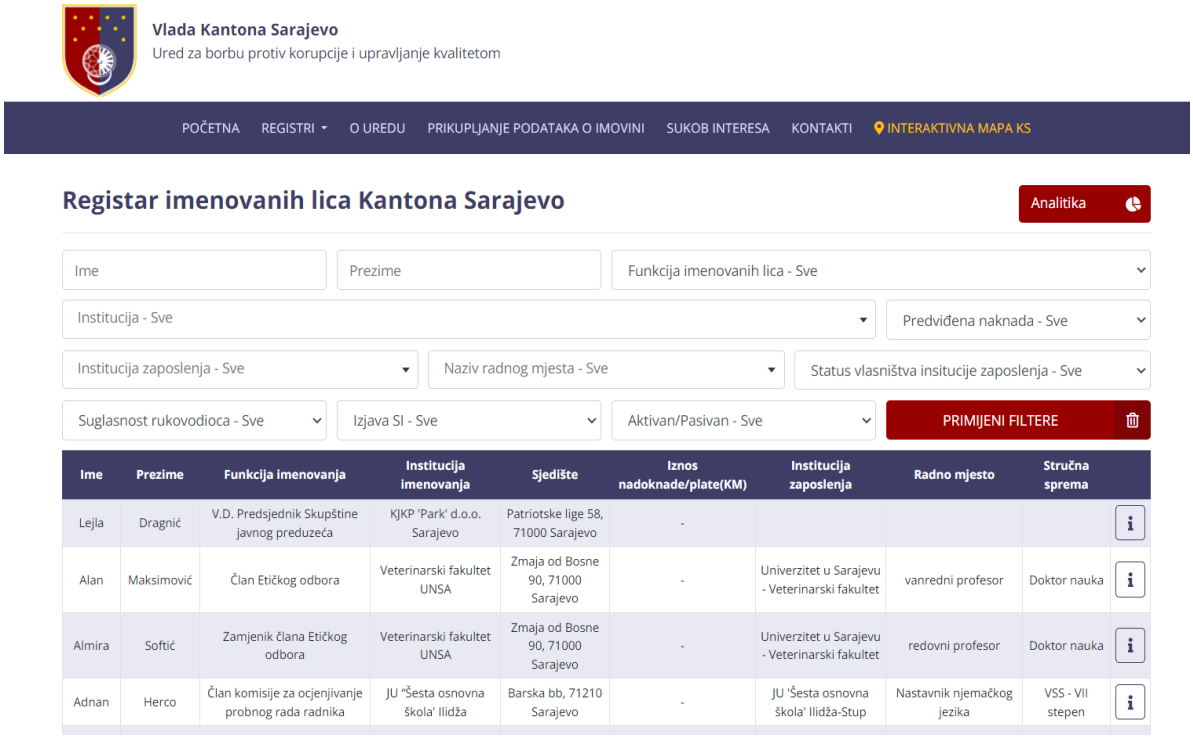
Access to elected officials' asset declarations via the CEC BiH website

The High Judicial and Prosecutorial Council of Bosnia and Herzegovina (hereinafter: *HJPC*) has developed and implemented an information system to support the process of asset data collection and verification for judges and prosecutors and their eligible family members in Bosnia and Herzegovina. The asset declaration database currently contains data from asset declarations of 242 judges and prosecutors who have consented to publication of their asset data via the HJPC web portal. Since the Law on the HJPC was amended a few months ago to enhance HJPC's competences in this matter, but the implementing acts have not been adopted yet, the system is still not used to its full capacity. The system envisages that judges and prosecutors can complete the asset declaration form electronically. Personal data other than the name and surname of the judge/prosecutor is anonymized before publication on the website. The system architecture is interoperable, meaning that it can use web services for retrieval of data from external systems for asset verification purposes.



Access to asset declarations of the judges and prosecutors via HJPC BiH website

Anticorruption and Quality Control Office of the Sarajevo Canton has established an electronic asset declaration system for public office holders in this canton and their eligible family members. Electronic search and access to asset declarations of the public office holders can be performed via the website of the Anticorruption and Quality Control Office of the Sarajevo Canton[29]. Public office holders personal data other than their name and surname is not shown.



Access to asset declarations of the public office holders in the Sarajevo Canton

Public office holders in the Sarajevo Canton can complete asset declarations electronically. However, they have to print the completed form, sign it and send it to the Anticorruption and Quality Control Office of the Sarajevo Canton by registered mail. Public office holders need to register in the asset declaration system before they can log in. For authentication they use the username and password created during the user registration process.

6.2.2.2 General findings on electronic asset declaration systems in Bosnia and Herzegovina

Unlike other Parties of the Treaty, Bosnia and Herzegovina lacks the central institution that executes powers and performs duties related to asset declaration and verification for public officials in the territory of the whole country. This is due to the specifics of the constitutional arrangement of Bosnia and Herzegovina. For this reason, several institutions have asset declaration collection and verification competences covering either specific type of public officials (CEC BiH for the officials elected at the local and general elections and their eligible family members, HJPC BiH for judges and prosecutors and their eligible family members) or specific territory (i.e. Sarajevo Canton).

[29] https://www.anticorrupiks.com/registar-imenovnaih-lica

These institutions have developed their own electronic asset declaration systems. None of the institutions have any kind of web services or other means of electronic data exchange in place to retrieve data from external registers and databases for the purposes of asset verification.

Having in mind the stated reasons and the fact that Bosnia and Herzegovina has not signed the Treaty and that it is completely unclear from the legal point of view which institution could become a Focal Point for the Treaty, a more thorough analysis of the IT infrastructure, information systems and IT governance and information security in the aforementioned institutions would serve no purpose.

6.2.2.3 E-Government

In accordance with the constitutional arrangements in Bosnia and Herzegovina, state and entity government levels have competences to enact laws to enable the digital transformation of public service delivery at their respective levels. Given that BiH aims to join the European Union, reforms are needed at the entity and central level to become compliant with the relevant EU policies and ensure that services provided online have the same legal standing as those obtained through other means. In Bosnia and Herzegovina, there is no countrywide strategic framework and policy vision to guide the whole-of-government approach to the digital transformation and development of digital services aimed at citizens and businesses, because responsibilities in the segment of public service delivery are decentralized. Policy for the Development of the Information Society in BiH for the period 2017-2021 was adopted at the state level. However, the state government level and the Federation of Bosnia and Herzegovina have not adopted the strategy for the development of e-government at these respective levels yet.[30] In March 2020, the Republika Srpska Government adopted the Strategy for Development of E-Government in Republika Srpska 2019-2027 (e-governance strategy).

BiH strives to harmonize its legislation on e-identification with eIDAS. The only BiH instrument that fully corresponds to eIDAS is the Draft Law on the Electronic Identification and Trust Services for Electronic Transactions, which has been in Parliamentary procedure since March 2019. The State, the two entities and Brčko District of Bosnia and Herzegovina claim to have autonomy to regulate this area in accordance with their constitutional competences. As a result, the regulatory framework has been developing at an uneven pace, with Federation of Bosnia and Herzegovina still not having its law on electronic identification in place. Moreover, the laws at different levels are not harmonized in a way that would ensure their interoperability.[31] A Single eID approach is still not functional in Bosnia and Herzegovina despite having all the technical and regulatory pre-conditions in place. In accordance with the Law on the Agency for Identification Documents, Registers and Data Exchange of Bosnia and Herzegovina (hereinafter: IDDEEA), IDDEEA is responsible for personalization and technical processing of identity cards and digital signing in the field of identification documents. There is a final step that must be completed before IDDEEA can start issuing qualified electronic certificates in the identity card of

[30] Draft strategy documents were developed in 2020 within the scope of the UK's Good Governance Fund "Support to e-government reforms and the digitalisation of services in Bosnia and Herzegovina" project.
[31] European Commission. The Bosnia and Herzegovina 2021 Report states that no progress has been made in ensuring the interoperability of the electronic signature system throughout the country.

citizens of Bosnia and Herzegovina for electronic identification of the assurance level high and qualified digital signing. That is the adoption of the Decision of the Council of Ministers on the prices of issuing eID cards.

Two public authorities (Indirect Taxation Authority and IDDEEA) and one private company have already been accredited as certification bodies for the provision of qualified electronic certificates by the Office for Supervision and Accreditation of Certification Authorities.[32] In Republika Srpska, certificate authority of the Ministry of Scientific and Technological Development, Higher Education and Information Society (hereinafter: *MNRVOID*) issues qualified electronic certificates to public administration bodies, as well as to natural and legal persons.

The State level still does not have operational unified public portal for central level services and information. Federation of BiH, Republika Srpska and Brčko District of Bosnia and Herzegovina also have unified public portals where e-services are organized by life or business events. However, these portals provide access to predominantly emerging (informational) or enhanced information services. Some portals like the one for Republika Srpska are technologically outdated and a new e-services portal needs to be built from scratch.

The existence of the common component to facilitate a unified governmental service and data bus is essential for successful development of a whole-of-government digital infrastructure. In Bosnia and Herzegovina, the Government Service Bus (GSB) or the Interoperability Information System (IIS) were implemented at the end of 2017 using a multiple Enterprise Service Bus (ESB) approach. It was based on brokered ESB integration architecture. It consists of four separate instances, one for each level of government (that is, BiH, Federation of BiH, Republika Srpska and the Brcko District of BiH). Every GSB instance is used as an e-service hub by providing access to relevant data and business processes for specific institutions at that government level. At the moment, the GSB platform is used in a very limited capacity at all government levels. At the BiH level, only IDDEEA has published its web services for authorized access to the registry of fines, registry of residence and stay and unique personal identification numbers of BiH citizens, ID cards of BiH citizens and ID cards for foreigners. At the FBiH level, the Federal Administration for Inspection Affairs, Tax Administration of the FBIH, Federal Ministry of Agriculture, Water Management and Forestry and the Federal Ministry of Justice have published web services to provide access to some of the data collected, processed and stored under their responsibility. At the Republika Srpska level, only three public administration bodies have published their services on the GSB: the Agency for Intermediary, IT and Financial Services APIF (data on business entities); the Inspectorate of RS (data on inspection supervision); and the Pension and Disability Insurance Fund of RS (data on employees – beneficiaries of the pension and disability fund contributions). The BD Inspectorate, BD Finance Directorate and Basic Court in Brčko are connected to the GSB instance for the level of Brčko District of Bosnia and Herzegovina.

[32] The state-level Office for Supervision and Accreditation of Certification Authorities carries out both ex-ante supervision (voluntary certification of trust service providers issuing secure electronic signatures) and ex-post supervision.

Instead of publishing their registries on the GSB, public administration bodies build their own interoperability infrastructure, which is used for data sharing with other institutions. Systems in most institutions are not interconnected based on interoperability standards and infrastructure. This makes both maintenance and integration a challenge, adversely impacting the ability to create new e-services.

Currently, there is no email box or e-payment platform at any government level in BiH.

In accordance with the constitutional organization of BiH, institutions from different government levels have the competences to establish, maintain and update electronic registers. Institutions at the state level maintain a limited number of important electronic registers (citizen register with data on ID cards, passports, driving and traffic licenses, register of minor offences, VAT and customs-related data, registry of bank accounts of business entities in BiH, transport permits for international and inter-entity transport, register of immigrants, asylum seekers, refugees). Republika Srpska and Federation of BiH (or cantons in the FBiH) maintain all other electronic registers such as business entity and entrepreneur registers, land registers, geospatial data, registers in the sector of direct taxation, pension, disability and health contributions, health services, education, social welfare, industry, agriculture, energy, intra-entity transport, etc. Most of the basic electronic registers are digitalized, but many of them are either neither interoperable nor published at the relevant GSB instance. Data from specific electronic registers is made available to other institutions, which are authorized by the legislation and signed bilateral or multilateral agreements. Such access is usually provided via point-to-point web services using interoperability infrastructure outside the GSB.

Information on the availability of national registers that are mostly used in the asset declaration verification process on the GSB platform or in electronic form is presented in the following table:

Electronic registry	Available in the electronic form	Published on the GSB
CITIZEN REGISTER (personal IDs, IDs for foreigners, passports, personal ID number, residence)	Yes	Yes (not for passports)
CITIZEN PERSONAL STATUS REGISTER (birth, marriage, death)	Yes	No
REGISTER OF MOTOR VEHICLES	Yes	No
REGISTER OF SHIPS/VESSELS	Unknown	No
AIRCRAFT REGISTER	Yes	No
REAL ESTATE REGISTER	Yes	No
REGISTER OF SECURITIES	Yes	No
TAX ADMINISTRATION REGISTERS (Records of all taxpayers, contributions and insured persons, data necessary for control and collection of tax payments, contributions and data for exercising rights based on compulsory and voluntary insurance)	Yes	Yes
REGISTER OF BUSINESS ENTITIESS	Yes	Yes (registered business entities only)
CENTRAL BANK REGISTER OF	Yes	No

COMMERCIAL BANK ACCOUNTS		
SOCIAL WELFARE REGISTER	Yes	No
REGISTER OF INTELLECTUAL PROPERTY	Unknown	Information will be provided in the interim phase

6.3 Kosovo*

6.3.1 Legal

6.3.1.1 Competent authority

The Agency for Prevention of Corruption was established in accordance with the Law Against Corruption no. 2004/34 ("Official Gazette" no.10/01, March 2007), as an independent body responsible for implementing the state policy for prevention and fight against corruption in Kosovo*.

The special Law no. 03/L-159 on the Anti-Corruption Agency was adopted on 29 December 2009, published in Official Gazette on 5 February 2010.

A new Law no. 08/L-017 on the Agency for Prevention of Corruption was adopted in July 2022. Pursuant to this law, the Agency is an independent and specialized body for the implementation of national policies for the prevention of corruption in Kosovo*. The organizational structure of the Agency is defined by the regulation on internal organization, approved by the Director of the Agency.

Competences:
In accordance with Article 5 of the Law No 08/L-017 on the Agency for Prevention of Corruption, The Agency is responsible for:

- implementation of the Law on Prevention of Conflict of Interest in Exercise of Public Function, Law on Declaration, Origin and Control of Assets and Gifts and the Law on Protection of Whistleblowers, which includes:
- overseeing and preventing cases of conflict of interest and taking measures provided by the special law;
- overseeing asset declarations, as provided by the law;
- overseeing the receipt of gifts related to performance of official duty and undertaking measures, as provided by the law;
- providing opinions related to the conflict of interest and supervision of gifts related to performance of official duty;
- overseeing and taking necessary measures for the protection of whistleblowers.
- Carrying out actions in the area of monitoring the action plan of the national anticorruption strategy, anticorruption assessment of legal acts, corruption risk assessments and integrity plans that include:
- providing professional and technical assistance, advice and support to initiatives undertaken by the institutions for the prevention of corruption;
- providing recommendations to the Assembly of Kosovo* and the Government of Kosovo* for the assessment of draft laws related to the prevention of corruption upon

request from these institutions or by decision of the Director of the Agency;

- monitoring the implementation of the National Strategy Against Corruption along with the action plan;
- cooperating with state institutions and the civil society to raise public awareness about the prevention of corruption;
- developing and overseeing corruption risk assessments;
- providing opinions on legal acts for the purpose of their approximation with international anticorruption standards;
- monitoring the implementation of integrity plans of public institutions;
- conducting administrative investigations and undertaking actions in cases within the competences of the Agency;
- referring criminal reports to the state prosecution office or, in case of administrative violations, forwarding the case to the competent administrative body;
- initiating minor offence proceedings within its scope of activity in accordance with the applicable law;
- imposing fines and other measures in accordance with the relevant applicable legislation;
- collecting, analysing and publishing statistical data or other data related to the status of cases pertinent to the competences of the Agency,
- reporting to the Assembly of Kosovo* on the work of the Agency;
- preparing and proposing the annual budget of the Agency;
- designing and implementing corruption prevention tools, such as training, research, education and public awareness raising;
- performing other duties as provided by the applicable legislation. Among other competences, the Agency is responsible for implementation of the Law on Declaration, Origin and Control of Assets and Gifts and for supervision of asset declaration in accordance with the law. The Agency oversees the assets of senior public officials and other persons as required by special law.[33]

According to the law, the Agency has the powers to verify the origin of declarant's assets and gifts, check for false declarations and file criminal charges in case of non-compliance with the current situation.

6.3.1.2 Legal framework

- Law no. 08/L- 017 - On the Agency for Prevention of Corruption ("Official Gazette" no. 19/21)

This law aims to regulate the status, organization and competences of the Agency for Prevention of Corruption as an independent body specialized in the prevention of corruption. The provisions of this law apply to public and private persons in order to prevent corruption and conflicts of interests, protection of whistleblowers, as well as to the origin and control of property and gifts.

[33] https://www.akk-ks.org/en/ballina

Chapter IV Article 17 of this Law regulates the initiation of administrative investigations. In accordance with this Article, the Agency may conduct an administrative investigation in cases within its mandate, which may be initiated:

- ex-officio;
- on the basis of information received from natural or legal persons: anonymous or public information, or the failure of a person to comply with any of the legal requirements set forth in the laws within the scope of the Agency.

During the administrative investigation, the Agency may undertake the following actions: request, collect, investigate and analyse documentation and other relevant information related to the case; request relevant information from any relevant persons or institutions; conduct interviews with any persons who may have information relevant to the administrative investigation; and examine any circumstances related to the case.

Article 20 paragraph 1 of this law prescribes the obligation to submit information and documents to the Agency: "*Upon request from the Agency, central and local bodies, public sector institutions, holders of public authority and other public or private legal entities, shall submit to the Agency free of charge, within eight (8) days after such request, all data, including personal data and documents required for the performance of the Agency's duties, in accordance with the provisions of other laws.*"

Related to paragraph 2 *of this article "If the authorities, natural and legal persons specified in paragraph 1, do not reply to the Agency within the period and in the manner specified in that paragraph, the Agency shall inform the body that oversees the work of such authorities and persons in order to take measures, and may submit a special report to the Assembly of Kosovo*."*

- Law no. 08/L-108 - On the Declaration, Origin and Control of Property and Gifts (Official Gazette /no. 21/10 August 2022)

The Law no. 08/L-108 - On the Declaration, Origin and Control of Property and Gifts was adopted on 14 July 2022 and entered into force six (6) months after its publication in the "Official Gazette.

This law aims to define the asset declaration system, including the ways and procedures for declaration of assets and gifts, origin and control of declared assets and gifts, as well as the declarants, in order to prevent corruption, conflict of interest and strengthen the integrity of public institutions, including sanctioning. In accordance with Article 2, this law is implemented by the Agency for Prevention of Corruption and the relevant institutions and is mandatory for the declarants subject to this law.

Declarants

According to Article 3 paragraph 1.13 of this law: "*A declarant is an official who, according to this law, has the obligation to declare his assets*."

This provision is connected to the list of senior officials in Article 4 and the list of public officials in Article 5 of this law:

Senior officials as declarants	
President of Kosovo*	Speaker of the Assembly
Members of Parliament	Prime Minister and ministers in the Government of Kosovo*
President of the Constitutional Court, deputy president of the Constitutional Court and judges of the Constitutional Court	President of the Judicial Council of Kosovo* and all presidents of the courts
Chairman of the Prosecution Council of Kosovo*, chief state prosecutor and all other chief prosecutors	Chairman of the Central Election Commission
Commander of the Kosovo* Security Force	Director of the Kosovo* Intelligence Agency
General director of the Kosovo* Police	People's advocate
Governor and board members of the Central Bank of Kosovo*	Chairman, board members of the Kosovo* Pension Savings Trust and managing director
Chairmen, board members and general directors of public enterprises	Auditor general
General director of Customs	General director of Tax Administration
Municipal mayors	Deputy Prime Ministers and deputy ministers in the Government of Kosovo*
Members of the Judicial Council and members of the Prosecution Council, judges and prosecutors	Deputy Commander of the Kosovo* Security Force;
Deputies of the People's Advocate	Ambassadors and consuls
Heads of independent agencies and executive agencies or equivalent positions defined by law or another by-law, and their deputies	All officials exercising the responsibilities of the ZKA, including: secretary general of the Assembly, secretary general of the Office of the Prime Minister and secretaries general of ministries, secretary of the Constitutional Court, director of the Secretariat of the Judicial Council, director of the Secretariat of the Prosecutorial Council
Advisors to the President of Kosovo*, Advisors to the President of the Assembly Kosovo*, advisors to the Prime Minister of Kosovo* and advisors to the ministers of the Government of Kosovo*, including external advisors in politics	Deputy directors of the Kosovo* Police, directors of divisions, directors of departments, directors of directorates, regional directors of the Kosovo* Police and commanders of Kosovo* Police Stations;
Deputy director of the Kosovo* Intelligence Agency, inspector general of the Kosovo* Intelligence Agency and public positions in the Kosovo* Intelligence Agency, as provided by special law	Head of the Secretariat and members of the Central Election Commission
Deputy governors of the Central Bank of Kosovo*	Chief executive officer, chairman, vice-chairmen and members of the Independent Media Commission
Members of collegial bodies of independent agencies, of public enterprises at the central and local level, chief executives of public enterprises at the central and local level, secretaries of public enterprises at the central and local level, members of regulatory authorities, members of other Commissions or Agencies established by law or bylaw	Deputy municipal mayors, chairmen, vice-chairmen, directors of municipal directorates
Rectors and vice-rectors of public universities, members of the governing councils of public universities, deans and vice-deans and secretaries of universities public and academic units	The leaders of all departments, directorates, audit units and units equivalent, finance, budget leaders in all public institutions in the local and central level and in public enterprises at the local and central level
Leaders and responsible persons of public procurement	Deputy directors, regional directors and managers in the Customs and Tax Administration of Kosovo*
Those appointed by the President, the Assembly, the Government Cabinet, the Prime Minister and the	

ministers, means all appointees whose positions are equivalent to those specified in paragraph 1. of Article 3	

* All officials who are executors/deputies in positions listed in Article 3 paragraph 1 that exercise their duties for more than three (3) months must declare their assets not later than thirty (30) days from the day when the period of incumbency exceeds three (3) months
* Senior officials that are appointed by decision and do not have citizenship of Kosovo* are not under the obligation to declare their assets

Public officials as declarants	
Licensed doctors practicing in public institutions at the secondary and tertiary level	Professors at public universities, including assistant professor, professor of associate and full professor
Forensic and forensic psychiatry experts	Internal auditors as well as auditors in the national audit office
Police inspectors	Central and local level inspectors from the Prime Minister's Office, ministries, judicial and prosecutorial system, executive agencies, independent agencies, commissions, inspectors in municipalities and various regulators established by law
Public procurement officials in all public institutions at the local and central level and in public enterprises at the local and central level	Experts of the Public Procurement Review Body
Managerial positions in courts and prosecutor's offices	Customs officials, tax inspectors as well as police investigators, and
Heads of units and officials performing investigation, inspection, licensing tasks, verification or certification in the Office of the Prime Minister, the ministries, the judicial system and prosecution, executive agencies, independent agencies, commissions, inspectors in municipalities and various regulators established by law	

* The Agency determines and regularly updates the list of positions for which declaration is required of the property according to this article, through a by-law approved by the Director of the Agency. Agency ensures that the list will be public and accessible, while the holders of those positions are notified by contact officers.

* Public officials appointed by decision and who do not possess the citizenship of Kosovo* are not obliged to declare assets.

Asset declaration – forms and content

The content of the asset declaration is determined in accordance with Article 6 of the Law and the Agency has created an appropriate form for it.

Asset declaration content	
Name and surname of the declarant, date of birth, personal number, civil status, name of one parent and fiscal number, if any	Name and surname of declarant's family members, date of birth, personal number, marital status and relationship with the declarant
Address of permanent residence and address of	Current position and other functions in the public and private sector, including the time period of exercising

any temporary residences	the function
Data on ownership, co-ownership or shares, management positions or other rights in any company, private institution or any other private activity with a description of the activity, declaration of businesses regardless of their status in the Agency responsible for registering businesses, as well as a description of the registered name or the name of the organization	Data on ownership, co-ownership or shares and rights that businesses or other entities from sub-paragraph 1.5. hold in another company, institute or private activity, with the description of the registered name or the name of the organization
Beneficial ownership, including ownership or co-ownership, as well as savings of family members	Net personal income for the year, from salary or participation in boards, commissions or any other activity that brings net personal income, including payments for trips abroad divided by trips, as well as details of other payments or allowances for participation in commissions and other similar groups. Income for each commitment is declared separately
Immovable property and real rights thereon, including information on the area in square meters or hectares, as the case may be, the plot number, the origin and/ or the manner of acquisition, the year and price of acquisition and the previous owner from whom the property was acquired	Movable property, including any separate part of movable property, including information on the origin and/or method of purchase or benefit, year of purchase and purchase price and the previous owner from whom the property was acquired
Ready cash, cash deposited in the current account and savings, as well as savings and interest earned from domestic and foreign deposits in the country, including in foreign currency, accounts in non-resident banks, dividends, savings from participation in pension schemes in trusts or other savings for yourself and other family members whose total value exceeds three thousand Euro (€3,000)	Data on ownership, co-ownership or shares and rights that declarants and their family members have in another company, institute or private activity, with the description of the registered name or the name of the organization, as well as investments in these shares
Types and values of securities and stocks, including securities issued by a foreign government and corporate bonds, if at the time asset declaration their total value exceeds the amount of three thousand euros (€3,000)	Debts, obligations or guarantees received, loans and borrowings encumbering the declarant's ownership, possession or use of the property, or extinguished immovable or movable property whose value exceeds the amount of three thousand euros (€3,000)
Expenses, donations and all transactions made during the reporting period, with value exceeding the amount of three thousand euros (€3,000)	Donations made to any political entity, regardless of donation type and value
Rights and revenues realized from intellectual property rights, if during the declaration period their total value exceeds three thousand euros (€3,000)	Types and values of digital currencies, if at any time within the period of declaration their total value has exceeded three thousand euros (€3,000)

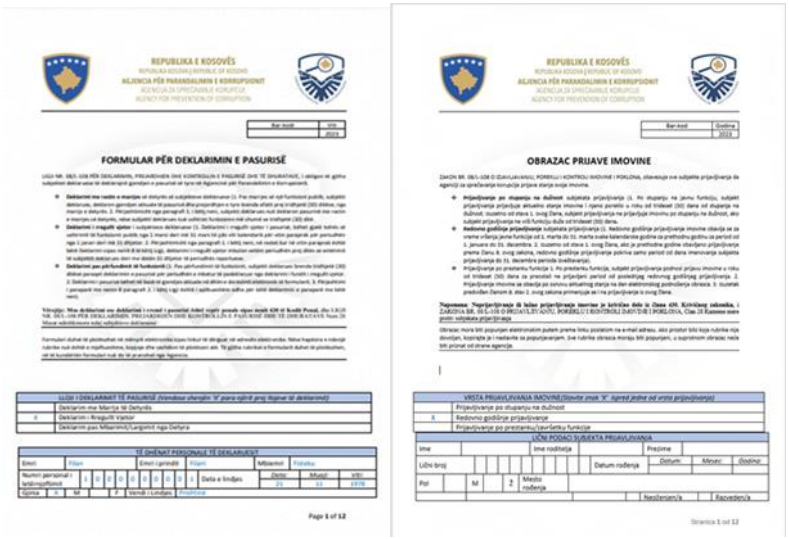
* In the asset declaration the declarant shall include data on the origin of the wealth and revenues used for the purchase of movable and immovable property which the declarant must declare according to this law. Data on inherited property shall include data on the type and value of the inheritance, including from whom it was inherited.

* All property values must be declared according to the amounts stated in the contract or invoice, also stating the year of benefit. If it is not possible to determine the value of the property, due to it being acquired through the process of inheritance, donation or similar, it must be reported with a detailed description, including the year of the benefit and how it was earned.

* For all the data presented in the property declaration form, the declarant must provide the relevant evidence of origin of the property according to the request of the Agency.

* The Agency may request any data mentioned in the content of the asset declaration in order to verify their accuracy, including bank statements the declarant submits to the Agency upon request, for all accounts in domestic and international banking/financial institutions, for himself and his family members.

* Bank statements are provided only for the purpose of full audit according to this law in order to verify the data included in the asset declaration and only for the period while the declarant holds public office.



Public officials must declare the assets of any family members living in the same household (spouse; extramarital spouse; parents and children).

According to Article 7 of the law, declarants must submit an asset declaration on 3 (three) occasions: upon taking office; regular annual declaration; upon termination or dismissal from public office.

- Declaration upon taking office

Upon taking public office, the declarant declares the current status of his/her assets and their origin within thirty (30) days from taking office. If the declarant does not remain in office for more than thirty (30) days, he/she does not have to make an asset declaration upon taking office.

- Regular annual declaration

The regular annual asset declaration is made while holding the public function from 1 March to March 31 of each calendar year for the previous year for the period from January 1 to on December 31. If asset declaration was made in the previous year according to Article 8 of the Law (*Declaration upon taking office*), the regular annual declaration covers only the period from the day of appointment of the declarant until 31 December of the reporting period.

- Declaration upon leaving public office

After the end of the function, the declarant submits the declaration within thirty (30) days, covering any property for the period remaining undeclared from the last regular annual declaration. The asset declaration is made based on the current status on the date of electronic submission of the form.

Declarants must electronically declare their assets using the Agency's electronic declaration system in accordance with Article 11 of the Law. The asset declaration is monitored and controlled by the Agency, which has access to data from all asset declarations of the declarants.

Each declarant has a secure and individual access to the electronic asset declaration system and has unlimited and full access to his/her own declaration. All data entered in the asset declaration by the declarant is stored in electronic form.

Data publication

In accordance with Article 12 of the Law - Publication of asset declarations, asset declarations are published on the online platform not more than thirty (30) days from the declaration deadline. Regarding paragraph 2 of this Article, "the following data are not published: date of birth; personal number; address and name of family members."

Also, paragraph 3 of this Article states that *"Declarants from the ranks of the Kosovo* Intelligence Agency or the Forces Security or their family members who hold confidential positions must declare their assets according to this Law, but their declaration is not public."*

Declarants' data published on the online platform will remain available for three (3) years after the end of the legal obligation to declare and must be removed from the online platform thereafter.

Data verification

The procedure for verification of asset declaration data is set out in the provisions of Article 18 of the Law - Full audit of declared data. Regarding this Article, the Agency performs a full audit of asset declarations made by declarants and their family members.

The full audit serves to verify the authenticity and accuracy of the data provided in the declaration form, compare that data with previous forms, as well as any data that was requested in the statement but not presented. The full audit includes issues related to the origin of assets and covers the period from the last full audit, if any. Otherwise, the full audit is done from the first declaration made upon appointment.

Also, the Agency carries out the full audit of assets by undertaking investigative administrative actions in order to verify the origin of assets by processing the data made available from various sources, including state institutions and other public authorities, as well as other data / information that the Agency obtains in different ways.

Data and information requested and made available by institutions or other persons are only related to the information included in the asset declaration.

In case of suspicion that a declarant is concealing assets or their origin, the Agency can conduct a full audit of the declaration of the declarant or his family members, ex-officio or according to information received.

Asset declarations and any data which are not published according to paragraph 3 of Article 12 of this Law can be used and processed further only for purposes of investigation and prevention of corruption or control of possible conflicts of interest of the senior public official in connection with the exercise of public functions.

According to Article 19, during the control of the declarant, the Agency requests data and information about the asset declaration and the sources of origin and checks the accuracy of these statements. In the event of a full assets audit, within fifteen (15) days from the Agency's request the declarant must provide relevant evidence for the required data, including bank statements for all bank accounts declared according to Article 6 of this Law. Failure to provide the clarifications and data required in paragraph 2 of this Article is considered grounds for the initiation of relevant procedures provided for by this Law.

Central and local bodies, public sector institutions, holders of public authorizations and other legal entities, whether public or private, must submit all the necessary data free of charge, including personal data and documents required for the execution of the Agency's responsibilities. This submission must take place within eight (8) days following the request and must comply with the provisions of other relevant laws.

Data protection

Law no. 08/L-108 - On the Declaration, Origin and Control of Property and Gifts (Official Gazette/ no. 21/10 August 2022) follows the provisions of the Law no. 06/L- 082 - On Personal Data Protection (Official Gazette/no.6/25 February 2019).

In relation to the above, the Law on the Declaration, Origin and Control of Property and Gifts complies with the General Data Protection Regulation (GDPR) (EU) 2016/679 and follows the principles it proclaims.

In terms of data protection, this Law stipulates that the Information Society Agency shall implement suitable technical and organizational measures to ensure data protection, and it will also carry out audits of the online platform's information technology. Furthermore, the Law stipulates that the processing of personal data found in the registry is in accordance with the Law on Personal Data Protection.

6.3.2 Technical

6.3.2.1 IT infrastructure

The information system for collection and verification of asset declaration data and supporting IT services are hosted at the Agency for Prevention of Corruption of Kosovo* (hereinafter: APK).

The APK data centre is located on its premises. Equipment in the data centre is surge protected by rack-mounted UPS devices and supplied by a generator that provides backup power in case of a mains power outage. Cooling of the data centre equipment is performed by professional air-conditioning systems. Technical protection of the data centre is achieved by an electronic access control system. Video surveillance and anti-burglary protection is currently not installed. The data centre has a fire alarm system, but lacks the NOVEC-based fire extinguishing system.

Hardware and network infrastructure in the datacentre consists of:

- Servers - virtualization hosts (3 x HPE ProLiant DL380 Gen 10)
- Storage system (1 x HPE MSA 2060 Storage) directly attached to servers via iSCSI[34].
- Core/aggregation/access switches
- Network and infrastructure security

Existing servers are relatively new (3 years old) and reach up to 70% of consumption of hardware resources. The storage system is also 3 years old and its disk storage capacity is almost half-full (40%).

Most of the critical server, storage and network components in the data centre are designed and configured as high-availability.

The disaster recovery centre has not been established yet.

Data centre processing capacity is optimized and consolidated to maximize the utilization of installed computing nodes in the server farm, reduce electricity consumption and maintenance costs by using a virtualization platform.

Core/aggregation/access switches (3 x Cisco Catalyst 9200 48-port) perform intelligent routing and filtering of traffic between different IP subnets (VLANs) and provide all LAN connections to virtualization hosts, storage systems, firewall LAN segments and management, etc. These switches are 3 years old.

The data centre has a fibre-optic link (10 Gbps download/1 Gbps upload) to AIS. VPN Site-to-site tunnels are established on firewalls to encrypt network traffic between APK's data centre and AIS' data centre. A single next-generation firewall device (1 x Cisco Firepower 1000 series, 3 years old) is leveraged to detect and block external sophisticated attacks by enforcing security policies at the application, port and protocol level, in addition to traditional functionalities such as stateful inspection of network traffic, traffic filtering, network address translation (NAT), VPN

[34] Internet Small Computer Systems Interface as a transport protocol that provides for the SCSI block protocol to be carried over a TCP-based IP network. iSCSI traffic can be run over a shared network or a network dedicated to storage. However, iSCSI does not support file access Network Attached Storage (NAS) or object storage access.

termination, Quality of Service, etc. This firewall provides remote access VPN to authorized APK employees to reach IT services hosted on the internal network from outer networks, once approved and allowed by the AIS system administrators[35]. External maintenance vendors also have limited access to the internal network through remote access VPN. Two Cisco ISR 1100 series routers (3 years old), configured in high-availability mode, perform routing of traffic from LAN towards the AIS network.

APK users and IT systems access the Internet via the Internet access point and proxy installed in the AIS using the aforementioned secure WAN link.

Microsoft Windows Server-based Active Directory is used for centralized management of user, password, workstation and server operating system settings through the enforcement of so-called "group policies". Active Directory Domain Controllers have been installed as virtual machines on the virtualized infrastructure to perform the aforementioned roles as well as dynamic allocation of IP addresses to internal hosts - Dynamic Host Configuration Protocol (DHCP) server and Domain name to IP address (and vice versa) resolution – Domain Name System (DNS).

APC uses an email server hosted by the AIS for all government and public administration institutions. Mail security and antimalware protection of the email server is provided by the AIS as well.

Antimalware protection is applied to workstations and servers. The above next-generation firewall represents an additional layer of network and application protection from malware and other forms of cyber threats.

Windows Server Update Services is deployed to download Microsoft product security and other update packages from the Official Microsoft sites and update workstation/ server operating systems and Microsoft-based services in accordance with patch management policies.

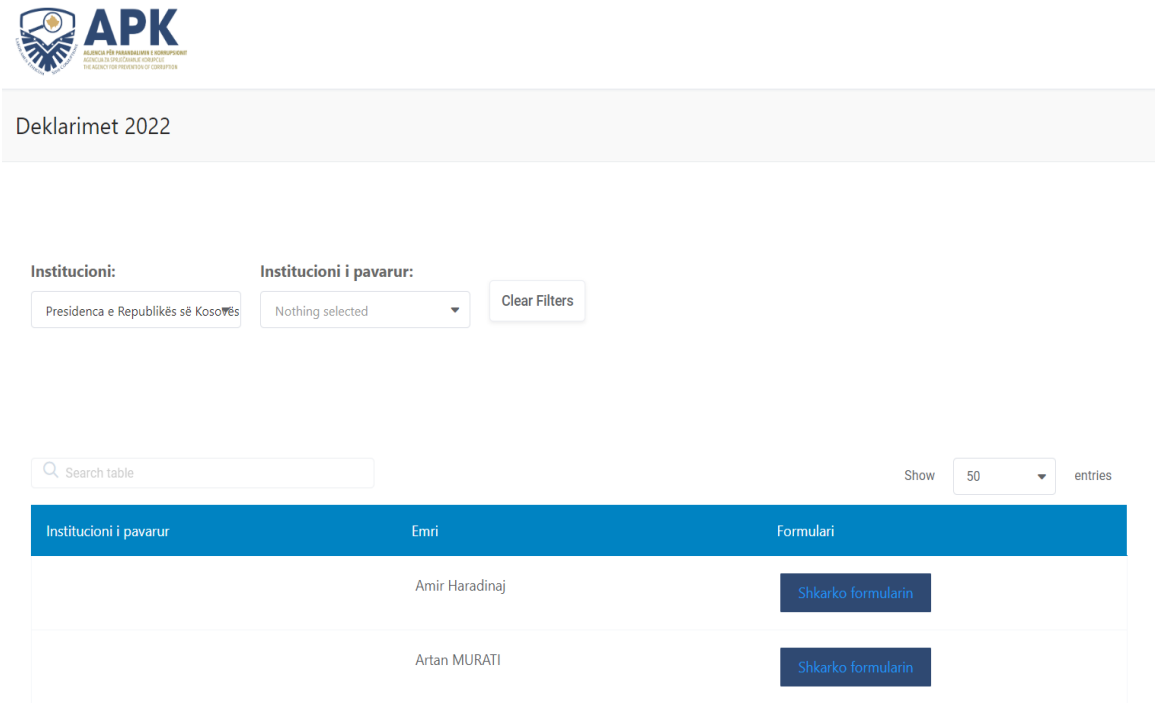
Specialized backup software is used for backing up the system and data on the dedicated backup storage (HPE Storage Once 3620 System Backup Solution, 3 years old).

6.3.2.2 Electronic system for collection, verification and exchange of asset declaration data

Following the enactment of the Law on Declaration, Origin and Control of Assets and Gifts, the Agency for Prevention of Corruption of Kosovo* launched an electronic asset declaration and verification system in 2023. According to the Law, public officials have an obligation to declare their assets electronically using this system. After entering data in the electronic system, it creates a PDF form with pre-populated data. Public officials have to print the exported PDF form, sign it and send it to the Agency for Prevention of Corruption of Kosovo* by registered mail. Public officials need to register to the asset declaration system before they can log in. For authentication they use their username and password created during the user registration process. Asset declarations are published on the website of the Agency for Prevention of

[35] AIS is responsible for management and administration of the jurisdiction wide area network connecting government and public administration institutions.

Corruption. Personal data such as personal numbers, date of birth, address and names of family members are not published.



*Access to asset declarations of the public officials via the website of the Agency for Prevention of Corruption of Kosovo**

Asset declaration and verification module is part of the Data Management System of the APK (hereinafter: *DMSA*). DMSA is developed by an outsourced partner. Development technology is Microsoft .NET framework, while Microsoft SQL Server is used as RDBMS. Load balancer/Reverse Proxy performs load balancing of web traffic between multiple web servers.

DMSA **supports** the following functionalities:

- Document Management
- Workflow Management
- Email or in-application notification for new tasks or alarms received
- The system provides user directions with respect to what next steps in the procedure should be undertaken and within which deadlines.
- Searching (including full-text search) and/or filtering of the data
- Calendar and scheduling of events
- Personal cabinet/dashboard
- Merging and splitting of cases/records
- Scanning of incoming paper documents
- OCR of the scanned documents
- Multilingual (Albanian, Serbian and English) support for menus and data fields

DMSA **does not support** the following functionalities at the moment:

- Support for BPMN
- Business Rules Management
- Option to define, create and maintain templates the users can use in their everyday life to generate specific content.
- Capability to prepare documents in a visual online rich text editor capable of combining static text and metadata in a dynamic template.
- Ability to manage documents in workgroups (multiple author participation), to facilitate document control, auditing, editing and timeline management.
- Identifying, classifying, storing, securing, retrieving, tracking, labelling and reporting of collected content for the purposes of process logs.
- Electronic archiving (classification and archiving of closed cases/records).
- Capability to sign, seal, store and transfer selected electronic documents using a qualified electronic certificate and qualified electronic time stamp.
- Capability to identify, accept and exchange signed messages with certification authorities (CA) registered in the National Register of Qualified Trust Service Providers.
- Capability to automatically check the validity of electronic signatures and electronic seals.
- Supporting roles and user profiles by granting access to resources (both functionality and data) related to specific profile combining the role and the user.
- Capability to define/select a group of cases /records under specific conditions and to perform a task over the selected cases/records to support consistent case/records operations.
- Data encryption is not supported but the APK is currently working on implementation of this functionality.
- Compliance with WAI (Web Accessibility Initiative) level A1 – accessible by people with disabilities.
- Remote (Out-of-office) access to users enabled via the Internet
- Ad-hoc Reports & Statistics (Tools for ad hoc analysis that can be used to create a non-predefined report or to drill deeper into a static report to get details about case data, transactions or records).
- Datawarehouse & Business Intelligence (Datasets included into DW/BI)

6.3.2.3 Interoperability infrastructure and data exchange with the relevant national registries and databases

APK's DMSA system currently retrieves and verifies information by integrating with the national GSB platform (Government Gateway) from the following national registers:

- CITIZEN (CIVIL) REGISTER (personal IDs, IDs for foreigners, passports, personal ID number, residence)
- CITIZEN PERSONAL STATUS REGISTER (birth, marriage, death)
- REAL ESTATE REGISTER

CITIZEN (CIVIL) REGISTER - question	CITIZEN (CIVIL) REGISTER - answer
Is external system data available in machine-readable format	Yes ☒
External system MIDDLEWARE	
Data exchange type	API web service ☒
Type of web service, if applicable	SOAP ☒
Web service architecture, if applicable	Peer to peer ☒ via GSB (ESB) ☐
Data format used	XML ☒
Communication protocol used	HTTPS ☒
Implemented security features	Authentication ☒ Authorization/access control ☒ SSL/TLS ☒ Data integrity/Signed by digital certificate ☒
Authentication used	Username ☒

DMSA will be capable of retrieving data from other relevant registers once these registers are published and made available via the GG.

Information on the availability of national registries mainly used in the asset declaration verification process on the GSB platform or in electronic form is presented in the following table:

Electronic registry	Available in the electronic form	Published on the GSB and available to DMSA
CITIZEN REGISTER (personal IDs, IDs for foreigners, passports, personal ID number, residence)	Yes	Yes
CITIZEN PERSONAL STATUS REGISTER (birth, marriage, death)	Yes	Yes
REGISTER OF MOTOR VEHICLES	Yes	No
REGISTER OF SHIPS/VESSELS	Yes	No
AIRCRAFT REGISTER	Unknown	No
REAL ESTATE REGISTER	Yes	Yes
REGISTER OF SECURITIES	Yes	No
TAX ADMINISTRATION REGISTERS	Yes	No
REGISTER OF BUSINESS ENTITIESS	Yes	No
CENTRAL BANK REGISTER OF COMMERCIAL BANK ACCOUNTS	Unknown	No
SOCIAL WELFARE REGISTER	Unknown	No
REGISTER OF INTELLECTUAL PROPERTY	Unknown	No

6.3.2.4 IT governance, information security, data protection

APK's IT Department is responsible for operational management and support for DMSA and the underlying infrastructure. IT Department has only 1 staff member, the Administrator/IT Systems Manager. This number is definitely not enough to ensure adequate management and support of numerous systems and technologies used within the institution. Furthermore, due to mostly salary constraints for IT professionals in the civil service, APK is not capable of attracting experienced IT engineers to develop and administer its information systems, IT infrastructure and IT security systems. Hence, it strongly relies on outsourcing partners for development and maintenance of the applications, databases and IT infrastructure.

APK must coordinate its activities related to network management, hosting of specific IT services (email, etc.) and electronic data exchange with other national registries with the AIS, which is responsible for operational management of Kosovo* digital services infrastructure such as eKosova portal, Government Gateway, Active Directory, Public Key Infrastructure that issues electronic certificates for public administration and the state data centre.

IT Department provides user support for DMSA usage. Additional training for existing staff and DMSA training for new staff is provided by the IT Department.

APK has not provided information about the annual budget for capital and operational expenditures for the information system and IT infrastructure.

APK has not been able to provide answers to questions related to information security in the submitted questionnaire, because this information is treated as confidential and not shared with third parties. However, APK has implemented many information security and data protection controls such as physical security of the data centre, deployment of next-generation firewalls, antimalware protection, backup, etc.

6.3.2.5 E-Government

The e-Government Strategy Kosovo* 2023-2027 was adopted in 2023 as an instrument to achieve the vision set out in the Digital Agenda of Kosovo* 2030 to transform Kosovo* into a successful digital society. Kosovo* has made good progress in the digitalisation of public administration by defining digitalisation as one of its priorities, but the strategy highlights opportunities for a more coherent and systematic approach to digitalisation in the public sector to further boost digitalisation efforts. The e-Government Strategy 2023-2027 focuses on citizens to whom digitalisation should provide tangible benefits in their day-to-day life. This includes redesigning digital services provided by the public administration following a more user-centric approach and helping to raise competencies in various topics, from digital services to cybersecurity.

In the recent years, the Government of Kosovo* has prioritised public administration reforms to transform its public sector into a more modern, efficient and citizen-centric administration and supported the use of information and communication technology (ICT) in public service delivery. In addition to the Public Administration Reform Strategy 2022-2027, there is the Administrative Burden Prevention and Reduction Programme 2022-2027 which was also approved at the end of

2022. It aspires to improve service delivery to citizens and businesses by developing, implementing and effectively reviewing public policies. The Administrative Burden Prevention and Reduction Programme 2022-2027 outlines the principles that will be used to prevent and reduce administrative burdens: the European Commission (EC) e-government principles and the general administrative principles for electronic governance.

Kosovo* has adopted laws and regulations related to electronic documentation, electronic signature, data protection and cybersecurity that are aligned with international standards and EU regulations.

Office of the Prime Minister (hereinafter: *OPM*) is primarily responsible for setting the vision for the e-Government Strategy and leading the consultation process with stakeholders. The Digital Transformation Unit (hereinafter: *DTU*) has been established in the Office of the Prime Minister to support the OPM in the coordination of digital government initiatives led by ministries, departments and agencies. The Digital Transformation Commission (hereinafter: *DTC*) was established for a high-level overview of digitalisation within the government. DTC's responsibility is to review and approve strategic priorities and new policy initiatives and financing of the government in the field of ICT and digitalisation. It reviews the implementation of relevant strategies and provides strategic direction and inter-institutional coordination in important projects. When it comes to operational bodies, the Agency for Information Society (hereinafter: *AIS*) is an executive agency within the Ministry of Internal affairs. Its duties include coordinating technical policies related to ICT in the institutions of Kosovo*, managing and supervising the implementation of projects related to ICT in institutions, supporting the development of ICT infrastructure, expansion of Internet services, administration and storage of data in the State Data Centre, etc.

Central and local governments currently provide over 700 services to businesses and citizens, but only 10 per cent of these services are provided online. A limited number of transactional services are available online and through one-stop-shops. Many online services are provided through individual agency portals, making data transfers across agencies difficult.

Currently, the dedicated governmental network is used by all governmental entities and enables secure communication between different institutions. The interoperability platform – Government Service Bus has been in place since 2017. GSB is the core back-end integration solution, but many services still remain to be connected, such as tax-related information systems. The e-Kosova portal is a single access point to transactional and personalised digital governmental services from all levels of government (state, regions, municipalities), providing more services to institutions and businesses. Citizens can log in, after completing the registration process, to the eKosova portal using a username and password, eID or a digital certificate issued by the eKosova PKI infrastructure. The eKosova platform has been integrated with the GSB, allowing full interactivity between the already connected electronic registers as well as the ePayment platform. However, Government enterprise architecture and interoperability framework are still missing or outdated.

The Civil Registry Agency has implemented a Public Key Infrastructure (PKI) used with national ID cards (eID). Additionally, AIS has implemented an internal PKI to be used for government systems and authorized government officials and agents (public notaries).

Key electronic registers (civil register, business register, tax register and cadastre) have been established and are functional. But interoperability is at an early stage of development. So far, the AIS has managed to interconnect the Civil Registry with the Kosovo* Business Registry, and the Customs Registry with the Food and Veterinary Agency Registry.[36] Several key agencies (e.g. Tax Administration, Civil Registry Agency, Kosovo* Cadastre Agency) have developed their own mini Gateways or interfaces, since their information systems were operational long before the establishment of the shared platform.

6.4 Moldova

6.4.1 Legal

6.4.1.1 Competent authority

The National Integrity Authority was established through the reorganization of the National Integrity Commission, succeeding its rights in accordance with the Law on the National Integrity Authority. The aim of this reorganization was to strengthen the independence and role of the Authority. This Law was adopted on 17 June 2016, came into force on 1 August 2016 and introduced a new mechanism for controlling assets and personal interests.

The National Integrity Authority is a public authority independent from other public organizations, other public or private legal entities and natural persons, which functions at the national level as a single structure.

The National Integrity Authority has a mission to ensure integrity in the execution of public functions or offices and to prevent corruption. This mission is accomplished through the oversight of assets and personal interests, as well as by ensuring compliance with the legal framework related to conflicts of interest, incompatibilities and restrictions.[37]

Competences:

According to Article 6, the Authority shall be assigned with the following functions:

a) exercising control of assets and personal interests;
b) checking compliance with the legal system on conflicts of interest, incompatibilities and restrictions;
c) finding and sanctioning any breach of the legal system on assets and personal interests, on conflicts of interest, incompatibilities and restrictions;
d) cooperating with other institutions, at both national and international level;

[36] World Bank, Strengthening the Enabling Environment for Digital Governance of Public Service Delivery, October 2019
[38] https://ani.md/en

e) ensuring proper organization of the Authority and managing operations involving the promotion of integrity of the declarants;
f) other functions established by law.

Related to Authority's duties in the exercise of control of assets and personal interests, the Authority shall:
a) collect, store and publish all declarations of assets and personal interests on its web page and shall ensure their permanent accessibility, except for the information and categories of declarations referred to in Article 9 (2) and (3) of the Law on Declaration of Assets and Personal Interests;
b) control the timely submission of the declarations of assets and personal interests;
c) conduct checks on assets held by the declarants, ascertain if there is any substantial and unjustified difference between the income gained during the exercise of a mandate, public function or office and the assets acquired in the same period and shall refer to the court with requests for an order to seize unjustified assets;
d) establish the existence of errors or missing data in the declarations of assets and personal interests and inform the prosecution body and/or the tax authority thereof in order to establish the existence of any crime and/or to check compliance with the fiscal regime;
e) establish contraventions regarding any breach of the legislation on assets and personal interests that fall under its competence, in accordance with the Contravention Code of the Republic of Moldova;
f) keep the electronic Register of Subjects of Declarations of Assets and Personal Interests.

6.4.1.2 Legal framework

- Law no. 132 - On the National Integrity Authority ("Official Gazette" no. 245-246/2016, Amended LP178/2017; LP238/2018; LP265/18; LP244/2020; LP130/2021; LP96/2022; LP52/2023)

This law regulates:

- The mission, functions, powers, organization and operation of the National Integrity Authority;
- The procedure for monitoring personal assets and interests, along with the verification of compliance with the legal framework concerning conflicts of interest, incompatibilities and restrictions.

Chapter IV, section 1 of this Law contains provisions about the inspection of assets and personal interests.
Inspection of assets and personal interests shall consist of control of the declarations, data and information about the existing assets, as well as of any changes which occurred during the mandate, public function or public office.

- Law no. 133 - On the Declaration of Assets and Personal Interests ("Official Gazette" no. 245-246/2016, amended LP66/2018; LP244/2020; LP130/2021; LP96/2022; LP336/2022)

This Law regulates:

- The obligation and procedure for declaring assets and personal interests by the declarant, as well as by their family members and cohabitants;
- The mechanism for checking the assets acquired by the declarant, their family members and cohabitants while exercising a mandate, public position or public office and checking compliance with the legal system on conflicts of interest, incompatibility and restrictions.

The purpose of this law is implementation of measures aimed at the prevention and combating of unjustified enrichment, conflicts of interest and incompatibility, as well as of violations of the legal system on restrictions.

Declarants

Article 3 of this Law defines declarants as follows:

Declarants	
Those who hold a public office pursuant to the provisions of the Addendum to Law No 199 of 16 July 2010 on the status of persons holding public office	Members of the Council of Observers of the National Audiovisual Public Institution "Teleradio-Moldova", institution Teleradio-Gagauzia; counsellors in village (commune), city (municipal) and district councils; deputies of the People's Assembly of the territorial self-governing unit of Gagauzia;
Members of the Superior Council of Magistrates and of the Superior Council of Prosecutors from among the teachers, as well as the members of the bodies operating under the Superior Council of Magistracy and the Superior Council of Prosecutors	Heads of public organizations and their deputies
Personnel from the cabinets of persons holding a public function	Public officials, including those with special status
Members of the Integrity Council;	Members of the boards/commissions for admission into a profession, evaluation, disciplinary and/or ethics boards of the professions associated with justice

* The above subjects shall be included in the electronic register of subjects of declarations of assets and private interests, kept by the National Integrity Authority

Asset declaration – forms and content

Regarding Article 5 of the Law no. 133 - On the Declaration of Assets and Personal Interests, *„Declaration of assets and personal interests is a personal and irrevocable act of the declarant submitted at his own responsibility in the form of an electronic document or in written form on paper. Declarants shall declare their assets and personal interests in accordance with the form provided in Annex 1 to the Law.*"

Declaration of assets and personal interests - content	
Income gained by the declarant together with their family members or cohabitant in the previous fiscal year	Movable and immovable goods, including any incomplete ones, owned with right of usufruct, of use, habitation, superficies by the declarant, including as beneficial owner, or by his/her family members or by his/her cohabitant or in their possession based on mandate, commission or trust agreements, as well as based on translative agreements of possession and of use
Goods transferred by the declarant whether for a consideration or free of charge, personally or by his/her family members or his/her cohabitant to any natural person or legal entity during the declaration period, if the value of each assets exceeds the value of 10 average national salaries	Financial assets of the declarant, namely the monetary amount in the national currency or a foreign currency which exceeds the value of 15 average national salaries and which does not represent the object of a deposit in a financial institution. Bank accounts, creation units in investment funds, equivalent forms of investments and savings, investments, bonds, checks, bills of exchange, loan certificates, other documents that include personal patrimonial rights of the declarant, of his/her family members or of his/her cohabitant, direct investments in the national currency or in a foreign currency, made by him/her or by his/her family members or his/her cohabitant, as well as other financial assets, if their combined value exceeds 15 average national salaries
Personal debts of the declarant, his/her family members or his/her cohabitant in the form of any debt, pledge, mortgage, guarantee issued for the benefit of a third party, loan and/or credit, if the value of the same exceeds the value of 10 average national salaries	Goods in the form of precious metals and/or stones, art and cult objects, objects that are part of the national or universal cultural patrimony, whose unit value exceeds the value of 15 average national salaries, held by the declarant in person or by his/her family members or his/her cohabitant
Collections of works of art, coins, stamps, weapons or other goods whose value exceeds 20 average national salaries, held by the declarant or by his/her family members or cohabitant;	Share/shares in the share capital of a company owned by the declarant either personally or by his/her family members or his/her cohabitant
Patrimonial rights, held by the declarant either personally or by his/her family members or cohabitant, deriving from copyrights, patents or intellectual property rights	Being a member of management, administration, review or inspection bodies of non-commercial organisations or trade companies, held by the declarant or by his/her family members or his/her cohabitant
Status of an associate, shareholder or member of an economic agent, a non-commercial organization or international organization held by the declarant or by his/her family members or his/her cohabitant	Agreements, including legal support, consultancy and civil agreements drawn up by the declarant, his/her family members or his/her cohabitant, or in development during the appointment/mandate being exercised, financed by the state or local budget and from external funds or contracted with trade companies owned by the state
Services or type of services procured by the declarant and family members/cohabitant, whose cumulative value over the course of a year exceeds 10 average monthly salaries	Virtual goods, including virtual currency, the value of which exceeds 10 average monthly salaries

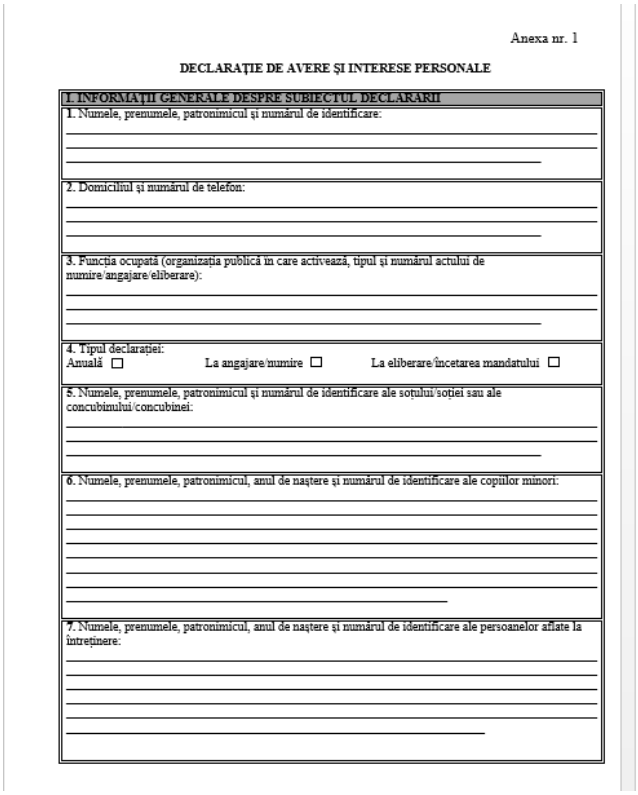
* The provisions of Article 4 paragraph (1) shall also apply to assets and personal interests of the declarant and his/her family members or cohabitant in the country or abroad.

* All presents, services and/or advantages received by the declarant free of charge from his/her family members, parents, siblings or children, whose individual value does not exceed 10 average national salaries shall be exempted from the obligation to be declared.

In accordance with Article 6 of the Law, the declaration of assets and personal interests shall be submitted as follows:

- Every year by 31 March, indicating the income earned by the declarant together with his/her family members or cohabitant in the previous financial year, assets held and his/her personal interests as provided for under Article 4 (1)(b) - (m) on the date of submission of the declaration;
- In case of employment, mandate validation or appointment to a position, as the case may be, the declaration shall be submitted within 30 days from the date of employment, mandate validation or appointment in the respective position, indicating the income gained by the declarant together with his/her family members or cohabitant during the previous financial year, as well as the assets held and his/her personal interests as provided for under Article 4 (1)(b)-(m) on the date of submission of the declaration;
- Upon changing functions within the same entity, by promotion or by appointment to another position, no new declaration shall be submitted;
- After the termination of the mandate or of the employment or service agreement, the declarant shall be under the obligation to submit the declaration within 30 days from the date of termination of the mandate, employment or service agreement. The declaration shall indicate the income earned by the declarant together with his/her family members or cohabitant in the previous financial year, the assets held and his/her personal interests under Article 4 (1) (b)-(m) on the date of its submission;
- Declarants who, pursuant to the legislation in force, have their employment or service agreements suspended, shall submit their declaration within 30 days after reappointment to their position, stating in the declaration the income earned together with their family members or cohabitant during the entire undeclared period, as well as the assets held and the personal interests provided for under Article 4 (1) (b)-(m) on the date of submission of the declaration (these provisions shall not apply if the suspension of employment or service agreement is shorter than a fiscal year).

The declarant is under the obligation to submit the declaration in electronic form using the electronic service available on the official website of the National Integrity Authority, according to the template indicated in Annex no. 1 of the Law.



Anexa nr. 1

DECLARAŢIE DE AVERE ŞI INTERESE PERSONALE

I. INFORMAŢII GENERALE DESPRE SUBIECTUL DECLARARII

1. Numele, prenumele, patronimicul şi numărul de identificare:

2. Domiciliul şi numărul de telefon:

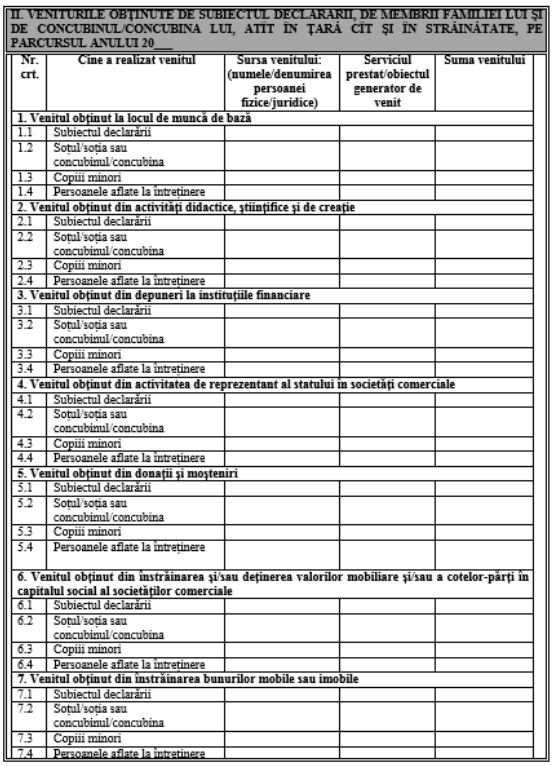
3. Funcţia ocupată (organizaţia publică în care activează, tipul şi numărul actului de numire/angajare/eliberare):

4. Tipul declaraţiei:
Anuală ☐ La angajare/numire ☐ La eliberare/încetarea mandatului ☐

5. Numele, prenumele, patronimicul şi numărul de identificare ale soţului/soţiei sau ale concubinului/concubinei:

6. Numele, prenumele, patronimicul, anul de naştere şi numărul de identificare ale copiilor minori:

7. Numele, prenumele, patronimicul, anul de naştere şi numărul de identificare ale persoanelor aflate la întreţinere:



II. VENITURILE OBŢINUTE DE SUBIECTUL DECLARARII, DE MEMBRII FAMILIEI LUI ŞI DE CONCUBINUL/CONCUBINA LUI, ATÎT ÎN ŢARĂ CÎT ŞI ÎN STRĂINĂTATE, PE PARCURSUL ANULUI 20___

Nr. crt.	Cine a realizat venitul	Sursa venitului: (numele/denumirea persoanei fizice/juridice)	Serviciul prestat/obiectul generator de venit	Suma venitului
1. Venitul obţinut la locul de muncă de bază				
1.1	Subiectul declarării			
1.2	Soţul/soţia sau concubinul/concubina			
1.3	Copiii minori			
1.4	Persoanele aflate la întreţinere			
2. Venitul obţinut din activităţi didactice, ştiinţifice şi de creaţie				
2.1	Subiectul declarării			
2.2	Soţul/soţia sau concubinul/concubina			
2.3	Copiii minori			
2.4	Persoanele aflate la întreţinere			
3. Venitul obţinut din depuneri la instituţiile financiare				
3.1	Subiectul declarării			
3.2	Soţul/soţia sau concubinul/concubina			
3.3	Copiii minori			
3.4	Persoanele aflate la întreţinere			
4. Venitul obţinut din activitatea de reprezentant al statului în societăţi comerciale				
4.1	Subiectul declarării			
4.2	Soţul/soţia sau concubinul/concubina			
4.3	Copiii minori			
4.4	Persoanele aflate la întreţinere			
5. Venitul obţinut din donaţii şi moşteniri				
5.1	Subiectul declarării			
5.2	Soţul/soţia sau concubinul/concubina			
5.3	Copiii minori			
5.4	Persoanele aflate la întreţinere			
6. Venitul obţinut din înstrăinarea şi/sau deţinerea valorilor mobiliare şi/sau a cotelor-părţi în capitalul social al societăţilor comerciale				
6.1	Subiectul declarării			
6.2	Soţul/soţia sau concubinul/concubina			
6.3	Copiii minori			
6.4	Persoanele aflate la întreţinere			
7. Venitul obţinut din înstrăinarea bunurilor mobile sau imobile				
7.1	Subiectul declarării			
7.2	Soţul/soţia sau concubinul/concubina			
7.3	Copiii minori			
7.4	Persoanele aflate la întreţinere			

Data publication

After the declarant signs the declaration of assets and personal interests , the declaration appears on the Declarations Portal which is on the official website of the National Integrity Authority. Anyone in the country or abroad can see the submitted declaration, in PDF format, without personal data which are not public.

The Authority`s obligation to publish declarations of assets and personal interests is primarily determined in Article 7 paragraph 1 of the Law no. 132 - On the National Integrity Authority: *"In the exercise of control of assets and personal interests, the Authority shall: a) collect, store and publish all declarations of assets and personal interests on its web page and shall ensure their permanent accessibility, except for the information and categories of declarations referred to in Article 9 (2) and (3) of the Law on the declaration of assets and personal interests".*
Article 9 paragraph (1) of the Law no. 133 - On the Declaration of Assets and Personal Interests - *Transparency of declarations*, prescribes that *"The National Integrity Authority publishes the declarations received on its official website within 30 days from expiry of the deadlines for submission of declarations, ensuring permanent access to them for 15 years from the date of submission, except for the data provided in par. (2) and (3)".*

Related to that, the data included in the declarations regarding the identification number assigned to the declarant, his/her permanent address and phone number, last name, first name, years of birth, addresses and identification numbers of his/her family members and of his/her cohabitant, addresses and cadastral numbers of immovable assets, registration numbers of movable assets, cash in national currency or foreign currency that is not the object of financial submissions, bank account numbers, any assets in the form of precious metals or stones, works

of art and cult objects, objects that are part of the national or universal patrimony, collections of works of art, coins, stamps, weapons and the signature of the declarant are not public and represent information with limited access.

Additionally, declarations of those declarants whose identity and quality constitute a state secret under Law no. 245/2008 on state secrets are not public.

Data Verification

Integrity inspectors of the National Integrity Authority perform the following activities: receive, collect, centralize and process data and information on the status of assets, income and expenses incurred by persons during the exercise of their terms of office, public office and public dignitary positions. This also includes assessing incompatibilities and conflicts of interest of persons holding a public office or public dignitary positions. The inspectors determine substantial differences by considering changes in the assets, income and expenses of the declared individuals during their terms of office.

Procedures for verifying the accuracy of declared assets are outlined in the Methodology for the control of assets and personal interests and addressing compliance with legal regulations regarding conflicts of interest, incompatibilities, restrictions and limitations.
As for cross-checking, this function is integrated into the 'e-Integrity' automated information system. However, due to technical incompatibility between various databases, inspector involvement is currently required for verification procedures.

Concerning this issue, Article 10 of the Law no. 133 - On the Declaration of Assets and Personal Interests - *Inspection of assets and personal interests*, refers to provisions of the Law No 132 of 17 June 2016 on the National Integrity Authority: *"The inspection of assets and personal interests of the declarant shall be conducted by the National Integrity Authority in accordance with the Law No 132 of 17 June 2016 on the National Integrity Authority*".

As mentioned, Chapter IV Section 1 of the Law no. 132 - On the National Integrity Authority, contains provisions about Inspection of assets and personal interests.

The inspection of assets and personal interests shall consist in the control of the declarations, data and information on the existing assets, as well as of the changes which occurred during the mandate, public function or public office.

The verification of the declarations of assets and personal interests shall be initiated after the expiry of the deadline for the submission of the declarations of assets and personal interests. At least 40 % of inspections of declarations of assets and personal interests carried out during a calendar year shall refer to public office holders, which will be randomly selected for ex officio control. The declarations of assets and personal interests subjected to inspection shall be distributed randomly through the electronic distribution system.

Article 32 of this Law prescribes the procedure for inspection of assets and personal interests. Regarding this procedure, the integrity inspector shall check the data and information on the existing assets of the person subject to inspection, as well as any asset changes occurring during his/her exercise of the mandate, public function or office. The inspection can be conducted during the mandate, public function or office, as well as within 3 years after its termination.

If the person subjected to inspection is married or in a cohabitation or if he/she has dependents and/or minor children, the check shall also extend to cover the assets of the family members and of the cohabitant of the inspected person.

During the inspection of assets and personal interests, the integrity inspector is entitled to request from any natural persons or legal entities governed by public or private law, including financial institutions, any documents and information required to conduct such inspection. Upon request from the integrity inspector, the above subjects shall provide to the Authority, within 15 days from receipt of such request, either on paper or in electronic format, all the required data, information, deeds and supporting documents.

The integrity inspector can also request any information necessary to conduct his/her activity from international organizations and associations, in accordance with the international treaties to which the Republic of Moldova is a party.

Data Protection

Law no. 132/2016 on the National Integrity Authority stipulates that the actions performed and the documents issued by the integrity inspector as part of asset control are not public and the documents shall be published on the official website of the Authority in compliance with the Law 133/2011 - On Personal Data Protection, including amendments (LP134/2016; LP185/2017; LP238/2018; LP124/2020; LP10/2021; LP175/2021; LP155/2022; LP60/2023).
Identification data of the complainants to the Authority are confidential unless the complainant expressly accepts or requests that his/her data be made public.

Article 37 paragraph (5) of the Law no. 132 - On the National Integrity Authority states that *"The actions and documents prepared by the integrity inspector during the asset inspection are not public, except for the ascertaining document, which shall be published on the official web page of the Authority, in compliance with the legislation on the protection of personal data".*

6.4.2 Technical

6.4.2.1 IT infrastructure

The information system for collection and verification of asset declaration data and the supporting IT services are hosted in the state-owned MCloud. The National Integrity Authority of the Republic of Moldova (hereinafter: NIA) is provided with Infrastructure as a Service (hereinafter: IaaS) consisting of virtual compute and storage nodes managed by the Information Technology and Cyber Security Service (hereinafter: STISC) cloud provider.

The state-owned fibre-optic network is used to connect NIA's Local Area Network with cloud-based resources. NIA has guaranteed speed of 1 Gbps towards the state-owned WAN network and cloud provider. VPN Site-to-site tunnels are established on the firewall to encrypt network traffic between NIA's Local Area Network and cloud provider. NIA also has 1 Gbps fibre-optic-based access to the Internet service provider. A single Fortinet Fortigate 100E Next-Generation Firewall is leveraged to detect and block sophisticated attacks by providing IPS, application control, threat protection and SSL inspection in addition to traditional firewall functionalities. Access to Internet from inner users and IT services is controlled and filtered by the web security appliance.

Microsoft Windows Server-based Active Directory is used for centralized management of user, password and workstation operating system settings through the enforcement of so-called "group policies". Active Directory Domain Controllers have been installed as virtual machines on the virtualized infrastructure to perform the aforementioned roles as well as Domain name to IP address (and vice versa) resolution – Domain Name System (DNS). A file server is deployed to store specific user files outside of the information system.

Antimalware protection is applied to workstations and servers. Endpoint Detection and Response technology is leveraged to identify suspicious behaviour and advanced persistent threats on endpoints (workstations, laptops, servers, mobile devices) in an environment, and alert administrators accordingly. NIA has also implemented Security Information and Event Management (SIEM) for real-time analysis and correlation of security alerts generated by applications and network hardware.

Specialized backup software is used for backing up virtual machines on the backup medium.

6.4.2.2 Electronic system for collection, verification and exchange of asset declaration data

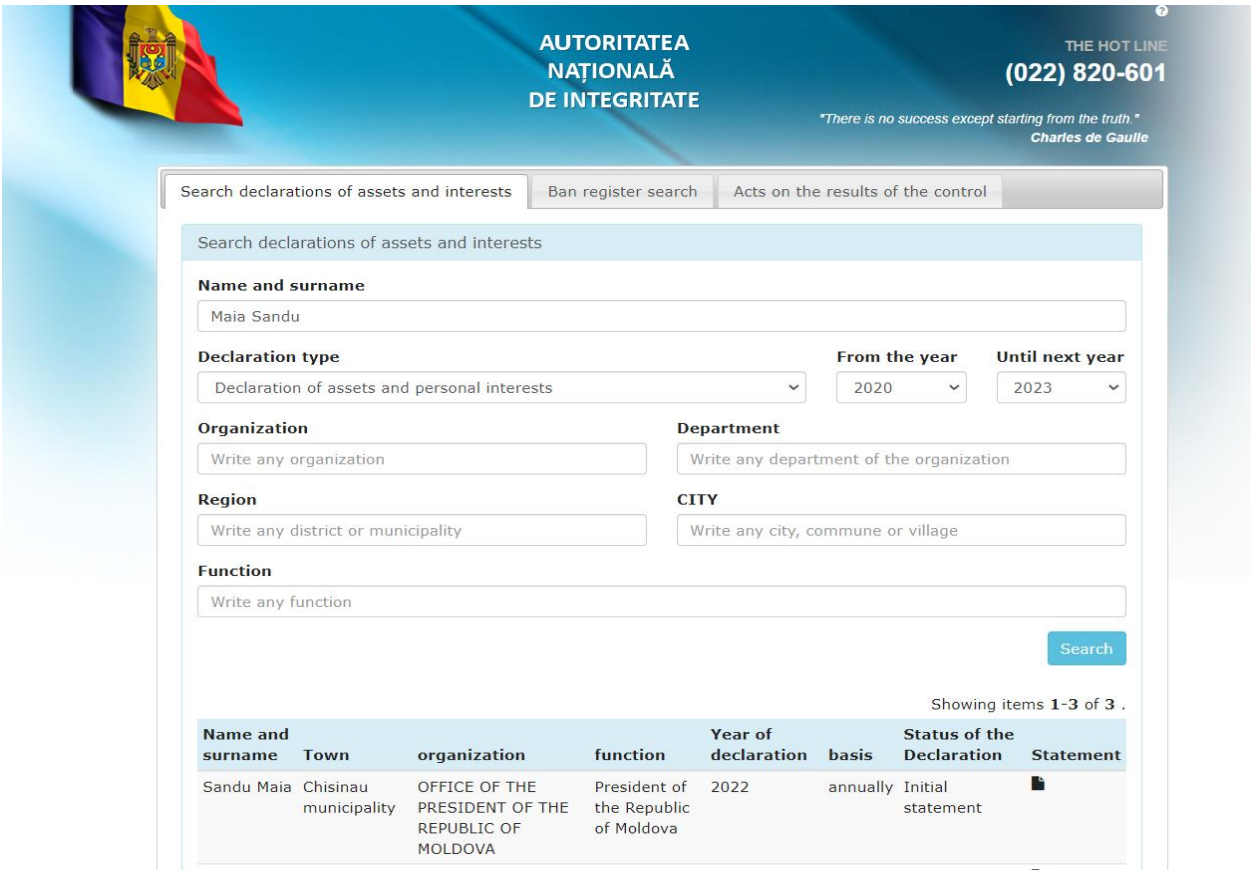
In 2018, NIA launched e-Integritate (hereinafter: e-Integrity system). The Government Decision no. 228 of 10 April 2020 approved the Regulation on the Organization and Functioning of the Automated Information System e-Integrity. The main functions of the e-Integrity system are:

- submission and signing of asset declarations by declarants
- automatic verification of declarations to detect discrepancies between the data in the declarations and the data held in state registers
- management of control files initiated based on notifications submitted by natural and legal persons or initiated by ex officio investigations
- entry and renewal of information in the electronic register of declarants
- registration, correction and removal of prohibitions to hold public positions as well as search, review and import of data to/from the register of persons prohibited from holding public positions

The e-Integrity system represents a useful tool for information and case management within the NIA. The system has several advantages and allows NIA to exceed the minimum requirements set by the law in certain aspects. For example, the e-Integrity system makes declarations of

assets and personal interests publicly available immediately after their electronic signing, although the deadline for public disclosure allowed by the law is 30 days from expiry of deadlines for submission of declarations (Article 9 paragraph 1 of the Law no. 133).[38]

The electronic asset declaration system is accessible to public officials via the NIA website.[39] Public officials have to log in to the system using a username and password or a digital certificate issued by the registered provider in Moldova. Once public officials complete an online asset declaration web form, they must sign it electronically using their electronic certificate issued by the national qualified trust services provider. Once the electronic signing process is complete, the asset declaration form is considered submitted and is automatically published on the NIA website. Public officials receive confirmation of submission of the declaration by email. Personal data, other than name and surname of the public official, are not published. Such data is blurred on the asset declaration PDF form which opens when the website user chooses to preview the public official's asset declaration. The electronic system offers the option to search asset declarations by choosing the following search parameters: i) name and surname, ii) declaration type, iii) reporting period from – to, iv) organization, v) department, vi) region, vii) city, viii) function.



Access to asset declarations of the public officials via the NIA website

[38] The project "Action against Corruption in the Republic of Moldova", Analysis of the legislative framework, procedures, organization and effectiveness of the National Integrity Authority of the Republic of Moldova, 06/2021

[39] https://declarant.ani.md/User/site/login

The e-Integrity system was developed by an outsourced partner. Object-Oriented Software Development Methodology is applied for software development. Yii2 Software LLC ® Framework [1] is used as middleware, while PostgreSQL represents the object-relational database management system. Load balancer/Reverse Proxy performs load balancing of web traffic between multiple web servers. Total hardware resources dedicated to the e-Integrity system on the virtual private cloud are the following: vCPU=71,30 GHz; RAM= 31 GB; HDD=1 524 GB; HDD offline= 8 192 GB. Expected growth of hardware resources to meet the needs of the system are: vCPU=14%; RAM= 35%; HDD=26%; HDD offline= 5%.

The e-Integrity system **supports** the following functionalities:

- Document Management
- Workflow Management
- Support for BPMN
- Business Rules Management
- Email or in-application notification for new tasks or alarms received
- The system provides user directions with respect to what steps in the procedure should be undertaken next and within which deadlines.
- Searching (including full-text search) and/or filtering of the data
- Calendar and scheduling of events
- Option to define, create and maintain templates the users can use in their everyday life to generate specific content.
- Personal cabinet/dashboard
- Electronic submission of asset declarations data and attaching documents using a web application accessible via the Internet.
- Merging and splitting of cases/records
- Identifying, classifying, storing, securing, retrieving, tracking, labelling and reporting of collected content for the purposes of process logs.
- Capability to sign, seal, store and transfer selected electronic documents using a qualified electronic certificate and qualified electronic time stamp.
- Supporting roles and user profiles by granting access to resources (both functionality and data) related to specific profile combining the role and the user.
- Support for Data Pseudonymisation
- Multilingual support for menus and data fields
- Automated, semi-automated or purely human mechanisms are implemented for monitoring the quality of data on a regular basis
- Remote (Out-of-office) access to users enabled via the Internet

e-Integrity **does not support** the following functionalities at the moment:

- Capability to prepare documents in a visual online rich text editor capable of combining static text and metadata in a dynamic template.
- Ability to manage documents in workgroups (multiple author participation), to facilitate document control, auditing, editing and timeline management.
- Electronic archiving (classification and archiving of closed cases/records).

- Capability to identify, accept and exchange signed messages with certification authorities (CA) registered in the National Register of Qualified Trust Service Providers.
- Capability to automatically check the validity of electronic signatures and electronic seals.
- Capability to define/select a group of cases /records under specific conditions and to perform a task over the selected cases/records to support consistent case/records operations.
- Data encryption
- Compliance with WAI (Web Accessibility Initiative) level A1 – accessible by people with disabilities.
- Ad-hoc Reports & Statistics (Tools for ad hoc analysis that can be used to create a non-predefined report or to drill deeper into a static report to get details about case data, transactions or records).
- Datawarehouse & Business Intelligence (Datasets included into DW/BI).

Transparency International, the media and CSOs in Moldova have requested that the published declarations be made available in machine-readable formats, which would make corroboration of information much easier. Currently, CSOs and investigative journalists spend extensive amounts of time analysing cumbersome PDF documents. Resorting to manual, selective blurring of personal information (on asset declaration forms) is one example of efficiency asymmetries in the NIA system. The NIA acknowledged this shortcoming and is looking for software solutions (AI, integrated analytics) from prospective donors to make its processes more efficient. It wants to deepen its analytics, including identifying high-risk corrupt individuals.[40]

6.4.2.3 Interoperability infrastructure and data exchange with the relevant national registries and databases

The e-Integrity system comprises a mechanism for automatic analysis of declarations which envisages comparison of asset declaration data with data from other state registers/systems (Article 18). The e-Integrity system ensures interaction and exchange of data with these systems through the governmental GSB platform MConnect.[41]

e-Integrity currently verifies information from the following national registers by calling the respective web services established via the MConnect GSB platform:

- CITIZEN REGISTER (personal IDs, IDs for foreigners, passports, personal ID number, residence)
- CITIZEN PERSONAL STATUS REGISTER (birth, marriage, death)
- REGISTER OF MOTOR VEHICLES
- REAL ESTATE REGISTER
- TAX ADMINISTRATION REGISTERS
- REGISTER OF BUSINESS ENTITIES

[40] USAID, DIGITAL ECOSYSTEM COUNTRY ASSESSMENT (DECA) MOLDOVA, November 2022
[41] Ibid

- SOCIAL WELFARE REGISTER

Technical characteristics of each web service are listed in the tables below:

CITIZEN REGISTER - question	CITIZEN REGISTER - answer
Is external system data available in machine-readable format	Yes ☒ No ☐
INSTITUTION RESPONSIBLE FOR MANAGEMENT/ADMINISTRATION OF THE EXTERNAL SYSTEM	Public Services Agency (www.asp.gov.md)
External system DEVELOPED	In-house ☒
Data exchange type	API web service ☒
Type of web service, if applicable	SOAP ☒
Web service architecture, if applicable	via GSB (ESB) ☒
Data format used	Other ☒ unknown_____
Communication protocol used	HTTP ☒
Implemented security features	Authorization/access control ☒
UDDI registry/service catalogue available at the service provider side?	Yes ☒
Web service description available in the form of WSDL file	Yes ☒
Authentication used	Username ☒
REMARK https://semantic.gov.md/en/assets/details/9d6fdb0e-a029-44ac-b490-5c15fc426ac6	

CITIZEN PERSONAL STATUS REGISTER - question	CITIZEN PERSONAL STATUS REGISTER - answer
Is external system data available in machine-readable format	Yes ☒ No ☐
INSTITUTION RESPONSIBLE FOR MANAGEMENT/ADMINISTRATION OF THE EXTERNAL SYSTEM	Public Services Agency (www.asp.gov.md)
External system DEVELOPED	In-house ☒
Data exchange type	API web service ☒
Type of web service, if applicable	SOAP ☒
Web service architecture, if applicable	via GSB (ESB) ☒
Data format used	Other ☒ _ unknown__
Communication protocol used	HTTP ☒
Implemented security features	Authorization/access control ☒
UDDI registry/service catalogue available at the service provider side?	Yes ☒
Web service description available in the form of WSDL file	Yes ☒
Authentication used	Username ☒
REMARK https://semantic.gov.md/en/assets/details/9cbf475d-1c59-4a15-862e-e798670ab2e2	

REGISTER OF MOTOR VEHICLES - questions	REGISTER OF MOTOR VEHICLES - answer
Is external system data available in machine-readable format	Yes ☒ No ☐
INSTITUTION RESPONSIBLE FOR MANAGEMENT/ADMINISTRATION OF THE EXTERNAL SYSTEM	Public Services Agency (www.asp.gov.md)
External system DEVELOPED	In-house ☒
Data exchange type	API web service ☒
Type of web service, if applicable	SOAP ☒
Web service architecture, if applicable	via GSB (ESB) ☒
Data format used	Other ☒ _unknown_____
Communication protocol used	HTTP ☒
Implemented security features	Authorization/access control ☒
UDDI registry/service catalogue available at the service provider side?	Yes ☒
Web service description available in the form of WSDL file	Yes ☒
REMARK https://semantic.gov.md/en/assets/details/8053c845-6951-4805-b9ad-12578c7bf950	

REAL ESTATE REGISTER – question	REAL ESTATE REGISTER - answer
Is external system data available in machine-readable format	Yes ☒ No ☐
INSTITUTION RESPONSIBLE FOR MANAGEMENT/ADMINISTRATION OF THE EXTERNAL SYSTEM	Public Services Agency (www.asp.gov.md)
External system DEVELOPED	In-house ☒
Data exchange type	API web service ☒
Type of web service, if applicable	SOAP ☒
Web service architecture, if applicable	via GSB (ESB) ☒
Data format used	Other ☒ _unknown___
Communication protocol used	HTTP ☒
Implemented security features	Authorization/access control ☒
UDDI registry/service catalogue available at the service provider side?	Yes ☒
Web service description available in the form of WSDL file	Yes ☒
Authentication used	Username ☒
REMARK https://semantic.gov.md/en/assets/details/8fad7c53-6882-4acc-b167-91429cc3f722	

TAX ADMINISTRATION REGISTERS - question	TAX ADMINISTRATION REGISTERS - answer
Is external system data available in machine-readable format	Yes ☒ No ☐
INSTITUTION RESPONSIBLE FOR MANAGEMENT/ADMINISTRATION OF THE EXTERNAL SYSTEM	National Office of Social Insurance (www.cnas.gov.md)
External system DEVELOPED	In-house ☒
Data exchange type	API web service ☒
Type of web service, if applicable	SOAP ☒
Web service architecture, if applicable	via GSB (ESB) ☒
Data format used	Other ☒ __unknown___
Communication protocol used	HTTP ☒
Implemented security features	Authorization/access control ☒
UDDI registry/service catalogue available at the service provider side?	Yes ☒
Web service description available in the form of WSDL file	Yes ☒
Authentication used	Username ☒
REMARK https://semantic.gov.md/en/assets/details/fa06ba87-3354-46ab-b372-86a1da749b9c	

REGISTER OF BUSINESS ENTITIESS - question	REGISTER OF BUSINESS ENTITIESS - answer
Is external system data available in machine-readable format	Yes ☒ No ☐
INSTITUTION RESPONSIBLE FOR MANAGEMENT/ADMINISTRATION OF THE EXTERNAL SYSTEM	Public Services Agency (www.asp.gov.md)
External system DEVELOPED	In-house ☒
Data exchange type	API web service ☒
Type of web service, if applicable	SOAP ☒
Web service architecture, if applicable	via GSB (ESB) ☒
Data format used	Other ☒ _unknown_____
Communication protocol used	HTTP ☒
Implemented security features	Authorization/access control ☒
UDDI registry/service catalogue available at the service provider side?	Yes ☒
Web service description available in the form of WSDL file	Yes ☒
Authentication used	Username ☒
REMARK https://semantic.gov.md/en/assets/details/17ce88fe-de47-4a4d-a5b3-feadf972dc7b	

SOCIAL WELFARE REGISTER - question	SOCIAL WELFARE REGISTER - answer
Is external system data available in machine-readable format	Yes ☒ No ☐
INSTITUTION RESPONSIBLE FOR MANAGEMENT/ADMINISTRATION OF THE EXTERNAL SYSTEM	National Office of Social Insurance (www.cnas.gov.md)
External system DEVELOPED	In-house ☒
Data exchange type	API web service ☒
Type of web service, if applicable	SOAP ☒
Web service architecture, if applicable	via GSB (ESB) ☒
Data format used	Other ☒ _unknown_____
Communication protocol used	HTTP ☒
Implemented security features	Authorization/access control ☒
UDDI registry/service catalogue available at the service provider side?	Yes ☒
Web service description available in the form of WSDL file	Yes ☒
Authentication used	Username ☒
REMARK https://semantic.gov.md/en/assets/details/fa06ba87-3354-46ab-b372-86a1da749b9c	

Information on the availability of national registries mainly used in the asset declaration verification process on the GSB platform or in electronic form is presented in the following table:

Electronic registry	Available in the electronic form	Published on the GSB and available to the IS
CITIZEN REGISTER (personal IDs, IDs for foreigners, passports, personal ID number, residence)	Yes	Yes
CITIZEN PERSONAL STATUS REGISTER (birth, marriage, death)	Yes	Yes
REGISTER OF MOTOR VEHICLES	Yes	Yes
REGISTER OF SHIPS/VESSELS	Yes	Data exchange is not available/applied
AIRCRAFT REGISTER	Yes	Data exchange in machine-readable format is not available/applied
REAL ESTATE REGISTER	Yes	Yes
REGISTER OF SECURITIES	Yes	Data exchange in machine-readable format is not available/applied
TAX ADMINISTRATION REGISTERS (Records of all taxpayers, contributions and insured	Yes	Yes

persons, data necessary for control and collection of tax payments, contributions and data for exercising rights based on compulsory and voluntary insurance)		
REGISTER OF BUSINESS ENTITIESS	Yes	Yes
CENTRAL BANK REGISTER OF COMMERCIAL BANK ACCOUNTS	There is no such external system, each commercial Bank manages its own IT system.	Data exchange in machine-readable format is not available/applied
SOCIAL WELFARE REGISTER	Yes	Yes
REGISTER OF INTELLECTUAL PROPERTY	Unknown	Unknown

e-Integrity will be capable of retrieving data from other relevant registers once these registers are published and made available via the MConnect GSB.

6.4.2.4 IT governance, information security, data protection

NIA's Information Technologies Service is responsible for operational management and support for the e-Integrity information system and underlying infrastructure. The IT Service has only 1 staff member. This number is definitely not enough to ensure adequate management and support of numerous systems and technologies used by the institution. Hence, it strongly relies on the outsourcing partners for development and maintenance of applications, databases and IT infrastructure.

NIA must coordinate its activities related to management of its virtual private cloud in the state data centre with the Information Technology and Cyber Security Service[42]. Activities related to electronic data exchange with other national registries are coordinated with the E-Governance Agency[43] and the Public Services Agency[44]

NIA has established a working group as the Change Management Advisory Body for further development and improvement of the e-Integrity information system. The institution possesses the source code for this system.

Usage and administration of the asset declaration and verification system is regulated by the implementing act.

The IT Service provides user support for e-Integrity usage. Service Desk (Ticketing) software is not implemented to track all relevant information related to submission and resolution of support and change requests. However, users can contact the Centralized Call Centre for assistance. Interactive multimedia online tutorials, help sections and FAQs are also available in the e-Integrity application and on the NIA website, as insightful knowledge management tools.

[42] The Information Technology and Cyber Security Service is responsible for management of the state data centre.
[43] The E-Governance Agency is responsible for governance/management of the Mconnect GSB
[44] The Public services Agency manages key state electronic registers.

The Directorate for Evaluation, Prevention and Implementation of Policies in the National Integrity Authority provides application-specific training for new staff or for new software features. 72 training sessions have been held in 2022, for approximately 6,867 declarants. User satisfaction surveys are not conducted at the moment to collect user feedback and new ideas for software improvements and development of new features.

NIA does not have funds allocated in its budget for digital skills or advanced IT trainings.

The table below shows the annual budget for maintenance of the information system and IT infrastructure.

Item	Amount
AIS e-Integrity technical administration services (Outsourcing)	492.960 MDL (24.648 €)
AIS e-Integrity adaptive and perfective maintenance services (Outsourcing)	450.000 MDL (22.500 €)
PC maintenance and repair services	20.000 MDL (1.000 €)
Technical information support services of local telecommunications networks	30.000 MDL (1.500 €)
Cartridge supply and regeneration services, printer repair	89.840 MDL (4.492 €)

The National Integrity Authority does not have ISO 27001 certification. However, it has developed the Security policy[45] and the Regulation[46] on the protection and data retention of personal data processed within the e-Integrity information system managed by the National Integrity Authority. The NIA has a Continuity Plan for the e-Integrity information system, developed by the Information Technology and Cyber Security Service on 01.06.2022, as the administrator of the IaaS that hosts the information system.

Management of security incidents is regulated by the aforementioned Security Policy. In the last three years 1 event was registered, qualified as an incident related to security and confidentiality of personal data in e-Integrity, which was promptly resolved by the Information Technology and Cyber Security Service together with the outsourced system developer upon notification of the incident by the NIA.

NIA has signed a service level agreement with the Information Technology and Cyber Security Service for the provision of IaaS cloud resources. Contracts with external service providers also include a service level agreement and non-disclosure agreements.

The National Integrity Authority has a person responsible for the protection of personal data, appointed by the ANI Disposition no. 7d of 22.07.2022. NIA organizes annual training activities for the institution's staff on the topic of rules of personal data protection in the process of their processing, as well as the dissemination of Best Practices and Cyber Security Guidelines.

[45] Approved by ANI Order no. 16 of 03.03.2018 (annex no. 3)
[46] Approved by ANI Order no. 16 of 03.03.2018 (annex no. 4)

6.4.2.5 E-Government

Over the last decade, Moldova's commitment to digital transformation has become increasingly clear and has accelerated at both policy and implementation level.[47] Under the new government, the Office of the Deputy Prime Minister (hereinafter: *DPM*) for Digitalization was established in August 2021—a first in the country's history. The Deputy Prime Minister for Digitalization with the Ministry of Economy oversees the synchronization of sectoral policies and strategies related to the technological modernization program of the Government of Moldova. The DPM for Digitalization also oversees the Electronic Governance Agency (hereinafter: *EGA*) and the Information Technology and Cyber Security Service, important stakeholders in digital public services and cybersecurity as well as in the maintenance and development of IT and communications infrastructure of public administration authorities. Currently, EGA's competencies include leading the digitalization and reengineering of services, developing interoperable solutions for efficiency, ensuring information security and overseeing the mainstreaming of digital inclusion initiatives. Access to key state registers for electronic services such as MPay, cadastre, registration of legal entities, or the national population register (ID cards, registration of life events) is managed by the Public Services Agency.

Moldova has established the legislative framework for digital government by adopting or amending the Law on Access to Information, Law on data exchange and interoperability, Law on Personal data protection, Cybersecurity Law, etc.

Over the past decade, the Government of Moldova (GoM) has steadily developed its e-government architecture through an ambitious series of open-source, cloud-based, interoperable platforms instituted at the central government level. It has also expanded the range of digital services available to Moldovan citizens and businesses. Currently more than 200 public services have been partially or fully digitalized and citizens can access 648 public services through the central public services portal. In 2021, the most used e-services included online income tax declarations, cadastral registrations and obtaining duplicate birth certificates.[48]

Moldova's e-government architecture is comprised of a series of interoperable building blocks or platforms:

- MConnect: a government-to-government (G2G) and government-to-business (G2B) data exchange (interoperability) platform, integrating over 53 public institutions and increasingly the private sector (banks, utilities) in real time. Through this platform public authorities exchange data in real time, without requesting it from citizens and the business environment in the form of certificates, reports, etc.
- Public Services Portal: a one-stop-shop, recently upgraded, for information on 648 public services provided by the central government and increasingly by local governments. In the new version, the portal offers citizens the convenience of accessing digital services over a single electronic counter and guides the user in finding information structured by life events, with a friendly interface and advanced search engine.

[47] Ibid.
[48] Ibid.

- MSign: is a form of digital identifier of a person using a cryptographic SIM card, created by the EGA. Moldova was among the first countries in the world to implement electronic Mobile eID/ mobile signature, which was operationalized through an innovative public-private partnership model.[49] The virtual ID solution allows users to authenticate themselves in cyberspace and to electronically sign any legally-binding transaction or document. This is simple, mobile-phone based, and does not require a separate card reader or drivers. The MSign service is hosted on the common government platform MCloud and complies with the security requirements provided by the legislation in force, including the use of electronic signatures.
- MPass: The government's Authentication and Access Control Service provides secure access to electronic services. MPass.gov.md integrates all electronic authentication tools legally available in the Republic of Moldova: Mobile Signature; Electronic signature on USB stick; Electronic identity card; 2-step authentication. Using one of the authentication mechanisms, you can access several electronic services in a secure way, without the need to register in advance with their providers. Government entities integrate their information systems and services with MPass to provide Single Sign On.
- MDelivery: Citizens of the Republic of Moldova can receive documents requested from state institutions at their place of residence, through the Governmental Delivery Service – MDelivery. The service aims to offer an efficient, reliable and modern technical solution to the authorities, public institutions and public service providers, to be used as a unique mechanism for physical delivery of the results of the provision of public services to the beneficiaries. The MDelivery information platform (www.mdelivery.gov.md) was developed by connecting three parties: the public service provider as the sender, the public service beneficiary as the recipient of the delivery, and the postal service provider. This platform will reduce costs for all three parties involved and will streamline the process of delivering the result of the public service to the beneficiary.
- MNotify: a service in which state institutions can notify and inform users of public services about important events in relation to the authorities, sending messages through different notification channels of the user's choice (email, citizen portal, push notifications, SMS, chat). These messages refer to debts, fines, discharges, payments, allowances, etc. that citizens have to perform to the state and/or vice versa. Through the mnotify.gov.md electronic service, the citizen (natural or legal person) is informed (notified) by public institutions about certain services provided by the state, without this service being requested by the beneficiary. Beneficiaries can be both natural and legal persons. The MNotify service is integrated into the Citizen's Government Portal and users receive electronic notifications, including through the MDelivery portal. In MNotify, notifications can be generated automatically by information systems or manually by operators of service providers through the web interface.
- MPay: a unified payment and invoicing system that allows citizens and businesses to engage with 57 institutions and pay for 644 public services (e.g., school fees, road taxes,

[49] USAID, DIGITAL ECOSYSTEM COUNTRY ASSESSMENT (DECA) MOLDOVA, November 2022

patents, utilities, court fees, fines, income tax).[50] Although MPay is primarily aimed at public sector e-services, it can also be successfully used for commercial services. MPay makes it possible to pay for services using several payment methods, such as bank cards, payment terminals, e-banking systems and cash payments. In case of cash payments, citizens who do not have access to the Internet can contact connected bank counters or Moldovan Post Offices. The payment procedure is very simple. The user accesses the e-Service on servici.gov.md and completes the online application. The service will calculate the amount to pay and offer the user an option to pay via MPay. The user will be redirected to the mpay.gov.md website, where he/she can select the payment method and make the payment. At the end of the operation, the service will provide a payment confirmation. The user can check the payment status at any time. The MPay service is carried out by the Government through the EGA, the STISC, the Ministry of Finance in partnership with the National Bank and the private banking sector.

- Semantic catalogue: The semantic catalogue is a digital work tool for public authorities and institutions, autonomous administrative authorities, which own state information resources, as well as for private law legal entities that, manage or own state information resources on behalf of public authorities and institutions. The catalogue ensures unification and standardization of definitions and classifiers, univocal description of data structures, reuse of this data and facilitation of interaction on the MConnect interoperability platform. EGA is designated as the competent authority for ensuring data exchange and interoperability through the interoperability platform and is carried out based on the semantic assets registered in the Semantic Catalogue established by the Government.
- MCloud: a shared, open-source, WSO2 cloud-based government platform that offers an accessible virtual environment for public institutions to host their information systems, data and e-services and eliminates redundancy in a secure online environment. In 2014, Government of Moldova began to consolidate and host all data on an open-source cloud platform (MCloud). The migration process was challenging, as not all government authorities were willing to switch to the cloud platform and continued to invest in their own data centres. In 2018, STISC was formed through the reorganization of the state enterprise—Special Telecommunications Centre— to oversee the consolidation process. STISC was mandated to host and maintain the governmental infrastructure of information networks, data centres, interoperability platform, CCTLD.md and the Government's technical cybersecurity functions.[51]

[50] USAID, DIGITAL ECOSYSTEM COUNTRY ASSESSMENT (DECA) MOLDOVA, November 2022
[51] Ibid.

6.5 Montenegro

6.5.1 Legal

6.5.1.1 Competent authority

The Agency for Prevention of Corruption is an autonomous and independent body, established by the Parliament of Montenegro in accordance with the Law on Prevention of Corruption and started its operations on 1 January 2016.

As a central preventive anticorruption body, the Agency assumed the responsibilities of the Administration for Anti-Corruption Initiative, Commission for Prevention of Conflict of Interest and a part of the competences of the State Election Commission related to the control of financing of political subjects and election campaigns.

Competences

In accordance with Article 78 of the Law on Prevention of Corruption, the Agency for Prevention of Corruption has the following duties:

- Establish the existence of conflict of interest in the exercise of public functions and take measures for its prevention;
- Control the restrictions on the exercise of public function;
- Conduct control of received gifts, sponsorships and donations;
- Conduct control of the data from the Report on income and assets of public officials;
- Provide an opinion on the existence of threats to public interest that indicate the existence of corruption and produce recommendations for prevention of threats to public interest and protection of whistleblowers;
- Monitor adoption and implementation of Integrity Plans, make recommendations for their improvement and assess the efficiency and effectiveness of Integrity Plans in accordance with this Law;
- Adopt acts within the Agency scope of competence in accordance with the law;
- Take initiatives to amend laws, other regulations and general acts in order to eliminate potential corruption risks or to bring them in line with international anticorruption standards;
- Provide opinions on draft laws and other regulations and general acts for the purpose of their alignment with international anticorruption standards;
- Initiate and conduct proceedings to establish any violation of the provisions of this and other laws governing the responsibilities of the Agency;
- Cooperate with competent authorities, higher education institutions and research organizations and other entities in order to implement activities in the area of prevention of corruption;
- Maintain records and registers in accordance with this Law;
- Issue misdemeanour reports and initiate misdemeanour and other proceedings;
- Conduct educational, research and other preventive anticorruption activities;
- Exercise regional and international cooperation in the prevention of corruption;

- Perform other duties prescribed by law. The Agency supervises the implementation of regulations governing lobbying and implements measures to control the financing of political entities and election campaigns, in accordance with special legislation.

The Agency shall supervise the implementation of regulations governing lobbying and implement measures to control the financing of political entities and election campaigns, in accordance with a special law. [52]

6.5.1.2 Legal framework

- Law on Prevention of Corruption ("Official Gazette" no. 53/2014)

This Law prescribes measures for prevention of conflict of public and private interest and regulates the restrictions in the exercise of public functions, submission of reports on assets and income by public officials, protection of whistleblowers, as well as other issues of importance for prevention and suppression of corruption.

Declarants

Article 3 of this Law determines the definition of „public official":

A public official, within the meaning of this law, is a person elected, appointed or assigned to a state body, state administration body, judicial body, local self-government body, local administration body, independent body, regulatory body, public institution, public enterprise or another economic entity, or a legal entity exercising public authority or activities of public interest, or is state-owned, as well as a person whose election, appointment or assignment requires approval from the authority, regardless of the permanence of the function and remuneration.

In relation to this provision, state ownership, within the meaning of this law, is any participation in a business entity in which the state or municipality, the capital city, or the main city, holds at least 33% of the capital.

Public officials as declarants	
A public official is a person elected, appointed or assigned to a:	
state body	state administration body
judicial body	local self-government body
local administration body	independent body
regulatory body	public institution
public enterprise/ or another economic entity	legal entity exercising public authority or activities of public interest/ or is state-owned
Also, a public official is a person whose election, appointment or assignment requires approval from the authority, regardless of the permanence of the function and remuneration	

[52] https://www.antikorupcija.me/me/

Asset declaration – forms and content

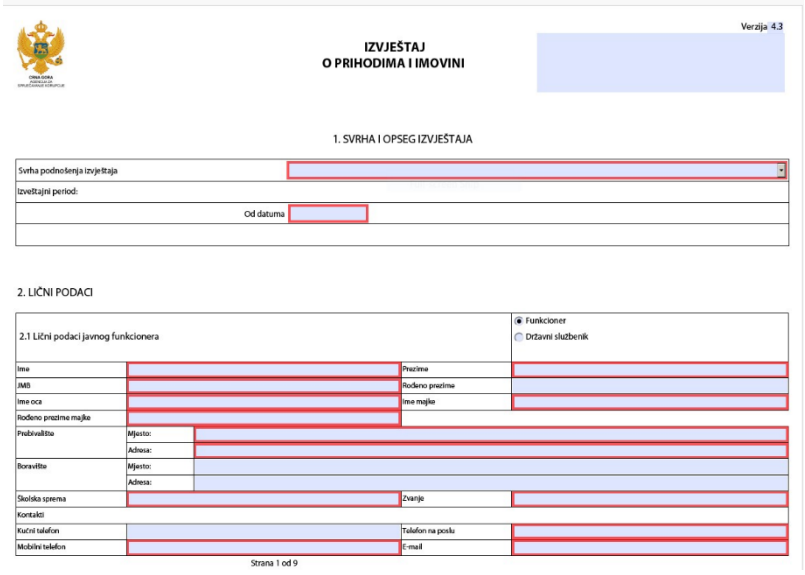
In accordance with Article 23 of this Law, "*A public official must submit to the Agency a report on their assets and income, as well as on the assets and income of their spouse (married or unmarried) and children living in the same household, within 30 days from the day of assuming office, appointment or assignment, based on the status on the day of election, appointment or assignment. The public official is required to provide accurate and complete information in the Report.*

During the performance of public functions, a public official submits the Report:

- once a year, by the end of March of the current year for the previous year;
- in case of changes in the Report related to an increase in assets exceeding 5,000 euros, within 30 days from the day of the change;
- upon the Agency's request in the event of initiating proceedings (Article 31, paragraphs 1 and 2), within 30 days from the date of receiving the request or initiating proceedings ex officio;

In case of termination of public functions, a public official is obliged to inform the Agency within 30 days from the date of termination of office and submit the Report.

Also, a public official whose function has terminated is required to submit the Report to the Agency once a year for the next two years after the termination of office, based on the status on the day of submitting the Report.


Verzija 4.3

IZVJEŠTAJ
O PRIHODIMA I IMOVINI

1. SVRHA I OPSEG IZVJEŠTAJA

Svrha podnošenja izvještaja	
Izvještajni period:	
Od datuma	

2. LIČNI PODACI

2.1 Lični podaci javnog funkcionera			◉ Funkcioner ○ Državni službenik
Ime		Prezime	
JMB		Rođeno prezime	
Ime oca		Ime majke	
Rođeno prezime majke			
Prebivalište	Mjesto:		
	Adresa:		
Boravište	Mjesto:		
	Adresa:		
Školska sprema		Zvanje	
Kontakti			
Kućni telefon		Telefon na poslu	
Mobilni telefon		E-mail	

Strana 1 od 9

The obligation to submit the Report and the procedure for verifying the data from the Report also apply to a state official who is required to submit the Report in accordance with a special law.

A public official shall submit the Report to the Agency electronically, and in written form, developed by the Agency and available on its website.

Regarding Article 24 of the Law, the Report on the income and asset contains the following data:

Report on the income and assets – content	
I. Personal information of the public official and members of the common household, including:	
name	unique identification number
residence or domicile	home address
educational background	profession
father's name, mother's name and mother's maiden name of the public official	
II. Information about the public function being performed	
III. Information about the assets and income of the public official and members of the common household as specified in Article 23, paragraph 1 of this Law, particularly:	
Right of ownership of immovable property and the right to lease immovable property for a duration longer than one year, both domestically and abroad	Right of ownership of movable property with a value exceeding 5,000 euros or subject to registration with the relevant authorities (motor vehicles, watercraft, aircraft, etc.)
Right of ownership of immovable and movable property of a business entity, institution, or other legal entity of which the public official is an owner or founder	Deposits in banks and other financial organizations, both domestic and abroad
Shares and stakes in a legal entity and other securities	Cash exceeding 5,000 euros
Rights based on copyright, patents and similar rights, intellectual and industrial property	Debts (principal, interest and repayment terms) and receivables
Source and amount of income from scientific, educational, cultural, artistic and sports activities	Membership in governing and supervisory bodies of public enterprises, public institutions or other legal entities with state or municipal ownership, as well as in scientific, educational, cultural, artistic, humanitarian, sports or similar associations

Data from the Reports shall be kept in the Register of Income and Assets of Public Officials, which is part of a unified information system of the Agency.

With that aim, the Agency has adopted the Rulebook on the Content and Manner of Keeping the Register of Income and Assets of Public Officials ("Official Gazette of Montenegro" 77/15).

This rulebook prescribes the manner of entering data from the Report on assets and income of a public official, as well as on the assets and income of married and common-law spouse and children if they live in a joint household, into the Register of Income and Assets of Public Officials, as well as the content and manner of keeping the register.

The content of the Report on the Income and Assets is prescribed in more detail with this Rulebook (in the form), compared with the Law.

Data publication

Publication of data is carried out on the basis of Article 27 of the Law on Prevention of Corruption, thus every electronically submitted report is processed using specially created software that ensures public disclosure of data.
According to Article 27 of the Law - *Data Available to the Public,* "Data from the Register shall be published on the website of the Agency, except for information relating to:

- Personal information referred to in Article 24, paragraph 1, item 1 of the present Law, except the names and surnames;
- Address of immovable assets;
- Children of public officials under the age of 16;
- Alimony and other income or payments on the basis of social and child welfare."

Data verification

In accordance with Article 30 of this Law, the Agency verifies the data from the Report by comparing it with the collected data on the assets and income of the public official from government authorities and legal entities that possess such information.

Such government authorities and legal entities have an obligation, within the deadline and in the manner determined by the Agency, to provide the requested information and notifications or to make available the requested documentation in accordance with the law.

If, during the verification process, the Agency determines that the assets and income of the public official and persons related to the public official exceed their actual income, the public official is required, upon request from the Agency, to provide detailed information about the sources of acquired assets and income within 30 days.

The Agency conducts the verification of data from the Report according to the annual verification plan for a specific number and category of officials. The procedure for verifying data from the Report is not accessible to the public. The annual verification plan is adopted annually, by the end of the current year for the next year. The specific method of verifying data is determined by Agency rules.

The data verification procedure is confidential, regarding this Law.

Employees in the Data Verification Department check the accuracy and completeness of the received reports through an integrated system and institutions that have data on the income and property of public officials and members of their common household.

The verification involves collaboration with various entities/institutions:

- Tax and Customs Administration (data on earned taxable income);
- Central Register of Business Entities (Information about companies and ownership);
- Cadastre and State Property Administration (data on property ownership rights);
- Ministry of Internal Affairs (information on ownership of registered movable property, such as motor vehicles and weapons);

- Central Securities Depository and Clearing Company of Montenegro (data on individuals owning securities, including shares in companies and other legal entities);
- Central Bank of Montenegro (relevant financial data);
- Commercial Banks (access to bank accounts, subject to the consent of the obligated person).

This collaborative approach and integration with various institutions aims to ensure a comprehensive and accurate verification process for the reported data.

The Agency has signed data exchange agreements with most of the aforementioned institutions.

In addition to the above, the Agency underlines that it is developing a new IT system, which will, upon submission of the Report on both income and assets of the public official, and upon initiation of the control procedure by the Agency's officials, match the reported data with the data available to the state authorities. The system will then create "red flags", indicating to acting employees where there are discrepancies between the reported data and data found in official registers - databases of state bodies.

This will contribute to a more effective implementation of the verification procedure.

Data protection

In relation to data protection, the Law on Prevention of Corruption specifies that:

Data from the Registry are made publicly available on the Agency's website, with certain exceptions for information related to:

- Personal data from Article 24 paragraph 1 point 1 of this Law, excluding name and surname;
- Address of the real estate property;
- Children of the public official under the age of 16;
- Child support and other income or contributions based on social and child protection.

Members of the Council, the director of the Agency and employees of the Agency who have access to classified information, unpublished data and personal data obtained in the course of their duties must adhere to regulations governing data confidentiality, protection of unpublished data and protection of personal data.
The data from records maintained by the Agency cannot be disclosed if such disclosure could impact ongoing proceedings, as well as in cases specified by this Law and the law governing data confidentiality and protection of personal data.
The Agency must ensure the protection of classified information and personal data both in its work and when providing information to the public.

6.5.2 Technical

6.5.2.1 IT infrastructure

The information system for collection and verification of asset declaration data and the supporting IT services are hosted at the Agency for Prevention of Corruption of Montenegro (hereinafter: ASK).

The ASK data centre is located on its premises. Equipment in the data centre is surge protected by a central UPS device and supplied by the generator that provides backup power in the case of mains power outage. Cooling of the data centre equipment is performed by professional air-conditioning systems. Technical protection of the data centre is achieved by the video surveillance, anti-burglary protection and electronic access control system. The data centre has a fire alarm system and a NOVEC-based fire extinguishing system.

Hardware and network infrastructure in the datacentre consists of:

- Servers - virtualization hosts (2 x Lenovo X3550 M4, 1 x Lenovo X3550 M5, 3 x Dell PowerEdge R520 backup server)
- Storage systems (2 x Lenovo V3700) connected with servers via FC SAN switches (2 x Lenovo B6505).
- Core/aggregation switches
- Network and infrastructure security

Existing servers are outdated (more than 5 years old) and have reached 70% or 90% of consumption of hardware resources. Therefore, new server infrastructure (3 x Dell EMC PowerEdge R640[53]) was procured in 2022 and put in production in 2023 to replace the existing servers and provide additional computing power for hosted IT services.

Lenovo storage systems are also outdated (more than 5 years old) and have reached 60% of consumption of hardware resources, as well as one FC SAN switch (more than 5 years old). SAN connections have recently been made fully redundant by installing and configuring another FC SAN switch.

The disaster recovery centre has not been established yet.

Data centre processing capacity is optimized and consolidated to maximize the utilization of installed computing nodes in the server farm, reduce electricity consumption and maintenance costs by using the VMware virtualization platform.

Core/aggregation switches (2 x Juniper EX3300) perform intelligent routing and filtering of traffic between different IP subnets (VLANs) and provide all LAN connections to virtualization hosts, storage systems, firewall LAN segments and management, etc. These switches are more than 5 years old and their manufacturer has announced end of support for this model on 30 June 2024.

[53] Each server has 1 x CPU (16 cores), 128GB RAM, RAID 8GB Cache, 2 x 600GB 10k SAS HDD, 6 x 1 Gbps Base-T LAN ports, 2 x 16 Gbps FC SAN ports, redundant power supply

The data centre has a 20 Mbps fibre-optic leased line to a state-owned WAN network. VPN Site-to-site tunnels are established on external firewalls to encrypt network traffic between ASK's data centre and data centres of other institutions that provide data used in the asset verification process. External next-generation firewall devices in high availability mode are leveraged to detect and block external sophisticated attacks by enforcing security policies at the application, port and protocol levels, in addition to traditional functionalities such as stateful inspection of network traffic, traffic filtering, network address translation (NAT), VPN termination, Quality of Services, etc. These firewalls provide remote access VPN to authorized ASK employees so that they can reach IT services hosted on the internal network from outer networks. External maintenance vendors also have limited access to internal network through remote access VPN. Two redundant and clustered FortiGate-100F external firewalls were procured 3 months ago to replace 2 existing FortiGate-100D devices that are 5 years old. Redundant and clustered internal firewalls (2 x Juniper SRX 340) have been deployed 5 years ago to protect the internal network from attacks that have passed the perimeter by controlling and monitoring network traffic between internal hosts, preventing unwanted access or isolating insider attacks.

Web application firewalls (2 x FortiWeb-100D), deployed 4 years ago, protect public-facing web applications and services by filtering and monitoring Layer 7 traffic between the web application and the Internet.

ASK is also using FortiAnalyzer virtual appliance (procured 5 years ago) for real-time collection and analysis of logs by applications, systems and network hardware.

Microsoft Windows Server-based Active Directory is used for centralized management of user, password, workstation and server operating system settings through the enforcement of so-called "group policies". Active Directory Domain Controllers have been installed as virtual machines on the virtualized infrastructure to perform the aforementioned roles as well as dynamic allocation of IP addresses to internal hosts - Dynamic Host Configuration Protocol (DHCP) server and domain name to IP address (and vice versa) resolution – Domain Name System (DNS). A two-factor authentication solution is used to provide one time password as another method of authentication to specific information systems deployed in the ASK.

The ASK hosts the email server on its virtual infrastructure. The email server is used for internal and external email communication of its employees and sending/receiving notifications from/to its information systems.

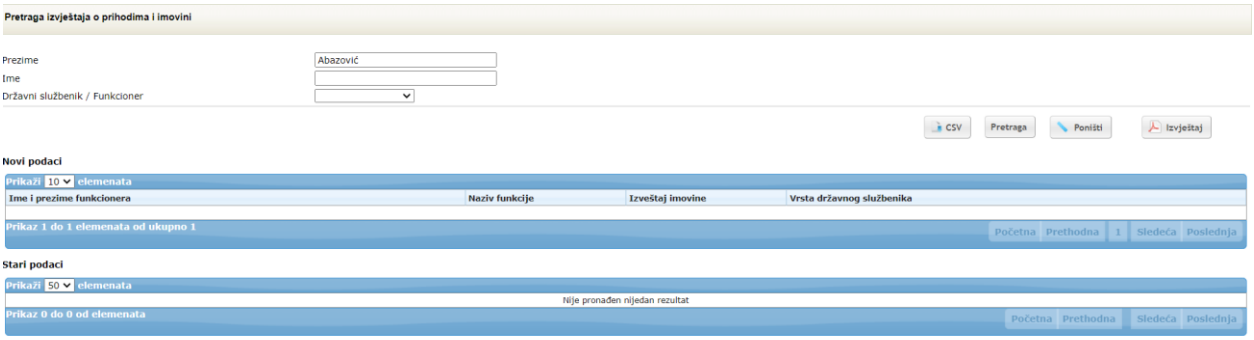
Antimalware protection is applied to workstations and servers, as well as real time scanning of messages and content stored in the email server database. The abovementioned next-generation firewalls and web application firewalls represent additional layers of network and application protection from malware and other forms of cyber threats.

Specialized backup software is used for backing up system and data on the dedicated backup server. Backup is also exported to the tape library (TS3100 with one LTO6 FC Drive), which is more than 5 years old.

6.5.2.2 *Electronic system for collection, verification and exchange of asset declaration data*

ASK runs an electronic asset declaration system for public officials and their eligible family members. The existing system does not support online submission of the asset declaration web form at the moment.[54] Public officials can download the PDF form to their computers from the ASK website.[55] The PDF form is designed to simplify data entry, because in many fields public officials can choose values from drop-down menus, they can copy and paste specific revenue rows to change specific data more easily. PDF forms also provide automatic calculation of the total revenue based on values of individual stated revenues. Once data entry into the PDF form is completed, public officials can upload the PDF file via the ASK website. The electronic asset declaration system in the backend generates a bar code within the uploaded PDF file and makes it available for download by the public official. Once the public official chooses the download action, the document is downloaded to his/her computer. The public official must print and sign the completed asset declaration PDF form, now with the generated bar code. The signed PDF form can be sent in hard copy by regular mail to the ASK (mandatory) or scanned to dedicated ASK's email address (optional). The expert assumes, since the system uses bar codes, that data is automatically retrieved from the PDF form to the database.

ASK publishes asset declarations of public officials on its website. Front-end of the asset declaration system provides capability to search asset declarations by name, surname or public official type (public official or civil servant). Search results can also be exported as a PDF or CSV report. Personal data other than name and surname of the public official is not published.



Search of public official's asset declarations via the ASK website

The ASK's information system for collection, verification and exchange of asset declaration data is a custom-made application based on the eDocumentus platform for electronic document management and business process automation. It is developed and maintained by the Serbian software development and system integrator company. The information system was implemented in 2016. The same platform is used by the Agency for Prevention of Corruption of the Republic of Serbia, but customized for its legislative framework.

The technology stack of the information system consists of MySQL (RDBMS) and Apache Tomcat (web/application server). Java is predominantly used as the development technology. The

[54] New software solution for asset declaration and verification will support online filling-in of the asset declaration web forms.
[55] https://www.antikorupcija.me/me/korisnicki-servisi/

implemented software architecture has not ensured high-availability/load balancing at the application layer.

Management of the ASK has decided few years ago to assess and evaluate the existing software solution from a technological and functional point of view. Findings and recommendations of the assessment were to develop a new information system from scratch. A detailed business analysis and technical specification for the new information system was developed. The information system is intended to integrate and support all business processes and legal competences of the ASK. It consists of software modules that will be developed and implemented in several phases. It supports document and workflow management. The software module for political parties has already been implemented and the tender for development of the module/register of public officials has been finalized. Development of the module for asset declaration and verification is in its final stages. The roll-out of the new module is expected to start on 1 January 2024.

Overview and comparison of the software functionalities supported by the existing and new software for asset declaration and verification is provided in the following table:

Functionality	Existing software	New software	Remark
Document Management	Partially	Yes	
Workflow Management	Partially	Yes	
Support for BPMN	No	Yes	
Business Rules Management	Partially	Yes	In the new software, it is implemented in the application, not as a separate BRM module
Email or in-application notification for new tasks or alarms received	Partially	Yes	
Searching (including full-text search) and/or filtering of the data	Partially	Yes	
Calendar and scheduling of events	No	Yes	
Option to define, create and maintain templates the users can use in their everyday life to generate specific content.	Partially	Yes	
In addition to the predefined, system-wide templates, capability to prepare documents in a visual online rich text editor capable of combining static text and metadata in a dynamic template.	No	Yes	
System users can manage documents in workgroups (multiple author participation) to facilitate document control, auditing, editing and timeline management.	Partially	Yes	
Personal cabinet/dashboard	Partially	Yes	

Identifying, classifying, storing, securing, retrieving, tracking, labelling and reporting of collected content for the purposes of process logs.	Partially	Yes	
Scanning of incoming paper documents	Yes	Yes	
OCR of scanned documents	No	Yes	
Electronic archiving (classification and archiving of closed cases/records).	Yes	Yes	
Capability to sign, seal, store and transfer selected electronic documents using a qualified electronic certificate and qualified electronic time stamp.	No	No	This functionality should be implemented in the next phase: development of the new ASK web portal.
Capability to identify, accept and exchange signed messages with certification authorities (CA) registered in National Register of Qualified Trust Service Providers.	No	No	This functionality should be implemented in the next phase: development of the new ASK web portal.
Capability to automatically check the validity of electronic signatures and electronic seals.	No	No	
Supporting roles and user profiles by granting access to resources (both functionality and data) related to a specific profile combining the role and the user.	Partially	Yes	
Support for Data Encryption	Yes	Yes	
Compliant with WAI (Web Accessibility Initiative) level A1 – accessible by people with disabilities.	No	No	
Multilingual support for menus and data fields	No	No	
Ad-hoc Reports & Statistics (tools for ad hoc analysis that can be used to create a non-predefined report or to drill deeper into a static report to get details about case data, transactions, or records).	No	Yes	
Datawarehouse & Business Intelligence (Datasets included into DW/BI)	No	Yes	This module can be added in the future, if needed.

6.5.2.3 *Interoperability infrastructure and data exchange with the relevant national registries and databases*

The information system currently verifies information from the following national registers by calling respective web services established via direct (peer-to-peer) connection with the competent institution:

- CITIZEN REGISTER (personal IDs, IDs for foreigners, passports, personal ID number, residence)
- CITIZEN PERSONAL STATUS REGISTER (birth, marriage, death)
- REGISTER OF MOTOR VEHICLES
- REGISTER OF SHIPS/VESSELS
- REAL ESTATE REGISTER
- REGISTER OF SECURITIES
- TAX ADMINISTRATION REGISTERS
- REGISTER OF BUSINESS ENTITIESS
- CENTRAL BANK'S REGISTER OF LOANS
- CRIMINAL REGISTER

The current information system allows only to receive responses from web services, but it does not enable retrieval and storage of data from external systems into the information system's database. This functionality will be available in the new information system.

Technical characteristics of each web service are listed in the tables below:

CITIZEN REGISTER - question	**CITIZEN REGISTER - answer**
Is external system data available in machine-readable format	Yes ☒ No ☐
INSTITUTION RESPONSIBLE FOR MANAGEMENT/ADMINISTRATION OF THE EXTERNAL SYSTEM	Ministry of Interior
Data exchange type	API web service ☒
Type of web service, if applicable	SOAP ☒
Web service architecture, if applicable	Peer to peer ☒
Data format used	XML ☒
Communication protocol used	HTTPS ☒
Implemented security features	Authentication ☒ Authorization/access control ☒ SSL/TLS ☒ Data integrity/Signed by digital certificate ☒ Time stamp ☐
UDDI registry/service catalogue available at the service provider side?	Yes ☒
Web service description available in the form of WSDL file	Yes ☒
Authentication used	Username ☒

CITIZEN PERSONAL STATUS REGISTER - question	CITIZEN PERSONAL STATUS REGISTER - answer
Is external system data available in machine-readable format	Yes ☒ No ☐
INSTITUTION RESPONSIBLE FOR MANAGEMENT/ADMINISTRATION OF THE EXTERNAL SYSTEM	Ministry of the Interior
Data exchange type	API web service ☒
Type of web service, if applicable	SOAP ☒
Web service architecture, if applicable	Peer to peer ☒
Data format used	XML ☒
Communication protocol used	HTTPS ☒
Implemented security features	Authentication ☒ Authorization/access control ☒ SSL/TLS ☒ Data integrity/Signed by digital certificate ☒
UDDI registry/service catalogue available at the service provider side?	Yes ☒
Web service description available in the form of WSDL file	Yes ☒
Authentication used	Username ☒

MOTOR VEHICLES/SHIPS REGISTER - questions	MOTOR VEHICLES/SHIPS REGISTER - answer
Is external system data available in machine-readable format	Yes ☒ No ☐
INSTITUTION RESPONSIBLE FOR MANAGEMENT/ADMINISTRATION OF THE EXTERNAL SYSTEM	Ministry of the Interior
Data exchange type	API web service ☒
Type of web service, if applicable	SOAP ☒
Web service architecture, if applicable	Peer to peer ☒
Data format used	XML ☒
Communication protocol used	HTTPS ☒
Implemented security features	Authentication ☒ Authorization/access control ☒ SSL/TLS ☒ Data integrity/Signed by digital certificate ☒
UDDI registry/service catalogue available at the service provider side?	Yes ☒
Web service description available in the form of WSDL file	Yes ☒
Authentication used	Username ☒

REAL ESTATE REGISTER – question	REAL ESTATE REGISTER - answer
Is external system data available in machine-readable format	Yes ☒ No ☐
URL of the external information system, if publicly available	https://www.ekatastar.me/ekatastar-web/action/elogin
INSTITUTION RESPONSIBLE FOR MANAGEMENT/ADMINISTRATION OF THE EXTERNAL SYSTEM	Real Estate Administration
Data exchange type	API web service ☒
Type of web service, if applicable	SOAP ☒
Web service architecture, if applicable	Peer to peer ☒
Data format used	XML ☒
Communication protocol used	HTTP ☒
Implemented security features	Authentication ☒ Authorization/access control ☒
UDDI registry/service catalogue available at the service provider side?	Yes ☒
Web service description available in the form of WSDL file	Yes ☒
Authentication used	Username ☒
REMARK ASK is not using publicly available web services but internal ones, accessible via the established VPN tunnel.	

REGISTER OF SECURITIES - question	REGISTER OF SECURITIES - answer
Is external system data available in machine-readable format	Yes ☒ No ☐
INSTITUTION RESPONSIBLE FOR MANAGEMENT/ADMINISTRATION OF THE EXTERNAL SYSTEM	Central Depository Agency
Data exchange type	API web service ☒
Type of web service, if applicable	SOAP ☒
Web service architecture, if applicable	Peer to peer ☒
Data format used	XML ☒
Communication protocol used	HTTP ☒
Implemented security features	Authentication ☒ Authorization/access control ☒
UDDI registry/service catalogue available at the service provider side?	Yes ☒
Web service description available in the form of WSDL file	Yes ☒
Authentication used	Username ☒

TAX ADMINISTRATION REGISTERS - question	TAX ADMINISTRATION REGISTERS - answer
Is external system data available in machine-readable format	Yes ☒ No ☐
INSTITUTION RESPONSIBLE FOR MANAGEMENT/ADMINISTRATION OF THE EXTERNAL SYSTEM	Tax Administration
Data exchange type	API web service ☒
Type of web service, if applicable	SOAP ☒
Web service architecture, if applicable	Peer to peer ☒
Data format used	XML ☒
Communication protocol used	HTTP ☒
Implemented security features	Authentication ☒ Authorization/access control ☒
UDDI registry/service catalogue available at the service provider side?	Yes ☒
Web service description available in the form of WSDL file	Yes ☒
Authentication used	Username ☒

REGISTER OF BUSINESS ENTITIESS - question	REGISTER OF BUSINESS ENTITIESS - answer
Is external system data available in machine-readable format	Yes ☒ No ☐
URL of the external information system, if publicly available	http://195.66.189.183:8083/
INSTITUTION RESPONSIBLE FOR MANAGEMENT/ADMINISTRATION OF THE EXTERNAL SYSTEM	Central Registry of Business Entities
Data exchange type	API web service ☒
Type of web service, if applicable	SOAP ☒
Web service architecture, if applicable	Peer to peer ☒
Data format used	XML ☒
Communication protocol used	HTTP ☒
Implemented security features	Authentication ☒ Authorization/access control ☒
UDDI registry/service catalogue available at the service provider side?	Yes ☒
Web service description available in the form of WSDL file	Yes ☒
Authentication used	Username ☒
REMARK ASK is not using publicly available web services but internal ones, accessible via the established VPN tunnel.	

CENTRAL BANK'S REGISTER OF LOANS - question	CENTRAL BANK'S REGISTER OF LOANS - answer
Is external system data available in machine-readable format	Yes ☒ No ☐
INSTITUTION RESPONSIBLE FOR MANAGEMENT/ADMINISTRATION OF THE EXTERNAL SYSTEM	Central Bank of Montenegro
Data exchange type	API web service ☒
Type of web service, if applicable	SOAP ☒
Web service architecture, if applicable	Peer to peer ☒
Data format used	XML ☒
Communication protocol used	HTTPS ☒
Implemented security features	Authentication ☒ Authorization/access control ☒ SSL/TLS ☒ Data integrity/Signed by digital certificate ☒
UDDI registry/service catalogue available at the service provider side?	Yes ☒
Web service description available in the form of WSDL file	Yes ☒
Authentication used	Username ☒
REMARK Service is available from 10h to 22h every working day.	

CRIMINAL REGISTER - question	Criminal Register - answer
Is external system data available in machine-readable format	Yes ☒ No ☐
INSTITUTION RESPONSIBLE FOR MANAGEMENT/ADMINISTRATION OF THE EXTERNAL SYSTEM	Ministry of Justice
Data exchange type	API web service ☒
Type of web service, if applicable	REST ☒
Web service architecture, if applicable	Peer to peer ☒
Data format used	JSON ☒
Communication protocol used	HTTPS ☒
Implemented security features	Authentication ☒ Authorization/access control ☒ SSL/TLS ☒
Authentication used	HMAC Token

Information on the availability of national registries mainly used in the asset declaration verification process on the GSB platform or in electronic form is presented in the following table:

Electronic registry	Available in the electronic form	Published on the GSB and available to IS
CITIZEN REGISTER (personal IDs, IDs for foreigners, passports, personal ID number, residence)	Yes	Yes (peer-to-peer)
CITIZEN PERSONAL STATUS REGISTER (birth, marriage, death)	Yes	Yes (peer-to-peer)
REGISTER OF MOTOR VEHICLES	Yes	Yes (peer-to-peer)
REGISTER OF SHIPS/VESSELS	Yes	Yes (peer-to-peer)
AIRCRAFT REGISTER	Unknown	No
REAL ESTATE REGISTER	Yes	Yes (peer-to-peer)
REGISTER OF SECURITIES	Yes	Yes (peer-to-peer)
TAX ADMINISTRATION REGISTERS	Yes	Yes (peer-to-peer)
REGISTER OF BUSINESS ENTITIESS	Yes	Yes (peer-to-peer)
CENTRAL BANK REGISTER OF COMMERCIAL BANK ACCOUNTS/LOANS	Unknown	Yes (peer-to-peer) only for loans
SOCIAL WELFARE REGISTER	Unknown	No
REGISTER OF INTELLECTUAL PROPERTY	Unknown	No
CRIMINAL REGISTER	Yes	Yes (peer-to-peer)

6.5.2.4 IT governance, information security, data protection

ASK's Department for Analytics and Information Technology is responsible for operational management and support of the information system and the underlying infrastructure. The Department for Analytics and IT has only 2 staff members, the Head and the Independent Advisor II. Another IT professional was engaged under a service contract to assist with system administration and user support. The existing number of staff members does not provide for adequate management and support of numerous systems and technologies used in the institution. Furthermore, mainly due to salary constraints for IT professionals in the civil service the ASK cannot attract experienced IT engineers to develop and administer its information systems, IT infrastructure and IT security systems. Hence, it strongly relies on outsourcing partners for development and maintenance of the IS and the IT infrastructure. ASK has also engaged an external consultant under a service contract to assist in business analysis and design of the new information system.

In 2023, 21.000 € is allocated in the ASK's annual budget for maintenance of IT equipment, while 376.930 € is available for software maintenance.

Use and administration of the asset declaration and verification system is regulated by an implementing act. The ASK has not yet established a working group as the Change Management Advisory Body for further development and improvement of the IS. User satisfaction surveys were recently introduced to collect user feedback on the quality of services provided by the ASK.

This instrument can also be used as a catalyst for collecting new ideas for software improvements and development of new features.

The institution does not have the source code for the existing information system, whereas it is in possession of the source code of the new Information system.

ASK's Department for Analytics and IT and outsourced partner(s) provide user support for the information system and the underlying IT infrastructure. However, Service Desk (Ticketing) software or call centre is not implemented to track all relevant information related to submission and resolution of support and change requests. It is not clear at the moment who is responsible for provision of application-specific training for new staff or for new features in the information system.

ASK does have certain funds allocated for employee training and education in its budget. ASK's training plan for 2023 and 2024 envisages specialized IT-related trainings.

ASK could not provide answers to questions related to information security in the submitted questionnaire, because this information is treated as confidential and is not shared with third parties.

ASK has not established an Information Security Management System, but intends to implement it and obtain the ISO/IEC 27001 certification in the near future. It has not developed and adopted the Business Continuity Plan, Information Security Incident Management or Data Retention Policy yet. Trainings to raise awareness about information security have not been organized for ASK's staff in a systematic manner. Since its establishment, some of the Agency's employees have undergone several trainings related to information security.[56] Internal information security training for all employees is planned to take place by the end of December or in January of 2023.

Service level agreements have not been envisaged in the contracts with external service providers. However, ASK has implemented many information security and data protection controls, such as physical security of the data centre, deployment of next-generation firewalls, web application firewalls, antimalware protection, backup, etc.

6.5.2.5 E-Government

Montenegro adopted the Digital Transformation Strategy 2022 – 2026 in December 2021. The Montenegro Digital Transformation Strategy 2022-2026 represents a development framework that will define the preconditions and initiatives needed for rapid adaptation to the increasingly complex digital environment and for agile and proactive development of digital Montenegro.

[56] Training through the TAIEX instrument in the Central Anti-Corruption Bureau of Poland; Cyber security - challenges of the 21st century; Open Data conference in Brussels; TAIEX workshop "Development of IT procedures for information system and data management"; Training for ISO Standard 27001 - Information security management system; Training on "Preserving electoral integrity through better cyber security", etc.

The Law on Electronic Government, the Law on Administrative Procedure, the Law on Electronic Document, the Law on Electronic Identification and Electronic Signature, the Law on Information Security and the Law on Personal Data Protection represent the legislative framework for e-Government and digital transformation of public services aligned with the principles of information security and data privacy.

The Law on Electronic Government provides for the possibility of communication with the Government in an electronic format, obliges state bodies to provide e-government services through a single information system and to use a single system for electronic data exchange (GSB), and also provides for a meta register to review electronic registers. The law also envisages the formation of a coordinating body, the Council for Electronic Government, with the task of coordinating, synchronising and directing activities for the development of electronic services "horizontally" in state administration bodies. In addition, the Law on Electronic Administration prescribes the obligation to create a catalogue of electronic services and publish them on the websites of certain public institutions. Another measure to overcome the lack of interoperability was the adoption of the new National Interoperability Framework (hereinafter: *NIF*) in 2019. The NIF aims to support the public administration in implementing interoperability activities, establishing relationships between private and public organisations, and simplifying procedures to guarantee efficient and effective digital services while ensuring that existing and new legislation does not undermine the interoperability initiative.

The Ministry of Public Administration is coordinating the development of eGovernment and the development of the information society in Montenegro. The Ministry is, inter alia, in charge of digitising the operation of public administration bodies through planning, development and support in the implementation of electronic services; Planning, developing and supporting the implementation of the information and communication portal for citizens; Managing and coordinating projects in the field of development of electronic administration and information society for the needs of State administration bodies and State bodies; Establishing a framework for the management of information systems of State administration bodies and State bodies in accordance with international standards, and; Establishing technological and security information infrastructure in State administration bodies and State bodies.

The Department for eGovernment Development in the Ministry of Public Administration is the central government body in charge of the Metaregistry. The Metaregistry contains the records of all registries in the institutions that provide eRegistries according to the Law on Electronic Administration.

According to the information provided in the Digital Transformation Strategy 2022 – 2026, although there are 523 e-services on the e-government portal in Montenegro, only 157 e-services have been developed to level 3 (online filling and downloading of forms), 2 services have been developed to level 4 (which provides for full interoperability of registers), while none of the services have reached Level 5 services (full online service).

The e-government portal, which has over 80,000 users, was implemented in 2011 and lags behind modern trends in terms of technology and good user experience. The Public Administration Reform Strategy and the Digital Transformation Strategy 2022 – 2026 identify the

need to improve the existing e-government portal established 10 years ago, both visually and technically/technologically. The establishment of the new portal envisages its integration with shared e-government systems, such as the electronic identification system, the system for collection of administrative fees and charges, etc. in order to enable the completion of electronic services and their sophistication at the highest level. Hence, activities in the "E-services and Digital Infrastructure as Covid-19 Response" project funded by the European Union and implemented by the UNDP encompass implementation of a single e-government portal with the roll-out of at least 10 priority services. E-services that are relevant for data exchange with the asset declaration system are: Application for issuance of ID cards and passports, Application for vehicle registration, e-Business, Electronic registration and deregistration of employees, e-Contributions.

The National Identification Number (hereinafter: *NIN*), which was introduced at the same time as the new ID cards, solves the service providers' problem of identifying their customers and on the other hand ensures personal data protection. This is not the case with the Unique Identification Number (hereinafter: *UIN*) because, in addition, UIN is not data that must be registered. Most systems in Montenegro (public administration bodies, banks, etc.) are still based on the UIN as the only immutable piece of data that uniquely identifies a person. Organising the exchange of data with the Ministry of the Interior (MoI) would enable public administration bodies and companies to automatically obtain data on NIB users by pairing with data from current versions of the ID card.

The Unified System of Electronic Data Exchange or GSB was put in operation at the end of 2018. The basic function of the central, interoperable system is to provide institutions with a single communication platform for secure and reliable data exchange and thus provide a basis for quality and fast delivery of services. The following registers, relevant for data exchange with the asset declaration system, are currently connected to the GSB:

- Central Population Register,
- Central Register of Taxpayers and Insured Persons (Register of Taxpayers and Register of Employees),
- Central Register of Business Entities
- Social Card information system

Based on the information provided in the Digital Transformation Strategy 2022 – 2026, the Real Estate Register should have been connected to the GSB by now.

The Information System for Electronic User Identification (NS eID) aims to enable electronic identification, i.e. authentication and authorisation of users when using electronic services. The system supports centralised management and use of various electronic mechanisms for authentication and authorisation, as well as various technical solutions. The Information System for Collection of Administrative Fees (NS - NAT) should enable electronic payment of public revenues. The NS-NAT system will enable in-person payments to State administration bodies and local self-government units by card, as well as payment of fees electronically on the eServices web portal.

The Ministry of Public Administration, Digital Society and Media provides non-commercial electronic trust services for state administration bodies, recognised in the Decree on the Organisation and Manner of Operation of State Administration (producing advanced electronic signature certificates) and as such entered in the Register of Electronic Trust Providers. As for development of trust services, it is necessary to point out the international agreements that Montenegro has signed:

- Agreement on Mutual Recognition of Qualified Certification Services for Electronic Transactions provided in Montenegro and Qualified Trust Services Provided in Serbia;
- Agreement with North Macedonia on Mutual Recognition of Certification Services for Electronic Transactions Provided in Montenegro and Qualified Trust Services Provided in the Republic of North Macedonia.

As already stated, a significant opportunity to accelerate the digital transformation is the introduction of new ID cards, along with digital certificates for qualified electronic signatures and electronic identification provided free of charge. The Ministry of Interior started issuing electronic ID cards on 1 June 2020. For this purpose, the Ministry of Interior is a registered qualified service provider. It has established a qualified certification body to provide electronic qualified trust services - TrustME. TrustME provides services such as issuing digital certificates for qualified electronic signatures and digital certificates as means of eID, in accordance with the Law on Electronic Identification and Electronic Signature.

The network of State bodies and the State data centre is managed by the Ministry of Public Administration. It is used for the needs of the information infrastructure of State bodies and management bodies. The Private Cloud System is available to all public administration bodies via the SelfService Portal and a virtual server environment, in compliance with the applicable requirements and necessary licences.

6.6 North Macedonia

6.6.1 Legal

6.6.1.1 Competent authority

The State Commission for Prevention of Corruption was established by the Parliament of the Republic of Macedonia on 12 November 2002, according to the Law on Prevention of Corruption (“Official Gazette of the Republic of Macedonia” no. 28 /2002).

The State Commission for Prevention of Corruption is autonomous and independent in the performance of the competences determined by the Law and shall have the capacity of a legal entity.

The State Commission for Prevention of Corruption shall be competent for the application of the measures and activities for prevention of corruption in the exercise of power, public authorizations, official duty and politics, measures and activities for prevention of conflict of interests, measures and activities for prevention of corruption in undertaking activities of public interest by legal entities related to execution of public authorizations.

This institution is specialized for prevention of corruption and conflict of interests in the public sector and encourages normative and institutional strengthening, promotes inter-institutional and international cooperation and develops a legal culture.

Competences:

The State Commission has the following competences:

- adopts a national strategy for the prevention of corruption and conflicts of interest, with an action plan for its implementation;
- conducts corruption proofing of laws, by-laws and other general acts, in accordance with the methodology it adopts;
- acts upon reports from individuals and legal entities about suspicions for corruption and conflict of interest;
- instigates initiatives before the competent authorities for procedure for determining liability of officials;
- instigates initiatives for criminal prosecution in the cases in which it acts;
- monitors the legality of the financing of political parties;
- monitors the legality of the financing of election campaigns;
- instigates initiatives before the competent authorities on the basis of reports from the State Audit Office;
- acts in cases of conflict of interest;
- records and monitors the assets and interests in a procedure in accordance with this Law;
- prescribes the form for declarations of assets and interests;
- checks the data from declarations of assets and interests;
- cooperates with other state authorities in providing the necessary information;
- cooperates with national bodies of other countries, as well as with international organizations in the field of prevention of corruption;
- exchanges information with competent bodies of other states and international organizations, on the basis of obligations undertaken under international agreements ratified in accordance with the Constitution of the Republic of Macedonia;
- cooperates with associations, foundations, scientific institutions and the private sector in relation to the prevention of corruption and conflicts of interest;
- prepares analyses of the risks of corruption in different sectors;
- undertakes activities in the direction of strengthening personal and institutional integrity;
- undertakes activities in the field of education and awareness raising on corruption and conflict of interest;
- keeps a register of elected and appointed persons;
- keeps a register of authorized persons for receiving disclosures from whistle-blowers, in accordance with the Law on Protection of Whistle-Blowers;
- prepares a catalogue of gifts on the basis of data obtained in accordance with Article 58 of this Law and publishes it on its website;

- conducts public opinion surveys to assess its own performance and the situation concerning corruption;
- adopts the annual working program of the State Commission;
- adopts the Code of Ethics of the State Commission and the Secretariat;
- adopts the Rules of Procedure of the State Commission;
- adopts acts for internal organization and systematization of posts in the Secretariat;
- regularly informs the public about its work related to its competences determined by this Law and in accordance with the Rules of Procedure of the State Commission; and
- performs other activities determined by law.[57]

6.6.1.2 Legal framework

- Law on Prevention of Corruption and Conflict of Interest ("Official Gazette of the Republic of Macedonia" no. 12/2019)[58]

This Law aims to regulate the measures and activities for prevention of corruption in the exercise of power, public authorizations, official duty and politics, measures and activities for prevention of conflict of interests, measures and activities for prevention of corruption in undertaking activities of public interest by legal entities related to execution of public authorizations. This law is based on the principles of legality, integrity, equality, publicity, protection and liability.

Declarants

Article 8 of the Law - *Meaning of the terms used in this Law*, in paragraph (1) and (2) refers as follows:
"(1) For determining the meaning of the terms elected or appointed person, legal entity, responsible person in a legal entity and a person performing public interest activities, the provisions on the meaning of the terms from the Criminal Code shall be applied.
(2) The term "official person" shall mean all elected or appointed persons and public sector employees."
Additionally, Article 82 paragraph (1) of this law determines that "An elected or appointed person, responsible person in a public enterprise, public institution or other legal entity disposing with state capital, notary, enforcement agent, administrative officer of category A determined by law or a person employed in the cabinet of the President of the Republic of Macedonia, the President and Vice-Presidents of the Assembly of the Republic of Macedonia, the President of the Government of the Republic of Macedonia, Deputy Prime Ministers of the Government of the Republic of Macedonia, Ministers and the Secretary General of the Government, with the aim to carry out tasks of a special adviser in the selection, appointment, designation or employment, and not later than 30 days after the election, appointment, designation or employment, shall submit a declaration of assets and interests."

[57] https://dksk.mk
[58] https://dksk.mk/wp-content/uploads/2021/04/LAW-ON-PREVENTION-OF-CORRUPTION-AND-CONFLICT-OF-INTERESTS.pdf

Declarants	
Elected or appointed person	Responsible person in a public enterprise, public institution or other legal entity disposing with state capital
Notary	Enforcement agent
Administrative officer of category A determined by law	Person employed in the cabinet of the: - President of the Republic of Macedonia, - President and Vice-Presidents of the Assembly of the Republic of Macedonia, - President of the Government of the Republic of Macedonia, - Deputy Prime Ministers of the Government of the Republic of Macedonia, - Ministers and - Secretary General of the Government with aim to carry out tasks of a special adviser

Asset declaration – forms and content

According to this Law, there are two situations when the above subjects are required to submit a Declaration of Assets and Interests:

- After assuming public duty - not later than 30 days after the election, appointment, designation or employment;
- After leaving public duty - within 30 days from the date of termination of their function or employment.

Furthermore, declarants have an obligation to promptly report any increase in their own property or the property of a family member if the value of the increase surpasses the equivalent of twenty (20) average net salaries in the Republic of Macedonia for the preceding three-month period. This obligation also extends to reporting changes in interests within 30 days.

The State Commission may request from an official person who is not obligated to submit a declaration of assets and interests according to this Law to submit a declaration, and may conduct a procedure to examine their asset status, when acting in a case in which that person is involved.

The content of the Declaration of Assets and Interests is determined in Paragraph 2 of Article 82.

Regarding this provision, the declaration of assets and interests shall contain:
- a detailed inventory of real estate, movables with a value exceeding the amount of twenty average net salaries in the previous three-month period, securities, receivables and debts, as well as other property in his/her possession, or ownership of the members of his/her family, stating the basis for acquiring the declared property;

- a statement of interests for him/her and his/her family members, which contains information on jobs and membership in management boards, membership in associations and foundations, and other data required in the prescribed form.


ПРИЛОГ 1 - ОБРАЗЕЦ

РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА
REPUBLIKA E MAQEDONISË SË VERIUT

ДКСК KSHPK

ИЗЈАВА
ЗА ИМОТНА СОСТОЈБА И ИНТЕРЕСИ И ПРИЈАВУВАЊЕ ПРОМЕНА ВО ИМОТНАТА СОСТОЈБА И ИНТЕРЕСИТЕ

Лични информации	Функции
ЕМБГ /	Активни функции
Име /	
Име на родител /	
Презиме /	
Адреса на постојано живеење /	
Адреса на престојување /	
Контакт телефон /	
E-адреса /	

СЕМЕЈСТВО
Име
Презиме
ЕМБГ
Сродство
Коментар

The form and content of the Declaration of Assets and Interests, as well as the form for reporting changes in assets and interests, is prescribed by the State Commission in the following rulebook:

- *Rulebook on the Form and Content of the Declaration of Asset and Interests and Reporting Changes in Assets and Interests ("Official Gazette of the Republic of North Macedonia" no. 73/2023)*

According to the Law and this Rulebook, elected or appointed persons are required to submit the Declaration of Assets and Interests electronically and to provide a printed copy to the State Commission.

The Declaration of Assets and Interests contains: personal data, data concerning family members, information about the public function, data about various types of assets and income and data concerning any interests, as follows:

Declaration of Assets and Interests – content	
<u>Declarant's personal data :</u> -Unique identification number, - First name, - Parent's name, - Surname, - Address of permanent residence, - Address of temporary residences, - Contact phone, - Email address, - Active function	<u>Data concerning family members:</u> - First name, - Surname, - Relationship, - Unique identification number
<u>Information about the public function:</u> - Type of submission – for appointment/election to a position, termination of position, or change in financial status and interests Position - Institution where the position is held - Date of election/appointment - Appointing authority - Number of the appointment/election act	<u>Data about various types of assets in the country/abroad and income in the country/abroad:</u> - Real estate - Movable property - Weapons - Securities - Bank accounts and deposits - Claims - Debts to individuals and legal entities - Debts to banks - Other property -Income from: employment, independent activities, copyright and other related rights, industrial

	property rights - Income from lease/sublease - Income from capital - Other income - Capital gains
Data concerning interests in the country/abroad: - Employment/other engagement, -Commercial companies/legal entities, -Associations of citizens and foundations, -Public authorizations/duties, employment, other work engagements for family members	

Data publication

In accordance with Article 87 - *Publicity of the declaration of assets and interests*, data contained in the declaration of assets and interests and the report on changes in assets and interests are considered information of public character, except for data protected by law. Data contained in the declarations of assets and interests and reports on changes in assets and interests submitted to the State Commission, excluding data protected by law, shall be published on the website of the State Commission.

Data verification

Article 92 of the Law outlines the procedure for verification of data on assets and interests. According to this article, the State Commission shall verify the authenticity of the data entered in the declaration of assets and interests when acting on a specific case or based on the annual plan referred to in Article 19 paragraph (1) of this Law.

The State Commission carries out this check by collecting, comparing and analysing data obtained from legal entities and individuals in possession of the necessary data.

In addition, Article 93 establishes the procedure for investigating assets. If there is a reasonable suspicion that the property of a person obligated to submit a declaration of assets and interests has disproportionately increased compared to their regular income or the income of their family members, the State Commission shall initiate a procedure to examine the property status. During the examination of assets, the State Commission invites the person under investigation to submit data concerning the basis for acquisition of the property, and the person must respond within 15 days from receipt of the request.

Article 94 states that state bodies, bodies of local self-government units, payment operations actors and other natural and legal persons, at the request of the State Commission, are under the obligation to provide all necessary information within the time limit set for determining the actual situation relevant to checking the data and examining the property and assets. In case of failure to comply with the request within the specified deadline, these entities must inform the State Commission promptly about the reasons for their failure to act. In such cases, the State Commission notifies the supervising body of those entities and may submit a special report to the Assembly of the Republic of Macedonia or inform the public.

In line with Article 95, if the procedure for examining the property and property status does not establish that the property was acquired or increased as a result of reported and taxed income, the State Commission initiates a criminal procedure by filing an initiative with the Public Prosecution against the person under investigation. Additionally, the State Commission notifies the body that appointed or elected the person, or the organization in which the person is employed or performing the function, about the activities undertaken.

Furthermore, Article 23 of the Law - *Acting of the State Commission*, outlines that the State Commission shall act upon its own initiative and on the basis of received reports and in order to fully determine the factual situation, the State Commission may request data and information from competent institutions, legal entities and natural persons.

The responsible person at the competent institution or a person authorized by him/her, shall undertake all measures and activities for submitting the requested information and shall submit them within 15 days from the day of receiving the request from the State Commission. In case the competent institution fails to act on the request within the determined period, the State Commission shall initiate a misdemeanour procedure.

In addition, it is very important to underline the implementation of Article 25 - *Requests for data from banks and other financial institutions and access to data bases*, which prescribes that upon initiating the procedure the State Commission may request data from banks and other financial institutions and the official person or the responsible person of the legal entity for which data are requested shall be informed thereof, immediately.

Banks and other financial institutions shall be obliged, within 15 days, to submit the requested data to the State Commission.

Submission of the requested data shall not constitute a breach of bank secrecy.

In the performance of its competences the State Commission has access to databases managed by other bodies and institutions, that is direct electronic access, and uses data free of charge from the databases of:

- Ministry of Interior;
- Pension and Disability Insurance Fund of Macedonia;
- Health Insurance Fund of Macedonia;
- Public Revenue Office;
- Employment Agency of the Republic of Macedonia;
- Agency for the Real Estate Cadastre;
- Central Securities Depository AD Skopje;
- Clearing House "KIBS" AD Skopje;
- Credit Bureau;
- Central Registry of the Republic of Macedonia;
- Customs Administration;
- Ministry of Justice – Office for Management of Registers of Births, Marriages and Deaths;

- Ministry of Labour and Social Policy;
- State Audit Office;
- Macedonian Stock Exchange;
- National Bank of the Republic of Macedonia; and
- Ministry of Economy.

The State Commission has signed data exchange agreements with most of the aforementioned institutions.

Data protection

Article 88 addresses the processing of personal data in the application of the provisions of the Law. According to this article:
Personal data collected under the provisions of the Law shall be processed and stored fairly and appropriately for the specific and clear objectives outlined in the law.
The personal data shall be maintained in a form that allows for the identification of the subject of the personal data.

Personal data shall not be retained for any longer than necessary to fulfil the purposes for which the data were collected, and for further processing in accordance with the law.

Upon request from the subject of the personal data, the State Commission shall supplement, modify, delete or suspend the use of personal data if the data are incomplete, incorrect, not updated, or if their processing is not in accordance with the law.

The request must specify the data for which the supplement, modification, deletion or suspension is required. If addition or modification is requested, the new data making the addition or modification must also be provided.

If it is determined that the personal data are incomplete, inaccurate or not updated, the State Commission takes measures to supplement, modify, or delete the data, regardless of whether the subject of the personal data has applied for such action.

The State Commission notifies the subject of personal data in person, as well as the users of personal data or third parties to whom personal data have been disclosed in accordance with the law, within 15 days from the day of receipt of the request, regarding the supplemented, modified or deleted personal data.

In addition to the above, the president, members and employees of the State Commission who have access to the databases from Article 25, are under the obligation to maintain confidentiality. They may use these databases exclusively for the purposes for which they are obtained and must not disclose them to third persons contrary to the law.

The State Commission is responsible for maintaining a Register of elected and appointed persons. The information entered in the Register is considered public information, except for

data protected by law. The data from the Register which are not protected by law shall be published on the State Commission's website.

Related to the Law on Personal Data Protection ("Official Gazette of the Republic of North Macedonia" no. 42/20 and 294/21), this Law has been harmonized with the European regulation on personal data protection, specifically: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) CELEX no. 32016R0679.

Regarding this Law, the laws and other acts which regulate collection, processing, storage, use and submission of personal data shall be aligned with the provisions of this Law within 18 months from the date of entry into force of this Law.

However, it is important to note that the Law on Prevention of Corruption and Conflict of Interest is still not aligned with this Law.

6.6.2 Technical

6.6.2.1 IT infrastructure

The information system for collection and verification of asset declaration data and the supporting IT services are hosted in the State Commission for Prevention of Corruption of North Macedonia (hereinafter: *SCPC*). Email and the public website are hosted by the cloud provider located in North Macedonia.

SCPC's data centre is located within its premises. Equipment in the data centre is surge protected by a central UPS device and supplied by the generator that provides backup power in the event of mains power outage. Cooling of the data centre equipment is performed by air-conditioning systems. The data centre is covered by video surveillance. The data centre has a fire alarm system and a NOVEC-based fire extinguishing system. Installation of an electronic access control system and anti-burglary protection is planned for the upcoming period.

Hardware and network infrastructure in the main data centres is rather old and consists of:

- Servers - virtualization hosts
- Storage systems connected with servers via an FC SAN network
- Top-of-the-rack access switches
- Network and infrastructure security

Many components of the IT infrastructure in the data centre are not redundant and thus do not provide high availability to IT services hosted here.

SCPC has not established a disaster recovery centre at the secondary location yet.

Procurement of the new compute, storage and network infrastructure for the data centre is planned to be finalized by the end of 2023. New infrastructure is designed to provide the currently missing high-availability characteristics.

Data centre processing capacity is optimized and consolidated to maximize the utilization of installed computing nodes in the server farm, reduce electricity consumption and maintenance costs by using a virtualization platform.

The data centre has 100 Mbps access to the Internet over fibre-optic medium. Static IP address is assigned by the Internet provider. Single Firewall/IPS device terminates VPN site-to-site tunnels between the SCPC and the Ministry for Information Society and Administration[59] as well as other institutions that exchange data with the SCPC for the purpose of verification of asset declarations. Access rules have been defined on the firewall in accordance with network security policies and security requirements of the IT services and deployed information systems to restrict network access to specific IP addresses, protocols and ports. The firewall performs routing and NAT translation of traffic to the Internet and DMZ zones and protects inner SCPC network segments against unauthorized intrusions and threats coming from an Internet network. The firewall also provides remote access to the inner SCPC network, primarily for remote system administration purposes.

Microsoft Windows Server-based Active Directory is used for centralized management of user, password, workstation and server operating system settings through the enforcement of so-called "group policies". Active Directory Domain Controller(s) have been installed as virtual machines on the virtualized infrastructure to perform the aforementioned roles, as well as dynamic allocation of IP addresses to internal hosts - Dynamic Host Configuration Protocol (DHCP) server and domain name to IP address (and vice versa) resolution – Domain Name System (DNS). File server is deployed to store specific user files outside of information system.

Antimalware protection is applied to workstations and servers. Windows Server Update Services is deployed to download Microsoft product security and other update packages from the official Microsoft sites and update workstation/server operating systems and Microsoft-based services in accordance with patch management policies. SCPC has also implemented Security Information and Event Management (SIEM) for real-time analysis and correlation of security alerts generated by applications and network hardware.

No specialized backup software is currently used for backing up virtual machines on the backup storage.

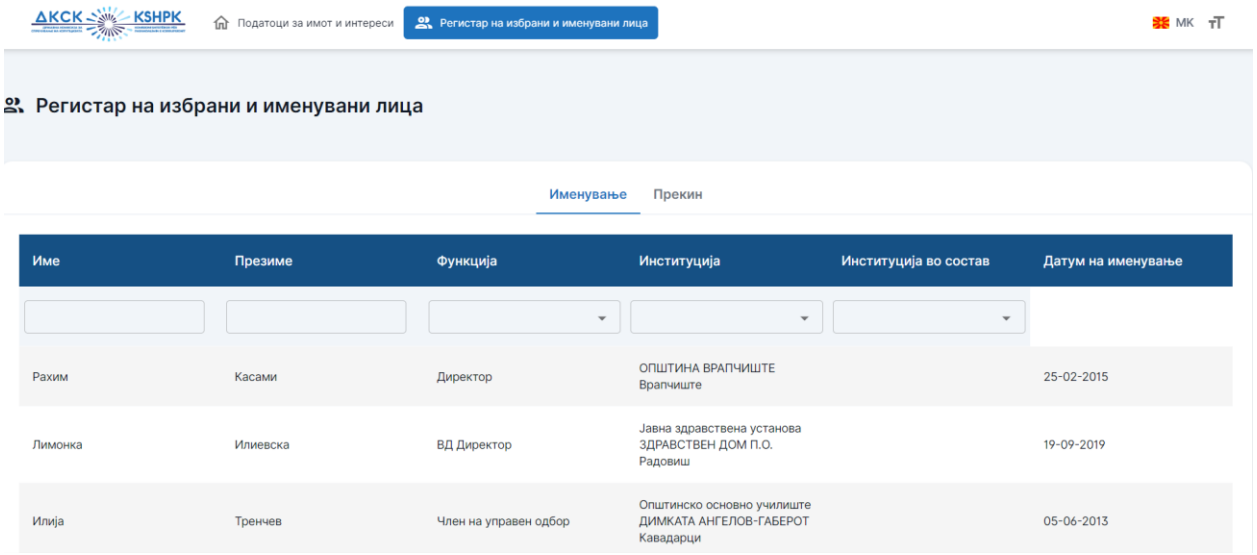
6.6.2.2 Electronic system for collection, verification and exchange of asset declaration data

The State Commission for Prevention of Corruption of North Macedonia (hereinafter: *SCPC*) has established the Register of public officials and their asset declarations. The Register of public officials holds the data contained in the forms submitted electronically by responsible persons (or persons authorized by them) of the institutions/authorities for verification on the mandate/election/appointment/designation/termination of office/duty of the public officials encompassed by the Law on Prevention of Corruption and Conflict of Interest. Authorized persons from the institutions and bodies of North Macedonia can log in to the Register via the

[59] This Ministry hosts the North Macedonia GSB.

national SSO portal using their username and password or the digital certificate issued by a registered provider in North Macedonia. New users have to complete the registration process before they can log in. The register is publicly available on the SCPC website. Each form submitted in electronic form is automatically published on the website of the SCPC, except for data protected by the Law (e.g. personal data).

Access to all data in the Registry is granted to the president and members of the State Commission for Prevention of Corruption, the general secretary and administrative officers performing work tasks directly related to the data in the Register.



Access and search of public officials registered in the SCPC's register via its website

The SCPC currently publishes a basic set of asset declaration data registered in the system from the paper forms received from public officials. The data contained in asset declarations, except for data protected by law, are published on the SCPC website.

Development of the new asset and interest declaration and verification information system (hereinafter: information system/IS) is in the final phase. The information system is currently being tested and is expected to enter the production phase in the beginning of 2024. It will enable public officials to electronically complete asset declaration web forms via the SCPC website. Public officials will still be obliged to send the signed paper version to the SCPC by regular mail. Access to all data from the asset declarations is granted to the president and members of the State Commission for Prevention of Corruption, the general secretary and administrative officers who perform tasks directly related to this data.

The SCPC is responsible for management and administration of its information system. The IS was developed by an outsourced partner. The development technology is Java/React, while MS SQL Server is used as RDBMS. RabbitMQ represents the system middleware. Load balancer/Reverse Proxy performs load balancing of web traffic between multiple web servers. Total hardware resources currently used by the system are: 32 vCPU, 32GB RAM and 300GB HDD.

The information system **supports** the following functionalities:

- Document Management
- Workflow Management
- Support for BPMN
- Email or in-application notification for new tasks or alarms received
- The system provides user directions with respect to what steps in the procedure should be undertaken next and within which deadlines – partially implemented
- Searching (including full-text search) and/or filtering of the data
- Personal cabinet/dashboard
- Electronic submission of asset declarations data and attaching documents using web application accessible via the Internet.
- Merging and splitting of cases/records
- Scanning of incoming paper documents
- OCR of scanned documents
- Electronic archiving (classification and archiving of closed cases/records).
- Capability to automatically check the validity of electronic signatures and electronic seals – not used at the moment
- Multilingual support for menus and data fields
- Remote (Out-of-office) access to users via the Internet is possible, but not active.

The information system **does not support** the following functionalities:

- Business Rules Management
- Calendar and scheduling of events
- Option to define, create and maintain templates the users can use in their everyday life to generate specific content.
- In addition to the predefined, system-wide templates, capability to create documents in a visual online rich text editor capable of combining static text and metadata in a dynamic template.
- Ability to manage documents in workgroups (multiple author participation), to facilitate document control, auditing, editing and timeline management.
- Identifying, classifying, storing, securing, retrieving, tracking, labelling and reporting of collected content for the purposes of process logs.
- Capability to sign, seal, store and transfer selected electronic documents using a qualified electronic certificate and qualified electronic time stamp.
- Capability to identify, accept and exchange signed messages with certification authorities (CA) registered in the National Register of Qualified Trust Service Providers.
- Capability to define/select a group of cases/records under specific conditions and to perform a task over the selected cases/records to support consistent case/records operations.
- Data Pseudonymisation
- Data Encryption
- Compliance with WAI (Web Accessibility Initiative) level A1 – accessible by people with disabilities.

- Ad-hoc Reports & Statistics (Tools for ad hoc analysis that can be used to create a non-predefined report or to drill deeper into a static report to get details about case data, transactions or records).
- Datawarehouse & Business Intelligence (Datasets included into DW/BI)

6.6.2.3 Interoperability infrastructure and data exchange with the relevant national registries and databases

The information system currently retrieves and verifies information, by integrating with the national GSB platform, from the following national registers[60]:

- CITIZEN REGISTER (personal IDs, IDs for foreigners, passports, personal ID number, residence)
- REGISTER OF MOTOR VEHICLES
- REAL ESTATE REGISTER
- TAX ADMINISTRATION REGISTERS
- REGISTER OF BUSINESS ENTITIESS
- CENTRAL BANK REGISTER OF COMMERCIAL BANK ACCOUNTS

The technical characteristics of each web service are listed in the tables below:

CITIZEN REGISTER - question	**CITIZEN REGISTER - answer**
Is external system data available in machine-readable format	Yes ☒
INSTITUTION RESPONSIBLE FOR MANAGEMENT/ADMINISTRATION OF THE EXTERNAL SYSTEM	Ministry for Information Society and Administration
External system DEVELOPED	Outsourcing ☒ In-house ☐
Data exchange type	API web service ☒
Type of web service, if applicable	SOAP ☒
Web service architecture, if applicable	via GSB (ESB) ☒
Data format used	XML ☒
Communication protocol used	HTTPS ☒
Implemented security features	Authorization/access control ☒ Data/message encryption ☒ SSL/TLS ☒ Data integrity/Signed by digital certificate ☒ Time stamp ☒
Web service description available in the form of WSDL file	Yes ☒

[60] These registers have already integrated with national GG.

REGISTER OF MOTOR VEHICLES - question	REGISTER OF MOTOR VEHICLES - answer
Is external system data available in machine-readable format	Yes ☒
INSTITUTION RESPONSIBLE FOR MANAGEMENT/ADMINISTRATION OF THE EXTERNAL SYSTEM	Ministry for Interior
External system DEVELOPED	Outsourcing ☐ In-house ☒
Data exchange type	API web service ☒
Type of web service, if applicable	SOAP ☒
Web service architecture, if applicable	via GSB (ESB) ☒
Data format used	XML ☒
Communication protocol used	Not specified
Implemented security features	Not specified

REAL ESTATE REGISTER - question	REAL ESTATE REGISTER - answer
Is external system data available in machine-readable format	Yes ☒
INSTITUTION RESPONSIBLE FOR MANAGEMENT/ADMINISTRATION OF THE EXTERNAL SYSTEM	Agency for Cadaster
Data exchange type	API web service ☒
Type of web service, if applicable	SOAP ☒
Web service architecture, if applicable	via GSB (ESB) ☒
Data format used	XML ☒
Communication protocol used	Not specified
Implemented security features	Not specified

TAX ADMINISTRATION REGISTERS - question	TAX ADMINISTRATION REGISTERS - answer
Is external system data available in machine-readable format	Yes ☒
Data exchange type	API web service ☒
Type of web service, if applicable	SOAP ☒
Web service architecture, if applicable	via GSB (ESB) ☒
Data format used	XML ☒
Communication protocol used	HTTPS ☒
Implemented security features	Not specified

REGISTER OF BUSINESS ENTITIESS - question	REGISTER OF BUSINESS ENTITIESS - answer
Is external system data available in machine-readable format	Yes ☒
Data exchange type	API web service ☒
Type of web service, if applicable	SOAP ☒
Web service architecture, if applicable	via GSB (ESB) ☒
Data format used	XML ☒
Communication protocol used	HTTPS ☒

CENTRAL BANK REGISTER OF COMMERCIAL BANK ACCOUNTS – question	CENTRAL BANK REGISTER OF COMMERCIAL BANK ACCOUNTS - answer
Is external system data available in machine-readable format	Yes ☒
Data exchange type	Not specified
Type of web service, if applicable	Not specified
Web service architecture, if applicable	via GSB (ESB) ☒
Data format used	XML ☒
Communication protocol used	HTTPS ☒

The following registers are available via direct (peer-to-peer) web service established with competent institutions:

- REGISTER OF SECURITIES
- COMMERCIAL BANKS ACCOUNTS, DEPOSITS, LOANS, SAFE CASH
- SOCIAL WELFARE REGISTER

REGISTER OF SECURITIES - question	REGISTER OF SECURITIES - answer
Is external system data available in machine-readable format	Yes ☒ No ☐
External system MIDDLEWARE	
Data exchange type	API web service ☒
Type of web service, if applicable	SOAP ☒
Web service architecture, if applicable	Peer to peer ☒
Data format used	XML ☒
Communication protocol used	HTTPS ☒
Implemented security features	Not specified

COMMERCIAL BANKS ACCOUNTS, DEPOSITS, LOANS, SAFE CASH - question	COMMERCIAL BANKS ACCOUNTS, DEPOSITS, LOANS, SAFE CASH- answer
Is external system data available in machine-readable format	Yes ☒
Data exchange type	Other ☒
Type of web service, if applicable	Not specified
Web service architecture, if applicable	Not specified
Data format used	Not specified
Communication protocol used	HTTPS ☒

SOCIAL WELFARE REGISTER - question	SOCIAL WELFARE REGISTER - answer
Is external system data available in machine-readable format	Yes ☒ No ☐
Data exchange type	API web service ☒
Type of web service, if applicable	Not specified
Web service architecture, if applicable	Not specified
Data format used	Not specified
Communication protocol used	Not specified

Information on the availability of national registries mostly used in the asset declaration verification process on the GSB platform or in electronic form is presented in the following table:

Electronic registry	Available in the electronic form	Published on the GSB and available to IS
CITIZEN REGISTER (personal IDs, IDs for foreigners, passports, personal ID number, residence)	Yes	Yes
CITIZEN PERSONAL STATUS REGISTER (birth, marriage, death)	Yes	No
REGISTER OF MOTOR VEHICLES	Yes	Yes
REGISTER OF SHIPS/VESSELS	Yes	No
AIRCRAFT REGISTER	Unknown	No
REAL ESTATE REGISTER	Yes	Yes
REGISTER OF SECURITIES	Yes	Yes (peer-to-peer)
TAX ADMINISTRATION REGISTERS	Yes	Yes
REGISTER OF BUSINESS ENTITIESS	Yes	Yes
CENTRAL BANK REGISTER OF COMMERCIAL BANK ACCOUNTS	Unknown	Yes
SOCIAL WELFARE REGISTER	Unknown	No
REGISTER OF INTELLECTUAL PROPERTY	Unknown	No

6.6.2.4 IT governance, information security, data protection

The SCPC's IT Department is responsible for operational management and support for its information system and the underlying IT infrastructure. However, the IT Department has only 1 staff member, which is definitely not enough for adequate management and support for numerous systems and technologies used in the institution. Hence, the SCPC strongly relies on outsourcing partners for development and maintenance of the IS and IT infrastructure.

The SCPC must coordinate its electronic data exchange activities with other national registries with the Ministry of Information Society and Administration, which is responsible for operational management of the North Macedonian digital services infrastructure.

Use and administration of the asset declaration system is regulated by an implementing act. The SCPC has still not established a working group as the Change Management Advisory Body for further development and improvement of the IS. The institution possesses the source code for the information system. User satisfaction surveys are also conducted to collect user's feedback and new ideas for software improvements and development of new features.

The IT Department and outsourced partner(s) provide user support. Service Desk (Ticketing) software is leveraged to track all relevant information related to submission and resolution of support and change requests.

Additional training for existing staff and Information System training for new staff is provided by the IT Department and the outsourced partner.

The SCPC has not provided information on the annual budget for capital and operational expenditures for the information system and IT infrastructure.

The SCPC could not provide answers to questions related to information security in the submitted questionnaire because this information is treated as confidential and not shared with third parties.

6.6.2.5 E-Government

North Macedonia has recently made significant steps towards the digital transformation of public administration by setting up the necessary legislative and governance framework, establishing horizontal building blocks, digitizing base registers and creating numerous electronic services in accordance with the European Interoperability Framework (EIF).

Specific issues related to digital public administration are regulated by the following laws:

- The Law on Electronic Management and Electronic Services (Official Gazette no. 98/2019) regulates the operations of ministries, other state administration bodies, governing organisations and local self-government units, legal entities entrusted to perform public competencies and legal entities delivering and providing services of public interest during electronic exchange of data and documents and provision of eServices, when stipulated by law. The Law also regulates issues related to the

establishment and functioning of the National eServices Portal, the Service Catalogue, the Single Point of Service and Interoperability.[61]

- The Law on Public Sector Data Use established the obligation for authorities and public sector institutions to publish the data created in the exercise of their responsibilities under the law and enabled natural or legal persons to create new information, content, applications or services.
- The Law on Electronic Documents, Electronic Identification and Trust Services regulates and prescribes the creation, preservation and processing of electronic documents, electronic identification and trust services, as well as the manner of use of electronic documents, electronic signatures, electronic seals and electronic trust services in administrative and court proceedings. The Law on Electronic Documents, Electronic Identification and Trust Services is fully harmonised with the eIDAS Regulation, which is transposed in the cited Law.[62]
- The new Law on Personal Data Protection enacted in 2020 is fully aligned with the General Data Protection Regulation (EU) 2016/679.
- The Law on the Security of Network and Information Systems, practically transposes the EU Network and Information Security Directive (hereinafter: NIS Directive) into the North Macedonian legislative framework.

The Ministry of Information Society and Administration is responsible for all issues pertaining to information technologies, including interoperability activities, the policy and strategy for E-Government and the modernisation of the Macedonian public administration. The National ICT Council was established in February 2018 to prepare and monitor the implementation of the National ICT Strategy, as well as to provide guidance on annual public procurement plans, and technical specifications applicable to tender documents for public sector institutions and the procurement of ICT equipment and/or software.

The most important horizontal building blocks established in North Macedonia are:

- eServices Portal[63] - The new national portal was launched in December 2019, offering, besides information about 707 services, complete provision of 128 eServices for citizens, including payment and issuing of eDocuments. Electronic services on the portal are grouped to correspond to life events. The new portal will closely relate with the National Central Population Register and offer a Single-Sign-On for citizens.[64]
- Government Service Bus / interoperability platform - The interoperability platform enables standardized and secure electronic exchange of data and documents between state institutions. Uninterrupted flow of information through the interoperability platform reduces the time and financial costs required for transfer of data and information between institutions, increasing the efficiency and cost effectiveness of the operation of state institutions and facilitating the provision of public services tailored to the needs of citizens and businesses. The interoperability platform is based on the National Interoperability Framework which follows the EIF 2.0. In May 2021, 34 state

[61] Digital Public Administration Factsheet 2020, Republic of North Macedonia, page 17.
[62] Digital Public Administration Factsheet 2020, Republic of North Macedonia, page 19.
[63] Uslugi.gov.mk
[64] Digital Public Administration Factsheet 2020, Republic of North Macedonia, page 29.

institutions, public and private companies were connected to the interoperability platform, establishing a total of 438 web services.

- Catalogue of Public Services - The Catalogue of Public Services is an electronic database used for structured entry and management of data for all public services, such as basic data, deadlines, payments, competent authorities, legal grounds, legal remedies, category, life event, etc. The data for 707 out of the 1267 services entered into the Catalogue of Public Services are published on the public section of the portal.[65]
- eID - When a citizen registers on the Single Sign-On System (SSO) on the National e-Services Portal, an eID is created after successful identity verification. The eID is an intangible tool for electronic identification of citizens for the eServices provided by competent authorities and other entities providing services via the National e-Services Portal.[66] With the National Population Register, the unique electronic number for persons was also introduced as information mandatory for access to personal data from the register.
- Single Sign-On System (SSO) - The Single Sign-On System (SSO) allows users to register and login to the National eServices Portal. At present, only physical persons can register on the SSO. When logging in to the Portal, the user is automatically redirected to the SSO to identify with his/her username and password or qualified electronic signature certificate. After successful identification, the SSO sends an authentication token to the Portal, which in turn grants access to the private section of the Portal.
- ePayment for eServices - The National eServices Portal offers an ePayment feature for the fees and administrative taxes due, in total, for the eServices requested on the Portal, regardless of the institution issuing/delivering the service. The Portal sends a data package for each individual payment to the bank chosen for payment transactions and clears each individual payment order to the Treasury or commercial banks.[67]

6.7 Serbia

6.7.1 Legal

6.7.1.1 Competent authority

The Agency for Prevention of Corruption is an independent state authority accountable to the National Assembly of the Republic of Serbia. The Agency was established by the Law on the Anticorruption Agency, adopted in October 2008 with full implementation as of January 2010.

As a key stakeholder in the preventive activities in the fight against corruption, the Agency contributes to the development of a society with zero tolerance for corruption. With consistent, efficient and professional performance and by implementing anticorruption laws and strategic documents in this area, the Agency actively enhances the integrity and transparency within the responsibilities of public officials.

[65] Digital Public Administration Factsheet 2020, Republic of North Macedonia, page 29.
[66] Digital Public Administration Factsheet 2020, Republic of North Macedonia, page 35.
[67] Digital Public Administration Factsheet 2020, Republic of North Macedonia, page 36.

In relation to asset declarations, the Agency maintains and publishes both the Register of Public Officials and the Register of Assets and Income of Public Officials. Additionally, the Agency is responsible for verification of asset and income reports submitted by public officials.[68]

Competences

According to Article 6 of the Law on Prevention of Corruption, the Agency has the following competences:
The Agency:

- Supervises the implementation of strategic documents, submits implementation reports to the National Assembly along with actionable recommendations, provides responsible entities with recommendations on how to eliminate shortcomings in the implementation of strategic documents and initiates amendments to strategic documents;
- Adopts general enactments;
- Institutes and conducts proceedings to determine the existence of violations of this Law and imposes measures in accordance therewith;
- Decides on the existence of conflict of interest;
- Performs tasks in accordance with the law governing the financing of political activities and/or the law governing lobbying;
- Files criminal charges, requests to initiate misdemeanour proceedings and initiatives for disciplinary proceedings;
- Maintains and publishes the Register of Public Officials and the Register of Assets and Income of Public Officials in accordance with this Law;
- Verifies asset and income reports submitted by public officials;
- Maintains and verifies data from records specified in this Law;
- Acts upon complaints submitted by natural and legal persons;
- Provides opinions about the application of this Law, on its own initiative or at the request of natural or legal persons, and takes positions of importance for the application of this Law;
- Initiates adoption or amendment of regulations, provides opinions on assessed corruption risk in draft laws in fields that are particularly susceptible to corruption risks and opinions on draft laws governing issues covered by ratified international agreements in the field of prevention and combat against corruption;
- Investigates the status of corruption, analyses corruption risks and prepares reports with recommendations to eliminate risks;
- Supervises the adoption and implementation of integrity plans;
- Adopts the Training Programme and instructions in the field of prevention of corruption and monitors training implementation in public authorities;
- Performs tasks related to international cooperation in the field of prevention of corruption;
- Performs other tasks set forth by law.

[68] https://www.acas.rs/eng/index

In performing tasks within its purview, the Agency shall cooperate with public authorities and other legal persons.

The Agency shall cooperate with scientific institutions and associations.

The cooperation shall consist of joint actions in the implementation of strategic documents in the field of fight against corruption, implementation of training programmes, research into the status of corruption and other activities important for the prevention of corruption.

The Agency shall cooperate with international institutions, organisations and initiatives with a view to developing mechanisms and standards and improving practices in the field of prevention of corruption.

In cooperation with the competent state authorities, the Agency shall monitor and, as needed, participate in the coordination of international cooperation in the prevention of corruption led by state bodies and organisations, as well as the authorities of the territorial autonomy and the local self-government units (municipalities).

The competent state authorities shall keep the Agency informed of international cooperation affairs related to the prevention of corruption.

6.7.1.2 Legal framework

- Law on Prevention of Corruption ("Official Gazette of the Republic of Serbia", no. 35/19, 88/19, 94/21 and 14/22)

This Law governs the legal status, competences, organisation and operation of the Agency for Prevention of Corruption, rules concerning the prevention of conflicts of interest in the discharge of public office, accumulation of public offices, assets and income disclosure reports of public officials, procedure for deciding on violations of this Law and other issues relevant for the prevention of corruption.

The general administrative procedure law shall be applicable to proceedings conducted by the Agency in accordance with this Law.

Declarants

Regarding Article 2 paragraph 1/3, a "public official" is any person who was elected, appointed or nominated to a public authority, with the exception of persons who are representatives of private capital in managing bodies of companies that are public authorities.

For clarification of this provision, the Assembly of the Republic of Serbia provides an authentic interpretation No 11/2021-3: "This provision should be understood to apply to and be implemented for individuals who are directly elected by citizens, as well as those appointed, nominated or elected by the National Assembly, the President of the Republic, the Supreme Cassation Court, the High Judicial Council, the State Council of Prosecutors, the Government of

the Republic of Serbia, the Assembly of the Autonomous Province, the government of the autonomous province and the bodies of local self-government units."

Public officials as declarants	
Individuals who are directly elected by citizens	
Individuals appointed, nominated or elected by:	
National Assembly	President of the Republic
Supreme Court	High Judicial Council
High Prosecutorial Council	Government of the Republic of Serbia
Assembly of the Autonomous Province	government of the autonomous province
bodies of local self-government units	

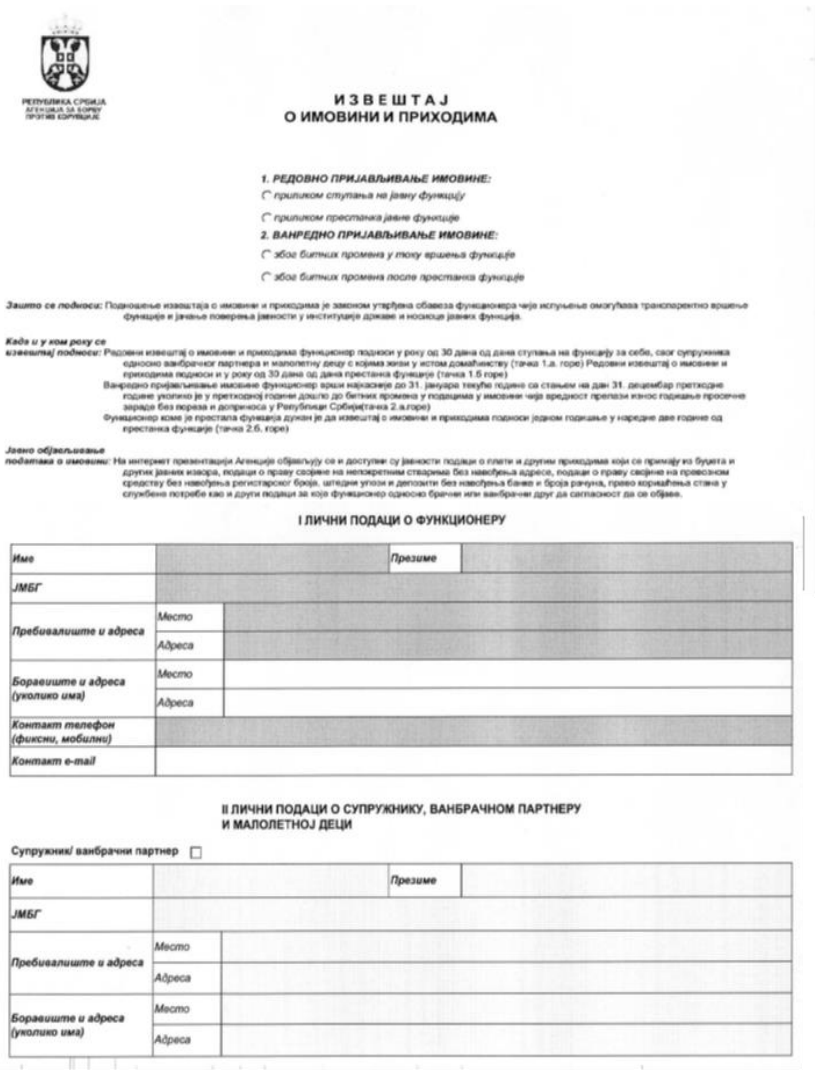
Asset declaration – forms and content

This law stipulates three cases when the public official is required to submit a report:

- *Regular Reporting of Assets and Income* (Article 68)

Within 30 days from the day of election, appointment or nomination, the public official is required to submit to the Agency a report on their assets and income, along with those of their spouse or common-law partner and under-age children if residing in the same household, as of the day of election, appointment or nomination.

A public official who is re-elected, re-appointed or re-nominated immediately upon the termination of public office needs not re-submit the report if there have been no changes in the data from the previous report. However, they must inform the Agency within 30 days from the day of re-election, re-appointment or re-nomination.



РЕПУБЛИКА СРБИЈА
АГЕНЦИЈА ЗА БОРБУ ПРОТИВ КОРУПЦИЈЕ

ИЗВЕШТАЈ
О ИМОВИНИ И ПРИХОДИМА

1. РЕДОВНО ПРИЈАВЉИВАЊЕ ИМОВИНЕ:
2. ВАНРЕДНО ПРИЈАВЉИВАЊЕ ИМОВИНЕ:

I ЛИЧНИ ПОДАЦИ О ФУНКЦИОНЕРУ

Име		Презиме	
ЈМБГ			
Пребивалиште и адреса	Место		
	Адреса		
Боравиште и адреса (уколико има)	Место		
	Адреса		
Контакт телефон (фиксни, мобилни)			
Контакт e-mail			

II ЛИЧНИ ПОДАЦИ О СУПРУЖНИКУ, ВАНБРАЧНОМ ПАРТНЕРУ И МАЛОЛЕТНОЈ ДЕЦИ

Супружник/ ванбрачни партнер ☐

Име		Презиме	
ЈМБГ			
Пребивалиште и адреса	Место		
	Адреса		
Боравиште и адреса (уколико има)	Место		
	Адреса		

The report is also mandatory for individuals whose public office has been terminated, and it must be submitted within 30 days from the day of the termination of public office, reflecting the situation as of the day of termination.

- *Extraordinary Assets and Income Report* (Article 69)

This provision prescribes that If there was a significant change in the assets or income of a public official during the previous year, the official is required to submit a report to the Agency as of 31 December of the preceding year. This report must be submitted not later than the deadline for filing the annual tax return for determination of personal income tax.
A significant change is defined as an increase or decrease in assets or income that exceeds the average annual salary without taxes and contributions in the Republic of Serbia, as reported in the preceding year. Additionally, any change in the structure of said assets is considered significant.
For individuals whose public office has been terminated, a report is to be submitted as of 31 December of the preceding year, two years after the termination of public office but not later than the deadline for filing the annual tax return for determination of personal income tax. This is required if there has been a significant change in assets and income compared to the preceding year.

- *Submission of a Report upon the Agency's Request (Article 70)*

This provision stipulates that regular and extraordinary reporting of assets and income is not applicable to councillors, members of municipal and city councils, members of municipal and city election commissions and members of bodies of public enterprises, companies, institutions and other organizations whose founder or member is a municipality, city or a city municipality. Additionally, regular and extraordinary reporting of assets and income does not apply to members of bodies of public enterprises, companies, institutions and other organizations whose founder or member is the Republic of Serbia or the autonomous province, unless the law, other regulation or enactment provides that the public official has the right to compensation based on membership.

However, in addition to that, this provision also stipulates that the Agency may require reports from the mentioned public officials within a deadline it has specified.

Article 71 prescribes the content of the Asset and Income Report, as follows:

Assets and Income Report – content	
Name and surname	Public office
National personal identification number	Permanent and temporary residence
Telephone number and email address	Other work, business activity and membership in the bodies of associations
Source and amount of net income the public official receives because s/he is discharging a public office and the source and amount of other net income s/he receives from the Budget and other public sources	Source and amount of net income from other work or business activity
Net income from scientific research, teaching,	Income from copyright, patent and other intellectual

cultural, artistic, humanitarian or sports activities	property rights
Source and amount of other net income	The right to use an apartment for official purposes
The right of ownership or the right of lease on real property	The right of ownership or the right of lease on moveable property subject to registration
Deposits in banks and other financial institutions, along with the name of the bank or financial institution, the types and numbers of accounts and the amounts of funds in said accounts	Lease of bank safes
Receivables and payables (principal, interest and period of repayment and maturity)	Shares and stakes in legal persons
Data on legal persons in which the legal person referred to in item 18 of this paragraph holds more than 3% of stakes or shares	Financial instruments
Business activity as entrepreneur	Other data considered by the public official to be important for the application of this Law

* The report shall contain the data concerning the assets and income of a public official and the family members.
* The report shall also contain the date and place of its drafting and the signature of the public official submitting it.
* The report shall list assets and income in the country and abroad.

The Agency is responsible for establishing and maintaining the Register of Assets and Income of Public Officials, which will encompass the data derived from the submitted Reports.
According to Article 67 paragraph 5 of the Law, the Assets and Income Report shall be submitted using the form and the manner prescribed by the Agency - Rulebook on the Register of Public Officials and Register of Assets and Income of Public Officials.

- Rulebook on the Register of Public Officials and Register of Assets and Income of Public Officials ("Official Gazette RS" no. 118/20, 96/2021)

This Rulebook regulates:

- The procedure and content of the notification form for entering public office and terminating public office;
- The procedure and content of the assets and income report form for public officials, spouses or common-law partners and minor children residing in the same family household;
- The method of maintaining and managing the Register of Public Officials and the Register of Assets and Income of Public Officials.

In line with this rulebook, a public official is required to electronically submit a Report to the Agency using the prescribed form within the legally specified period. This submission aims to obtain a code generated by the program. Both the Register of Public Officials and the Register of Property and Income of Public Officials are maintained in both electronic and written formats. Data from these registers, considered public under the Law on Prevention of Corruption, are published on the Agency's website. The Agency, in the process of publication, adheres to regulations governing the protection of personal data.

Data publication

Article 73 of the Law defines the data contained in the Register of Public Assets and Income of Public Officials report that are publicly accessible:
1) Name and surname of the public official;

2) The public office s/he discharges;
3) Source and amount of net income of the public official received from the budget and other public sources;
4) The right to use an apartment for official purposes, with the exception of the address where the apartment is located;
5) The right of ownership or the right of lease on real property, with the exception of the address where the real property is located;
6) The public official's right of ownership or the right of lease on moveable property subject to registration, with the exception of their registration numbers;
7) Deposits in banks and other financial institutions, without the name of the bank or other financial institution and without stating the types and numbers of accounts and the amount of funds in said accounts;
8) Shares and stakes in legal persons;
9) Legal persons in which the legal person referred to in item 8 of this paragraph has more than 3% of stakes or shares;
10) Business activity as entrepreneur.
Exceptionally, data from the Reports of public officials in state authorities that are specified in the laws governing the organisation and competence of state authorities in the suppression of organised crime, terrorism and corruption shall not be available to the public until a period of two years has elapsed since the termination of public office.

Data verification

The procedure for verification of the Report is regulated by Article 75 and Article 76 of the Law. According to Article 75, the Agency shall verify the accuracy and completeness of the data provided in the Report, as well as the timeliness of submission of the Report, according to the annual verification plan adopted by the Director.

The annual verification plan shall be adopted on the basis of a preceding analysis conducted by the Agency, considering in particular the category of public officials, the amount of their income and the amount of Budget funds at the disposal of the public authorities in which public officials discharge a public office.

The Agency shall conduct extraordinary verification of the accuracy and completeness of the data from the Report if it suspects that a Report does not present accurate and complete data.
According to Article 76 - Monitoring the Financial Status, in the process of verifying the financial status, the Agency shall assess whether there is a discrepancy between the data contained in the Report and the actual situation, or a discrepancy between the increased value of the assets and the reported income.

In the event of a discrepancy, the Agency shall invite the public official or persons referred to in Article 68, paragraph 1 of this Law, to state the reasons for said discrepancy within a period of 15 days.

If, while verifying the Report, the Agency suspects that a public official is concealing the actual value of his assets or income, the Agency may request that associated persons submit data on their assets and income directly, within 30 days from the day of receipt of the request.

Once it establishes the existence of a discrepancy, the Agency shall notify the competent authority thereof to enable it to take measures within its purview, which authority shall inform the Agency about the undertaken measures within three months from the day of receipt of the notification.
In relation to verification procedure, Article 36 of the Law prescribes that public authorities and other persons exercising public powers have an obligation, at the written and reasoned request of the Agency submitted to enable it to perform tasks within its purview, to provide the Agency with direct access to databases kept in electronic form.

If access to data in this manner is not possible, public authorities and other persons exercising public powers have an obligation, within 15 days from the date of receipt of the Agency's written and reasoned request, to submit all documents and information at their disposal and/or provide the Agency with direct insight into those documents to enable it to perform the tasks within its purview.
Other legal persons are also bound by above mentioned obligations, with the exception of banks and other financial institutions.

For the purpose of performing the tasks within its purview, the Agency is entitled to obtain data about the accounts of public officials from banks and other financial institutions; the Agency may also obtain data about the accounts of other persons, with their consent.

Additional, Article 37 of the Law - Duty to Respond to the Call of the Agency, prescribes that public officials, employees and persons engaged to perform tasks in a public authority, as well as other persons, have an obligation to respond to the call of the Agency aimed at establishing the facts in the proceedings conducted by the Agency.

The provisions mentioned above indicate that the right to immediate access to data from other public bodies represents one of the most significant advancements in the new Law on Prevention of Corruption.

The Agency now possesses the authority to gather information and documentation through highly effective and expedient procedures, representing a significant improvement from previous versions of the Law. The Agency is now empowered to have direct access to data for the purpose of executing tasks within its purview. Public authority bodies and other entities exercising public powers are under the obligation to grant the Agency direct access to databases they maintain in electronic form, as per the Agency's written and reasoned request. If direct access is not feasible, these bodies must provide all requested documents and information within 15 days of receiving the Agency's written and reasoned request. They should also allow the Agency direct insight into these documents to facilitate tasks within the Agency's scope of work. Other legal entities, excluding banks and other financial institutions, are also subject to

these obligations. However, the Agency may, for the purpose of executing tasks within its scope, obtain data on financial accounts of public officials from banks and other financial institutions, as well as data on accounts of other persons (such as associated individuals), with their consent.

Concerning verification of assets and income reports, the Agency has access to allowed set of data kept by Business Registers Agency, Republic Geodetic Authority, Central Securities, Depository and Clearing House, Ministry of Interior, whilst it also exchanges data with the Tax Administration, Administration for Prevention of Money Laundering and other relevant state bodies in writing. Furthermore, the Agency has online access to the allowed set of data from databases and registers of the Business Registers Agency, Ministry of Interior, Republic Geodetic Authority etc.

Data protection

On 9 November 2018, the National Assembly adopted a new Law on Protection of Personal Data ("Official Gazette of RS" no. 87/2018), which entered into force on 21 November 2018. It applies after nine months from the date of entry into force of the Law, except for the provisions of Article 98 (referring to the Central Register of Data Collections), which applies from the date of entry into force of the Law. With the adoption of this Law, the regulation for the protection of personal data is aligned with the General Data Protection Regulation (GDPR) (EU) 2016/679 Regulation.

In connection with the Law on Prevention of Corruption, Article 74 of this Law outlines the use of data from the Report. Regarding this, public officials within the Agency, as well as employees and individuals assigned tasks within the Agency, who have access to data from the Register of Assets and Income of Public Officials not available to the public, are prohibited from communicating, submitting or in any way providing access to such data.

Data from the Report, not accessible to the public, shall only be utilized during the verification process and, in the procedure, to determine the existence of a violation of this Law. The Agency is authorized to submit data not available to the public to the court, the public prosecutor's office, the Ministry responsible for internal affairs, the Administration for the Prevention of Money Laundering, the Tax Administration and other competent authorities, in accordance with the law.

6.7.2 Technical

6.7.2.1 IT infrastructure

The information system for collection and verification of asset declaration data and the supporting IT services are hosted in the Agency for Prevention of Corruption of the Republic of Serbia (hereinafter: *APC*).

The APC data centre is located on its premises. Equipment in the data centre is surge protected by a central UPS device and supplied by a generator that provides backup power in case of a

mains power outage. Cooling of the data centre equipment is performed by professional InRow[69] air-conditioning systems. Technical protection of the data centre is achieved by the video surveillance and electronic access control system. Data centre has a fire alarm system and NOVEC-based fire extinguishing system.

Most of the hardware and network infrastructure in the data centre has been recently renewed. IT infrastructure in the APC data centre comprises:

- Servers - virtualization hosts
- Storage systems connected with servers via an FC SAN network. UNOPS is currently conducting procurement of 2 storage systems. The first storage is intended to replace the outdated existing storage in the primary data centre, while the second one will be deployed on the disaster recovery location.
- Top-of-the-rack access switches
- Core/aggregation switch
- Network and infrastructure security

Data centre processing capacity is optimized and consolidated to maximize the utilization of installed computing nodes in the server farm, reduce electricity consumption and maintenance costs by using the VMware virtualization platform.

Top-of-the-rack access switches provide all LAN connections to virtualization hosts, storage systems and firewall LAN segments and management. Core switches perform intelligent routing and filtering of traffic between different IP subnets (VLANs).

The data centre has a high-speed fibre-optic access to the state-owned WAN network. APC's access to the Internet will be improved by implementing the 10 Gbps connection to the Internet access point established by the Office of IT and e-Government (hereinafter: OITeG). Checkpoint Next-Generation[70] Firewall devices in high availability mode are leveraged to detect and block sophisticated attacks by enforcing security policies at the application, port and protocol levels, in addition to traditional functionalities such as stateful inspection of network traffic, traffic filtering, network address translation (NAT), VPN termination, Quality of Services, etc.

Microsoft Windows Server-based Active Directory is used for centralized management of user, password, workstation and server operating system settings through the enforcement of so-called "group policies". Active Directory Domain Controllers have been installed as virtual machines on the virtualized infrastructure to perform the aforementioned roles as well as dynamic allocation of IP addresses to internal hosts - Dynamic Host Configuration Protocol (DHCP) server and domain name to IP address (and vice versa) resolution – Domain Name System (DNS).

[69] In-row cooling technology is a type of air conditioning system commonly used in data centres in which the cooling unit is placed between the server cabinets in a row to provide cool air to the server equipment more effectively.

[70] Next-Generation firewalls include intrusion prevention/detection, SSL and SSH inspection, deep-packet inspection, reputation-based malware detection as well as application awareness and control.

APC hosts a Microsoft Exchange based email server on its virtual infrastructure. The email server is used for internal and external email communication of its employees and sending/receiving notifications from/to its information systems.

Antimalware protection is applied to workstations and servers, including real time scanning of messages and content stored in the email server database. The above mentioned next-generation firewalls and Cisco IronPort mail security system represent additional layers of network, application and mail protection from malware and other forms of cyber threats. A sandbox appliance is also used to automatically launch suspicious files, programs or web links in an isolated environment and determine whether they are malicious or not based on their behaviour. Sandboxing has been proven as the most effective form of protection against ransomware[71].

VEEAM backup software is used for backing up virtual machines on the backup storage.

APC is in the process of reaching agreement with OITeG to host APC's equipment or provide OITeG's equipment in the State Data Centre in Kragujevac for the purpose of disaster recovery of APC's services.

6.7.2.2 Electronic system for collection, verification and exchange of asset declaration data

APC has established the information system that encompasses electronic registration of the:

- Notifications on entry/termination of public office for public officials
- Gifts received by public officials
- Asset declarations of public officials and their eligible family members
- Notifications on public procurement, privatization or other procedures

Public officials first need to register to the asset declaration system before they can login to the APC's information system via its website[72]. For authentication they use their username and password created in the user registration process. Once successfully logged in, public officials can perform one of the four aforementioned procedures, including asset declaration. After entering data in the electronic system via the web form, the system automatically generates the PDF form with pre-populated data and a bar code identifier. The generated PDF is automatically downloaded to the personal computer of the public official. Public officials have to print the exported PDF form with the bar code identifier, sign it and send it to the APC by registered mail.

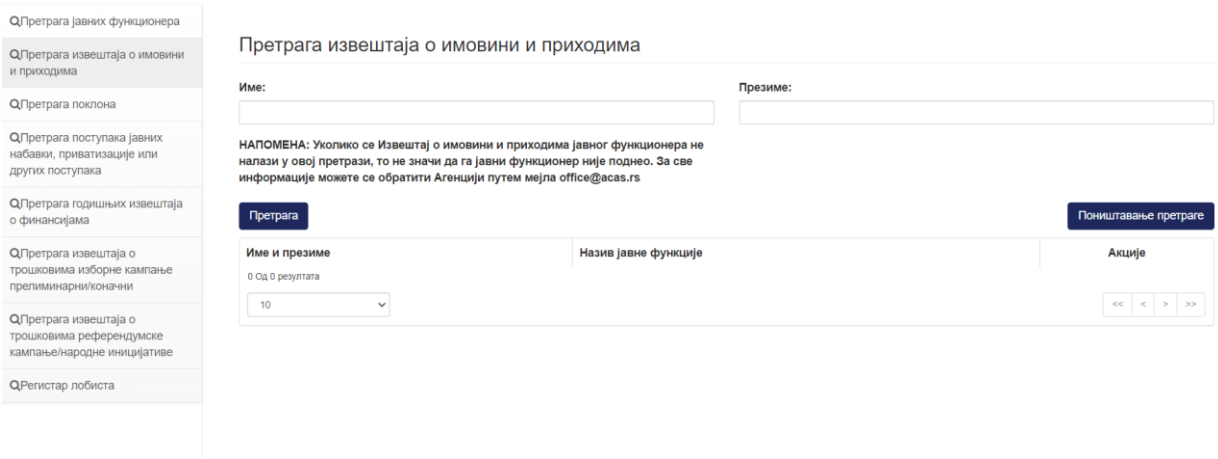
If necessary, the user can copy the data from the submitted form and create a new form with the same data. This action is extremely useful for creation and submission of any subsequent asset declaration because the public official will change or add some data, while the majority of data and information, including personal data, remains unchanged.

[71] Ransomware is a type of malware that locks and encrypts the victim's data, files, devices or systems, rendering them inaccessible and unusable until the attacker receives a ransom payment.
[72] https://publicapp.acas.rs/#/login

A public official who possesses a qualified electronic certificate may submit an electronically signed asset declaration. In that case, the public official does not have to send it in paper form via regular mail. When selecting an electronically signed document, the system checks the existence of an electronic signature on the PDF document. If the electronic signature does not exist, the user will not be able to select the document and submit it electronically.

Asset declarations are published on the website of the Agency for Prevention of Corruption. Personal data such as the personal number, date of birth, address and names of family members are not published.

The APC publishes asset declarations of public officials on its website. Front-end of the asset declaration system provides the capability to search asset declarations by name or surname. Personal data, other than name and surname of the public official, is not published.



Search of public officials' asset declarations via the APC website

APC's electronic system for collection, verification and exchange of asset declaration data (hereinafter: information system) is a custom-made application based on the eDocumentus platform for electronic document management and business process automation. It was developed by a Serbian software development and system integrator company. The application was recently improved to meet specific user needs and ensure compliance with legislative requirements.

eDocumentus is an application system designed for users who handle huge amounts of documents. It is designed to facilitate business activities in organizations that need to create, organize, distribute and view large volumes of business documents on a daily basis. This system also enables management of business processes that make up the "life cycle" of a document: from its creation to archiving in electronic form. Some of the important eDocumentus functionalities include document identification and classification, recording, reviewing, tracking changes, versioning and managing business processes. One of the key features of the eDocumentus application is that it can be integrated with other external systems. eDocumentus is a modular enterprise system that, in addition to its basic functionalities, provides certain advanced functions to its users with the assistance of software tools.

APC's information system also supports the following functionalities:

- Support for BPMN
- Business Rules Management
- Email or in-application notification for new tasks or alarms received
- Searching (including full-text search) and/or filtering of the data
- Option to define, create and maintain templates the users can use in their everyday life to generate specific content.
- Capability to prepare documents in a visual online rich text capable of combining static text and metadata in a dynamic template.
- Merging and splitting of cases/records
- Scanning and OCR of incoming paper documents
- Capability to sign, seal, store and transfer selected electronic documents using a qualified electronic certificate and qualified electronic time stamp.
- Capability to identify, accept and exchange signed messages with certification authorities (CA) registered in the National Register of Qualified Trust Service Providers.
- Capability to automatically check the validity of electronic signatures and electronic seals.
- Supporting roles and user profiles by granting access to resources (both functionality and data) related to specific profile combining the role and the user
- Support for Data Encryption
- Ad-hoc Reports & Statistics (Tools for ad hoc analysis that can be used to create a non-predefined report or to drill deeper into a static report to get details about case data, transactions, or records).

The information system technology stack is based on open-source software components.

6.7.2.3 Interoperability infrastructure and data exchange with the relevant national registries and databases

To ensure more efficient data control, the APC signed the Protocols on Business and Technical Cooperation with a number of institutions (e.g. Ministry of Interior, Republic Public Prosecutor Office, Commission for Protection of Rights in the Public Procurement Procedures, Commission for Protection of Competition, Public Procurement Office, Central Securities Depository and Clearing House, Ministry of Finance - Treasury, Tax Administration, Customs Administration, Administration for the Prevention of Money Laundering, as well as with the Business Registers Agency and the Republic Geodesic Authority). There is also a Memorandum on Cooperation signed among the Supreme Court of Cassation, Anticorruption Council and Privatization Agency. On 13 July 2023, the Serbian Business Registers Agency (hereinafter: *SBRA*) and the Agency for Prevention of Corruption signed a new agreement on data retrieval which will enable regular access and retrieval of data from SBRA's databases on business entities, beneficial owners and related parties in the upcoming period.

The APC's information system currently retrieves and verifies information, by integrating with the national GSB or NKOS[73] platform, from the following national registers[74]:

- CITIZEN REGISTER (personal IDs, IDs for foreigners, passports, personal ID number, residence)
- REGISTER OF MOTOR VEHICLES
- ARMS REGISTER
- REGISTER OF BUSINESS ENTITIESS
- CENTRAL REGISTER OF COMPULSORY SOCIAL INSURANCE

Authorized officers of the APC have been provided with user accounts and access via the respective websites to the following registers:

- REAL ESTATE REGISTER (meta data and orto-photo records)
- REGISTER OF SECURITIES

As per APC's request, National Bank of Serbia is sending data from the CENTRAL BANK REGISTER OF COMMERCIAL BANK ACCOUNTS in a machine-readable file format, which is imported into the information system.

The APC sends written data verification requests to the Tax Administration and receives data exported as a PDF file via the secure email system. A similar procedure is followed for verification of bank account data with commercial banks in the Republic of Serbia.

Information on the availability of national registries mainly used in the asset declaration verification process on the GSB platform or in any electronic form is presented in the following table:

Electronic registry	Available in the electronic form	Published on the GSB and/or available to IS
CITIZEN REGISTER (personal IDs, IDs for foreigners, passports, personal ID number, residence)	Yes	Yes
CITIZEN PERSONAL STATUS REGISTER (birth, marriage, death)	Yes	No
REGISTER OF MOTOR VEHICLES	Yes	Yes
REGISTER OF SHIPS/VESSELS	Yes	No
AIRCRAFT REGISTER	Unknown	No
REAL ESTATE REGISTER	Yes	No, but APC has an electronic insight into data from the register via website of the competent institution

[73] The National Criminal Intelligence System intended to facilitate secure data exchange between law enforcement agencies, judicial and other institutions involved in the detection, suppression, prosecution and prevention of criminal activities.

[74] Data is requested in the information system and retrieved from the External System by calling the respective web service (initiated by user action in the information system).

REGISTER OF SECURITIES	Yes	No, but APC has an electronic insight into data from the register via website of the competent institution
TAX ADMINISTRATION REGISTERS	Yes	No
REGISTER OF BUSINESS ENTITIESS	Yes	Yes
CENTRAL BANK REGISTER OF COMMERCIAL BANK ACCOUNTS	Unknown	No (manual import of received file into Information System)
CENTRAL REGISTER OF COMPULSORY SOCIAL INSURANCE	Unknown	Yes
REGISTER OF INTELLECTUAL PROPERTY	Unknown	No

6.7.2.4 IT governance, information security, data protection

APC's Sector for General Affairs and IT is responsible for operational management and support of its information system and the underlying IT infrastructure. However, mainly due to salary constraints for IT professionals in the civil service, the APC is not capable of attracting experienced IT engineers to develop and administer its information systems, IT infrastructure and IT security systems. In-house IT resources are used predominantly for basic (first level) hardware and application support. Hence, APC strongly relies on outsourcing partners for development and maintenance of the information system and IT infrastructure. To overcome these challenges, APC is considering an option to engage OITeG for maintenance of specific IT infrastructure and provision of services such as Internet access and disaster recovery.

New organisational structure within the APC has been drafted. It envisages the establishment of separate sector that will deal with IT affairs only. Although the new structure is expected to release the current IT management from dealing with other general affairs (such as procurement), problems related to the lack of IT engineers and inadequate IT staff salaries of will remain. This is due to the fact that these problems must be systematically resolved at the national civil service level.

Usage and administration of the information system is regulated by an implementing act. APC has not yet established a working group as the Change Management Advisory Body for further development and improvement of the information system. The institution possesses the source code for the information system.

APC has very limited funds available in the annual state budget for capital and operational expenditures for the information system and IT infrastructure. However, APC manages to contract maintenance of the information system and key IT infrastructure components. Maintenance of the information system also includes application improvements that have to be implemented due to legislative changes.

APC is currently in the process of preparation of the Information Security Policy and Business Continuity Plan. It is expected that these documents will be finalized and adopted by the end of the year. However, APC has implemented many information security and data protection controls, such as physical security of the data centre, deployment of next-generation firewalls, sandboxing, mail security, antimalware protection, backup, etc. As previously mentioned, the disaster recovery location will soon be established and equipped in cooperation with OITeG, international donor and implementing partners. The outcome of the implemented technical security measures and the designed high-availability IT infrastructure is almost 100% of the availability of IT services in the recent two years.

The APC currently does not have a data protection officer.

6.7.2.5 E-Government

Serbia's digital transformation accelerated in 2017 with the government's focus on building a digital government. In 2017, the OITeG was formed under the Prime Minister's Office. The Office is responsible for, inter alia: Design, harmonization, development and functioning of eGovernment and information systems, as well as the infrastructure of state administration bodies and Government services; Development and implementation of standards when introducing information and communication technologies in state administration bodies and Government services; Design, development, establishment, maintenance and improvement of the computer network of republic bodies; Provision of design, development and operation services for Internet access, Internet services and other centralized electronic services; Development planning and procurement of computer and communication equipment for the needs of state administration bodies and Government services, as well as other tasks determined by special regulations.

Key legislative enablers of digital transformation in public services and enforcement of interoperability and e-government principles are the Law on Electronic Government, the Law on Administrative Procedure, the Law on Electronic Document, Electronic Identification and Trust Services in Electronic Business, the Law on Information Security and the Law on Personal Data Protection.

The eGovernment Portal[75] of the Republic of Serbia is the central place for electronic services for all citizens, businesses and employees in the state administration, launched in 2010. The use of the Portal facilitates citizens' communication with state authorities and the entire public administration by making it easier to obtain information and appropriate forms and by simplifying the submission of requests and receiving of decisions and other documents. There are almost a million active users, who can use 800 electronic services provided by various state authorities, making the Portal the most used and most visited of all national portals. the eGovernment Portal is integrated with the emailbox and e-payment building blocks. Citizens can authenticate on the eGovernment portal using several authentications mechanisms (username and password, eID or other qualified electronic certificate issued by one of authorized and

[75] https://www.euprava.gov.rs

registered qualified identity providers), as well as via the mobile application ConsentID linked to their qualified electronic certificate.

Emailbox provides secure retrieval of electronic documents sent by public administration bodies to citizens or businesses.

All users of the eGovernment Portal can pay administrative fees electronically for all services available on the Portal. Payment by national payment card - DinaCard, MasterCard, Maestro or Visa payment cards of all the banks operating on the Serbian market, as well as electronic money, is available. Citizens can pay for the services on the eGovernment Portal via integrated electronic banking.

The Serbian National Interoperability Framework, adopted in January 2014, aims to ensure that interacting government systems protect citizen safety through adherence to regulations on privacy and personal data protection. A key piece of Serbia's interoperability approach is the Government Services Bus (GSB) – a shared communication channel that connects government databases and allows secure information exchange. OITeG established the GSB in late 2019 with support from the World Bank's Enabling Digital Governance project. GSB is a sophisticated information tool that enables data retrieval ex officio, representing a major step forward in the automation of administrative procedures and introduction of modern electronic administration in Serbia. The holders of the largest databases - the Ministry of Public Administration and Local Self-Government, Ministry of Internal Affairs, the Disability and Pension Fund of the Republic of Serbia, the Central Registry of Compulsory Social Insurance, the National Employment Service, the Ministry of Justice, the Tax Administration of the Republic of Serbia and the Republic Geodesic Authority have made dozens of their databases accessible through the Government Service Bus. According to the OITeG's estimate, in the first year after the GSB was introduced the citizens saved 500,000 hours of waiting at service counters, while the state saved about 20 million dinars on printing and publishing on paper.

The OITeG is registered in the Register of Electronic Identification Service Providers and the Identification Schemes of basic and high level of assurance. The OITeG is responsible for electronic identification and authentication of users of the Electronic Identification Portal. Establishment of the eID Portal is a prerequisite for optimal integration and interoperability of electronic administration, greater availability of services, more reliable identification and authentication and protection of electronic administration users. Its establishment enables a single sign-on for access to services and a single sign-out from all available software solutions and services, based on authentication on the eID Portal, thus satisfying the identity federation functionality.

The OITeG has established a State Data Centre, one of the most modern in the region in terms of technical and security standards, which holds the key information and communication infrastructure of the Republic of Serbia. The Centre meets the Tier 3+ standard, and the Centre's services are provided in accordance with the ISO 27001 security standard, ISO 9001 quality standards, as well as ISO 20000 for quality of service provision. The State Data Centre, in addition to storing state authorities' equipment, also provides the Government cloud service. Resources in the Data Centre are offered to the state authorities under the IaaS (Infrastructure

as a Service) model, i.e. virtual server resources are allocated upon the public administration body's request.

The eGovernment network is an information and communication network for data transmission between the authorities, managed by the OITeG. The network consists of a computer network of the Office, along with external connections that connect it to the server and computer infrastructure, state authorities, other institutions and the Internet. It includes all devices owned or leased by the OITeG and all telecommunication links that the OITeG owns or rents from telecommunications providers. This network allows the state administration to access and use the Internet and information services in the country, including connections with other national and international networks.

7. BLUEPRINT

7.1 Legal

7.1.1 Blueprint key notes

The Blueprint contains conclusions and recommendations for efficient implementation of the Treaty into national legislations of the beneficiary countries through comprehensive legal solutions. It is important to consider the need to amend laws related to asset declaration collection, verification, disclosure and data exchange.

The legal aspects of the Blueprint, along with the long-term implementation plan, should encompass recommendations for the amendments required to operationalize and transpose the Treaty into domestic legal frameworks.

7.1.2 Conclusions and recommendations for each beneficiary jurisdiction

Several conclusions and recommendations that could facilitate the implementation of the International Treaty have emerged from the assessment of beneficiary jurisdictions. The assessment approach is based on issues essential for the implementation of the Treaty.

Article 1 of the International Treaty on Exchange of Data for the Verification of Asset Declarations outlines the purpose and scope of the Treaty. The primary purpose is to prevent corruption by facilitating direct administrative exchange of information concerning asset declarations among the Parties of the Treaty. The Treaty applies to the exchange of information regardless of whether the declaration systems of the involved Parties share identical financial or personal interest aspects, cover the same categories of declarants, use similar verification procedures, or entail the same consequences. Additionally, the Treaty applies even if the Party from which information is requested does not mandate asset declarations for declarants under its jurisdiction.

Furthermore, the definitions in Article 2 of the Treaty provide clarity on key terms used in the document:
(a) “asset declaration” shall mean a declaration made to appropriate authorities disclosing finances or personal interests as generally provided for in Article 8, paragraph 5 (conflict of interest and incompatibilities), and Article 52, paragraph 5 (financial disclosure), of the United Nations Convention against Corruption and as defined by the legislation of each Party;
(b) “declarants” shall mean persons whose finances or personal interests are disclosed by means of an asset declaration, as defined by the declaration system of the requesting Party, including but not limited to the public official and his or her family members;
(c) “verification” shall mean the process of verifying the truthfulness of an asset declaration by comparing its data with information from state databases and other sources and thus detecting hidden wealth or undeclared conflicts of interest or incompatibilities;
(d) “targeted verification” shall mean a verification of an individual declaration following, in particular, a complaint, an irregularity or a similar specific indication;

(e) "random verification" shall mean a verification of a sample of declarations based on criteria defined by law of one of the Parties to the present Treaty;
(f) "Focal Point" shall mean an authority of one Party, designated according to Article 9 of this Treaty, which is competent to exchange information with a similar authority of another Party.

In this context, it is crucial to highlight the provisions of the Treaty relating to confidentiality:
Article 9. - Confidentiality
1. [Data protection] Any information obtained by a Focal Point shall be treated as confidential and protected in the same manner as information obtained under the domestic law of the respective Party and, to the extent needed to ensure the necessary level of protection of personal data, in accordance with the safeguards which may be specified by the supplying Focal Point as required under its domestic law.
2. [Circle of disclosure] Such information shall in any case be disclosed only to persons or authorities (including courts and administrative or supervisory bodies) concerned with the verification of, the enforcement or prosecution in respect of, or the determination of appeals in relation to, the veracity of asset declarations of that Party, or the oversight of the above. Only the persons or authorities mentioned above may use the information and then only for such purposes. They may, notwithstanding the provisions of paragraph 1, disclose it in public civil or administrative court proceedings or in judicial decisions of civil or administrative courts relating to asset declarations.
3. [Open data] Paragraphs 1 and 2 do not apply to information obtained under Article 7.

The legal framework governing the exchange of data in the process of verification of asset declarations is crucial for effective implementation of the Treaty.
Starting from the purpose and scope of the Treaty and the above terms, the assessment of the competences of the beneficiary countries is based on several key aspects:

- The competent authority and its competences;
- Legal framework for asset declaration collection, verification, disclosure and data exchange:
    - laws/bylaws,
    - declarants,
    - asset declaration (forms and content),
    - data publication,
    - data verification, and
    - data protection.

7.1.2.1 Albania

Albania	
Competent authority	High Inspectorate for the Declaration and Audit of Assets and Conflicts of Interest
Legal framework	- Law on the Declaration and Audit of Assets, Financial Obligations of Elected Persons and Certain Public Officials - Order no. 223/2017 "*On the approval of private interest declaration forms*" - Order no. 284/2017 "*On the approval of asset and private interest declaration forms for the candidates for different positions in the justice system*
Declarants	Clearly and specifically defined in Article 3 of the Law
Asset declaration – forms/content	Declaration of Private Interests - Electronic form Content is prescribed in the Law (article 4)
Data publication	In accordance with the legislation applicable to the right to information on official documents and protection of personal data (Article 34)
Data verification - data exchange	The procedure is prescribed in the Law - based on the Code of Administrative Procedures Public and private institutions have an obligation to provide the requested data (Article 26)
Data protection	The Law on the Declaration and Audit of Assets, Financial Obligations of Elected Persons and Certain Public Officials prescribes that collection, verification and exchange of data shall be carried out in accordance with Law no. 9887/2008 "On the Protection of Personal data". Cooperation agreements between HIDAACI and other institutions contain specific provisions for the protection of individuals' asset declaration data.

<u>Conclusions and Recommendations</u>

The crucial first step towards implementation of the International Treaty would indeed be for the Republic of Albania to sign the Treaty. This would establish commitment to the terms and principles outlined in the Treaty, fostering international cooperation in the prevention of corruption. Once signed, subsequent steps can include ratification of the Treaty and any necessary amendments or improvements of domestic legislation to ensure its alignment with the provisions of the Treaty.

Following the assessment of regulations in the Republic of Albania, it can be concluded that the situation in Albania is solid and provides a good basis for implementation of the Treaty. The law distinctly outlines which public officials are under the obligation to submit asset declarations and the procedures for collection, verification and exchange of asset declaration data are comprehensively developed in the regulations.

On the other hand, in comparison with the legislation in other countries, the law lacks detailed provisions specifying which data is required from the various institutions. Thus it would be advisable to specify the types of registry data the Inspectorate requests in the verification process and, consequently, to specify the institutions/legal entities that maintain those registries.

Regarding data protection, due to the need to ensure consistent European personal data protection standards for Albanian citizens, the Commissioner's Office (Information and Data Protection Commissioner) has intensified its efforts to align the Albanian legislation with the GDPR by drafting the Law "On Personal Data Protection", which has not been adopted yet.[76]

In this context, non-compliance with the European regulations is also implied in the provisions of the Law on the Declaration and Audit of Assets, Financial Obligations of Elected Persons and Certain Public Officials. This is particularly relevant for the content of the asset declaration, which is broadly defined in the Law. Specific details of the content that is subject to collection, verification and exchange are set in the prescribed form through an order, rather than precisely stated in the Law. This is not in accordance with Article 6 of the GDPR - Lawfulness of processing.

To address these concerns, it is recommended that the content of the asset declaration be precisely specified by a provision in the Law, outlining all the data to be collected, verified and exchanged.

Albania	
Recommendations	**Priority**
Amend the Law on the Declaration and Audit of Assets, Financial Obligations of Elected Persons and Certain Public Officials with provisions that specify the types/categories of data from various registers and the institutions that maintain those registers	Mid-term
Harmonize regulations on the protection of personal data with the GDPR by enacting a new law	Mid-term
Amend the provision of the Law on the Declaration and Audit of Assets, Financial Obligations of Elected Persons and Certain Public Officials concerning the content of the asset declaration to ensure that all data specified in the prescribed form are listed in it.	Mid-term

[76] https://www.idp.al/wp-content/uploads/2016/11/ENGLISH_Strategjia-Institucionale-2022-2025_revised.pdf

7.1.2.2 Bosnia and Herzegovina

Bosnia and Herzegovina	
Competent authorities	- Central Election Commission - Agency for Prevention of Corruption and Coordination of the Fight Against Corruption - Anticorruption and Quality Management Office of the Sarajevo Canton - Anticorruption and Quality Management Office of the Tuzla Canton - Republic Commission for the Prevention of Conflict of Interest in the Authorities of Republika Srpska
Legal framework	- Election Law of BiH - Law on Reporting and the Procedure for Data Validation of the Property of Public Position Holders in the Sarajevo Canton - Law on Declaration, Origin and Control of Assets of Elected Officials, Holders of Executive Functions and Advisors in the Tuzla Canton - Law on Prevention of Conflict of Interest in the Government Bodies of the Republika Srpska
Declarants	Various categories of public officials have been identified as declarants in the laws
Asset declaration – forms/content	The aforementioned laws specify various types of declarations
Data publication	The regulation of data publication is insufficient
Data verification - data exchange	Verification procedures are established in some of the above laws, while others do not regulate this issue at all Similarly, data exchange is addressed in some of the laws, while in others, there is no specific regulation.
Data protection	The Law on Personal Data Protection of Bosnia and Herzegovina is not in compliance with the European regulation for the protection of personal data (GDPR)

Conclusions and Recommendations

Given the territorial organization of Bosnia and Herzegovina, the complexity of its legislation logically follows. The analysis of regulations in Bosnia and Herzegovina leads to the conclusion that the situation concerning collection and verification of asset declarations is exceptionally complex. This complexity arises from the absence of a central institution with the competence to collect and verify asset declarations of public officials across the entire territory of the country.

To implement the International Treaty in the national legislation, it is necessary to fulfil certain prerequisites:

1. Establishment of an institution exclusively responsible for collection, verification and exchange of data on the property status of public officials across the entire state territory, covering all categories of public officials.

2. Harmonization of Bosnia and Herzegovina's legislation with European and regional legislation, with special consideration given to the significance of the International Treaty.

Bosnia and Herzegovina	
Recommendations	Priority
Establishment of an institution exclusively responsible for collection, verification and exchange of data on the property status of public officials across the entire state territory, encompassing all categories of public officials	Mid-term
Harmonization of Bosnia and Herzegovina's legislation with European and regional legislation, with special consideration given to the significance of the International Treaty	Mid-term
Harmonizing the regulations for the protection of personal data with the GDPR by enacting a new law	Mid-term

*7.1.2.3 Kosovo**

Kosovo*	
Competent authority	Agency for Prevention of Corruption of Kosovo*
Legal framework	Law no. 08/L- 017 - On the Agency for Prevention of Corruption Law no. 08/L-108 - On the Declaration, Origin and Control of Property and Gifts
Declarants	Senior officials/ Public officials as declarants Clearly and specifically defined in the Article 4 and Article 5 of the Law on the Declaration, Origin and Control of Property and Gifts
Asset declaration – forms/content	Declaration of assets - Electronic form Content is prescribed in the Law (Article 6)
Data publication	On the online platform, not later than 30 days from expiry of the declaration deadline (Article 12) Not published: date of birth, personal number, address, names of family members.
Data verification - data exchange	The procedure is prescribed in Article 18 of the Law - *Full control of declared data* Central and local bodies, public sector institutions, holders of public authorizations and other legal entities, are mandated to submit, at no cost, all necessary data, including personal data and documents the Agency requires to perform its duties
Data protection	Law on the Declaration, Origin and Control of Property and Gifts complies with the General Data Protection Regulation (GDPR) and follows the principles it proclaims

Conclusions and Recommendations

If Kosovo* signs the International Treaty, this will be the key foundational step signalling its commitment to international cooperation in preventing corruption. Subsequent ratification and alignment of domestic legislation are crucial for a seamless integration into the framework outlined by the Treaty. This process ensures that legal structures, procedural mechanisms and data protection measures are in harmony with the Treaty's stipulations, facilitating effective collaboration in the global effort against corruption.

It is positive to note that the regulations in Kosovo* provide a solid foundation for the implementation of the Treaty. Clearly outlined public officials who are required to submit asset declarations, compliance with data protection regulations and comprehensive procedures for data collection, verification and exchange are the essential components for effective implementation.

There is room for improvement in Kosovo's* legislation in terms of specifying the types of data and the institutions or legal entities relevant for the verification process. Adding detailed provisions can enhance the clarity and efficiency of the verification procedure, ensuring a more comprehensive and effective implementation of the Treaty.

Kosovo*	
Recommendations	**Priority**
Amend the Law to include provisions specifying the types or categories of data from various registers and the corresponding institutions responsible for maintaining those registers	Mid-term

7.1.2.4 Moldova

Moldova	
Competent authority	National Integrity Authority
Legal framework	- Law no. 132 - On the National Integrity Authority Law - Law no. 133 - On the Declaration of Assets and Personal Interests
Declarants	Defined in Article 3 of the Law on Declaration of Assets and Personal Interests
Asset declaration – forms/content	Declaration of assets and personal interests - Electronic form Content is prescribed in the Law (Article 5) The form is indicated in Annex no. 1 of the Law
Data publication	The National Integrity Authority publishes the declarations received on its official website and ensures permanent access to them for 15 years from the date of submission (Article 9) The Law prescribes which data are not public and represent information with limited access

Data verification - data exchange	The inspection of assets and personal interests of the declarant shall be conducted by the National Integrity Authority in accordance with the provisions of the Law on the National Integrity Authority (Article 32). The integrity inspector is entitled to request from any natural persons or legal entities governed by public or private law, including financial institutions, any documents and information required in order to conduct such inspection. Upon this request, the mentioned subjects shall submit to the Authority all required data, information, deeds and supporting documents
Data protection	Actions performed and the documents issued by the Integrity inspector as part of asset inspections are not public and the documents shall be published on the official website of the Authority in compliance with the Law on Personal Data Protection (Article 37)

Conclusions and Recommendations

On 23 October 2023, the Republic of Moldova officially signed the International Treaty. This significant move positioned Moldova among the pioneering signatories of the Treaty, alongside Montenegro, North Macedonia and Serbia. It underscores Moldova's pivotal commitment to the anticorruption agenda and the promotion of collaboration within the Southeast Europe (SEE) region. The subsequent phase involves ratification of the agreement in the national legislation, marking a crucial step toward its implementation.

Following the assessment, it is evident that Moldova possesses a comprehensive and well-developed regulatory framework in the domain of collection, verification and exchange of data from asset declarations. However, there is a possibility for certain improvements in the legal provisions, as follows:

Article 3 of the Law determines declarants with specificity in certain sections, but adopts a more general approach in others. The recommendation is to precisely list all public officials obligated to submit a declaration. This approach aims to eliminate any possibility of free interpretation and ensures clarity in the application of the Law.

The National Integrity Authority publishes the declarations received on its official website and ensures permanent access to them for 15 years from the date of submission, in accordance with Article 9 of the Law. There should be a reassessment of the need for public access to the declaration for a period of 15 years from submission.

Identified areas of improvement in Moldova's legislation highlight the need to specify the types of data and the pertinent institutions or legal entities involved in the verification process. Incorporating detailed provisions in this regard can enhance the clarity and efficiency of the verification procedure, contributing to a more comprehensive and effective implementation of the Treaty.

Moldova	
Recommendations	**Priority**
Amend the provision of the Law on Declaration of Assets and Personal Interests to precisely list all public officials obligated to submit a declaration - declarants	Mid-term
Reassess the provision concerning public access to the declaration for a period of 15 years from its submission	Short-term
Amend the Law on the National Integrity Authority with provisions that specify the types/categories of data from various registers and the institutions that maintain those registers	Mid-term

7.1.2.5 Montenegro

Montenegro	
Competent authority	Agency for Prevention of Corruption
Legal framework	- Law on Prevention of Corruption - Rulebook on the Content and Manner of Keeping the Register of Income and Assets of Public Officials
Declarants	Article 3 of the Law determines the definition of "public official"
Asset declaration – forms/content	Report on assets and income - Electronic form The content is prescribed in the Law (Article 24) and determined in more detail in the Rulebook on the Content and Manner of Keeping the Register of Income and Assets of Public Officials.
Data publication	Data from the Register shall be published on the website of the Agency The law prescribes which data are not public
Data verification - data exchange	The verification procedure is prescribed in the Law (Article 30) and is confidential. Checking the accuracy and completeness of the received reports through an integrated system and institutions that have data on the income and property of public officials and members of their common household
Data protection	The Law on Prevention of Corruption refers to the Regulation on Personal Data Protection

Conclusions and Recommendations

Montenegro, alongside North Macedonia and Serbia, took the pioneering step and became the first signatory of the International Treaty on 19 March 2021 in Belgrade, Serbia. This act

unequivocally demonstrated Montenegro's commitment to implementing the Treaty, a process that necessitates its integration into national legislation through parliamentary ratification.

After the assessment, it can be concluded that Montenegro has a well-developed legal framework for collection, verification and exchange of data from asset declarations. But certain improvements can be made in the specific legal provisions, as indicated below.

Article 3 of the Law defines declarants too broadly. The recommendation is to precisely list all public officials who have an obligation to submit a declaration. This approach aims to eliminate any possibility of free interpretation and ensures clarity in the application of the legal provision.

The content of the Report on Assets and Income is prescribed in Article 24 of the Law and determined in more detail by the Rulebook on the Content and Manner of Keeping the Register of Income and Assets of Public Officials. It is necessary to assess whether the legal basis for data collection set in this way follows the regulations for the protection of personal data, related to Article 6 of the GDPR - Lawfulness of processing.

The identified areas of improvement in Montenegro legislation emphasize the need to specify the types of data and the institutions or legal entities relevant for the verification process. The addition of detailed provisions in this regard can significantly enhance the clarity and efficiency of the verification procedures.

Montenegro	
Recommendations	**Priority**
Amend the provision of the Law on Prevention of Corruption to precisely list all public officials who have an obligation to submit a declaration	Mid-term
Assess the provision on the content of the asset declaration in relation to data protection regulations	Short-term
Amending the Law on Prevention of Corruption with provisions that specify the types/categories of data from various registers and the institutions that maintain those registers	Mid-term

7.1.2.6 North Macedonia

North Macedonia	
Competent authority	State Commission for Prevention of Corruption
Legal framework	- Law on Prevention of Corruption and Conflict of Interest - Rulebook on the Form and Content of the Declaration of Asset and Interests and Reporting Change in Asset and Interests
Declarants	Article 82 along with Article 8 paragraph (1) and (2) of the Law determines the declarants
Asset declaration – forms/content	Declaration of Assets and Interests - Electronic form The content is prescribed in Article 82 paragraph (2) of the Law and is determined in more detail by the Rulebook
Data publication	The data from the declaration of assets and interests and the report on changes in assets and interests are considered information of public character, except for data protected by law. These data, excluding any data protected by law, shall be published on the website of the State Commission.
Data verification - data exchange	The verification procedure is prescribed in the Law (Article 92-94) The State Commission has access, i.e. direct electronic access, to databases managed by other bodies and institutions and uses the data from the databases free of charge (list of institutions, registers)
Data protection	The Law on Prevention of Corruption contains a provision on data protection and refers to the Regulation on Personal Data Protection

Conclusions and Recommendations

North Macedonia, along with Montenegro and Serbia, made history by becoming the first signatory of the International Treaty on 19 March 2023 in Belgrade, Serbia. This decisive action unequivocally showcased North Macedonia's commitment to implementing the Treaty, a process requiring its integration into national legislation through parliamentary ratification.

After the assessment, it can be concluded that Macedonia has a well-developed legal framework for collection, verification and exchange of data from asset declarations. But certain improvements can be made in the specific legal provisions, as indicated below.

Article 8 paragraphs (1) and (2), along with Article 82 paragraph (1) of the Law defines declarants in overly expansive terms. The suggestion is to precisely list all public officials obligated to submit a declaration. This approach seeks to eliminate any possibility of subjective interpretation and guarantees precision in application of the legal provision.

The content of the Declaration of Assets and Interests is defined too broadly in Article 82 paragraph (2), and is further detailed by the Rulebook on the Form and Content of the Declaration of Assets and Interests and Reporting of Changes in Assets and Interests. In order to

comply with the Personal Data Protection Law, it is necessary to amend the legal provision to specify all data contained in the declaration form in the Law.

Related to the Law on Personal Data Protection ("Official Gazette of the Republic of North Macedonia" no. 42/20 and 294/21), this Law was harmonized with the European personal data protection regulation (GDPR) Regulation (EU) 2016/679. Regarding this Law, the laws and other acts governing collection, processing, storage use and submission of personal data shall be aligned with provisions of this Law within 18 months from the day of entry into force of this Law. However, it is important to note that the Law on Prevention of Corruption and Conflict of Interest has not yet been aligned with this Law. Therefore, it is imperative to amend the Law on Prevention of Corruption and Conflict of Interest to bring it in line with the provisions of the Personal Data Protection Law.

North Macedonia	
Recommendations	**Priority**
Amend the provision of the Law on Prevention of Corruption and Conflict of Interest to precisely list all public officials who have an obligation to submit a declaration	Short-term
Assess the provision on content of the asset declaration in relation to data protection regulation	Short-term
Amend the Law on Prevention of Corruption and Conflict of Interest to bring it in line with the provisions of the Personal Data Protection Law	Short-term

7.1.2.7 Serbia

Serbia	
Competent authority	Agency for the Prevention of Corruption
Legal framework	- Law on Prevention of Corruption - Rulebook on the Register of Public Officials and Register of Assets and Income of Public Officials
Declarants	Article 2 paragraph 1/3 of the Law, along with authentic interpretation no. 11/2021-3 determines the declarants
Asset declaration – forms/content	Asset and Income Report - Electronic form Article 71 of the Law prescribes the content of the Report The Report shall be submitted using the form and the manner prescribed by the Agency`s Rulebook
Data publication	Article 73 of the Law defines the data from the Register of Public Assets and Income of Public Officials that are publicly accessible
Data verification - data exchange	The procedure for verification of the Report is regulated by Article 75 and Article 76 of the Law. Article 36 of the Law prescribes that public authorities and

	other persons exercising public powers have an obligation, at the written and reasoned request of the Agency submitted to enable it to perform tasks within its purview, to provide the Agency with direct access to databases kept in electronic form.
Data protection	The Law on Prevention of Corruption contains data protection provisions and refers to the regulation on personal data protection which complies with the General Data Protection Regulation (GDPR)

Conclusions and Recommendations

Serbia, along with Montenegro and North Macedonia, became a pioneer signatory to the International Treaty. This significant move demonstrated Serbia's commitment to the adoption of the Treaty, a process that requires its implementation in the national legislation through parliamentary ratification. After the assessment, it can be concluded that Macedonia has a well-developed legal framework for collection, verification and exchange of data from asset declarations.

Following the assessment, it can be affirmed that Serbia possesses a well-established legal framework governing collection, verification and exchange of data from asset declarations. Additionally, the text below outlines areas where specific legal provisions could be enhanced and refined.

Article 2 paragraph 1/3 of the Law, as well as the authentic interpretation no. 11/2021-3, present declarants in overly broad terms. The recommendation is to precisely list all public officials obligated to submit a declaration. This approach aims to minimising any possibility for subjective interpretation and ensures precise implementation of the legal provision.

The Law on Prevention of Corruption currently lacks detailed provisions specifying the required data from various institutions. In this regard, it is advisable to delineate the types of data from registries that the Agency requests during the verification process. Subsequently, it is recommended to specify the institutions or legal entities responsible for maintaining those registries. This clarification would enhance the precision and effectiveness of the verification process.

Serbia	
Recommendations	**Priority**
Amend the provision of the Law on Prevention of Corruption to precisely list all public officials who have an obligation to submit a declaration	Mid-term
Amend the Law on Prevention of Corruption with provisions that specify the types/categories of data from various registers and the institutions that maintain those registers	Mid-term

7.2 Technical

7.2.1 Blueprint key notes

Blueprint contains recommendations for improvements in IT infrastructure, asset declaration collection, verification and disclosure information systems and the data exchange architecture in each beneficiary jurisdiction. Recommendations are focused on fulfilling technical pre-requisites for establishment of the asset declaration data exchange mechanism at the regional level.

This includes the proposed concept for establishing data exchange necessary for the technical implementation of the Treaty.

7.2.2 Conclusions and recommendations for improvement of IT infrastructure, information systems and information security measures in each beneficiary jurisdiction

7.2.2.1 Albania

Recommendations	Priority
IT infrastructure	
From the IT infrastructure point of view, there are no obstacles to establishment of asset declaration data exchange.	N/A
Electronic system for collection, verification and exchange of asset declaration data	
The EACIDS system meets minimum functional and architectural requirements to act as national backend system that can receive and process asset verification requests from other jurisdictions and send a response to the other Focal Point.	N/A
Design and implement the ASDEVEDEX Gateway and Connector for e-Delivery of data and messages between Focal Points.	Mid-term*
Design and develop e-signature functionality in the EACIDS system to be capable to: • **sign, seal, store and transfer selected electronic documents using a qualified electronic certificate and qualified electronic time stamp.** • **identify, accept and exchange signed messages with certification authorities (CA) registered in the National Register of Qualified Trust Service Providers.** • **automatically check the validity of electronic signatures and electronic seals.**	Mid-term
Design and develop data encryption functionality in the EACIDS database	Mid-term
Interoperability infrastructure and data exchange with the relevant national registries and databases	
Perform customization of the EACIDS backend system in order to enable calls to appropriate web services to enable retrieval of data from other relevant electronic registers once these registers are published and made	Short-term**

available via GG.	
Creation and sharing of web service authentication parameters, testing calls to web services and putting them into production	Short-term**
Implement functionalities that will enable direct retrieval and import of data in machine-readable format from external systems that can then be leveraged to perform automatic asset verification routines under pre-defined rules.	Short-term
IT governance, information security, data protection	
From the IT governance point of view, there are no obstacles to establishment of the asset declaration data exchange.	N/A
Improve the labour status of IT professionals in HIDAACI in terms of salaries and other financial and non-financial benefits.	Short-term
The IT expert cannot provide any recommendations related to improvement of the information security framework and implementation of technical measures for personal data protection, since HIDAACI was not able to share relevant information on the current status of this aspect due to confidentiality of such data.	N/A

* Depends on the legal incorporation of the Treaty into national legislation.

** Depends on existence of the legal basis and availability of an interoperable electronic database from which to retrieve data.

7.2.2.2 Bosnia and Herzegovina

Recommendations	Priority
Focal Point	
Designate an institution that will act as the Focal Point in accordance with the Treaty once Bosnia and Herzegovina signs the Treaty and incorporates it into its legislation.	Mid-term
Design and develop an information system that will act as national backend IT system for: **• Reception of the digitally signed electronic message with accompanying electronic documents (request for data verification) from the Focal Point of the other jurisdiction and verification of the sender** **• Registration of the electronic message in the national asset declaration and verification IT system (hereinafter: national backend IT system)** **• Sending the data exchange (query) from the national backend IT system to the competent national electronic register (based on the requested data from other jurisdiction) using the already established data exchange mechanisms (i.e. web service) between respective endpoints in accordance with applicable legislation.** **• Reception of the electronic response from competent national electronic register in the national backend IT system** **• Forwarding of the electronic response from the national backend IT system to the Focal Point of the other jurisdiction using ASDEVEDEX technical interoperability components (national Gateways and Connectors) based on mutually agreed semantic interoperability documents.** **• Registration of the request for data verification in the national backend IT system and sending of the digitally signed electronic message with**	Mid-term

accompanying electronic documents to the Focal Point of the other jurisdiction using ASDEVEDEX technical interoperability components (national Gateways and Connectors) based on mutually agreed semantic interoperability documents **• Reception of the electronic response from the Focal Point of the other jurisdiction and registration in the national backend IT system using ASDEVEDEX technical interoperability components (national Gateways and Connectors) based on mutually agreed semantic interoperability documents**	
Design and implement ASDEVEDEX Gateway and Connector for e-Delivery of data and messages between Focal Points.	Mid-term*
Connect the national backend IT system to GSB instance at the level of Bosnia and Herzegovina to enable retrieval of data from external systems – registers relevant for the asset declaration verification process at all governance levels in Bosnia and Herzegovina. The national backend system should be capable of receiving aggregate responses from the GSB instance. This implies, for example, sending one query to check whether a foreign official has property registered in the real estate registers in both entities and receiving one response from the GSB instance that will contain aggregated information from real estate registers in the Federation of Bosnia and Herzegovina and Republika Srpska. **The national backend IT system at the Focal Point should implement functionalities that will enable direct retrieval and import of data in machine-readable format from external systems via the GSB instance at the level of Bosnia and Herzegovina that can then be leveraged to perform automatic asset verification routines under pre-defined rules.**	Mid-term
E-government	
Adopt the Law on Electronic Identification and Trust Services for Electronic Transactions at the state level, maintain and publish a single node with the national eID scheme and trust list for Bosnia and Herzegovina in accordance with eIDAS provisions. A national eIDAS node should be established at the level of Bosnia and Herzegovina for exchange of electronic eID schemes with EU member states and WB6 countries, thus ensuring cross-border interoperability and recognition of qualified certificates issued by BiH trust service providers in regional and international projects, such as the implementation of the Treaty.	Short-term
The laws regulating electronic identification and trust services at all levels in Bosnia and Herzegovina should envisage mutual recognition of trust services provided by all trust service providers at different levels, for online services offered anywhere in BiH.	Short-term
Establishment of organizational, technical and semantic aspects of the Interoperability Framework across all government levels in BiH.	Mid-term
Perform technological refreshment of the GSB instances at the level of Bosnia and Herzegovina and Federation of Bosnia and Herzegovina, and	Short-term
Draft and adopt e-government laws at all governance levels in Bosnia and Herzegovina that will proclaim mandatory for public administration bodies to electronically exchange data with other institutions that have the legal basis to access such data. Data exchange would be performed by publishing web services at the respective GSB instance. In the context of implementation of the Treaty, it would be necessary that all web services, providing queries to	Mid-term

and responses from national registers relevant for asset declaration verification processes, are published at the respective GSB instance (i.e. web service of the real estate register in Republika Srpska is published on the Republika Srpska GSB instance, while the web service of the real estate register in the Federation of Bosnia and Herzegovina is published on the FBiH GSB instance.	

* Depends on the legal incorporation of the Treaty into national legislation and establishment of the national backend IT system at Focal Point.

*7.2.2.3 Kosovo**

Recommendations	Priority
IT infrastructure	
From the IT infrastructure point of view, there are no obstacles to establishment of asset declaration data exchange.	N/A
To further improve physical and environmental security of the data centre, the APK should install video surveillance, anti-burglary protection and Novec-based fire extinguishing system in the data processing facility.	Short-term
Deploy an additional firewall in clustered mode the with existing device in order to achieve high-availability and redundancy of network security functions performed by these firewalls.	Short-term
Establish the disaster recovery location and related business continuity management policies. The preferred, cost-efficient solution would be to reuse the state disaster recovery centre, if it exists. If it does not exist, consider planning a disaster recovery location in coordination with the AIS.	Short-term
Electronic system for collection, verification and exchange of asset declaration data	
The DMSA system meets minimum functional and architectural requirements to act as the national backend system that can receive and process asset verification requests from other jurisdictions and send a response to the other Focal Point.	N/A
Design and implement ASDEVEDEX Gateway and Connector for e-Delivery of data and messages between Focal Points.	Mid-term*
Further improve the information system to ensure the following capabilities: • **Option to define, create and maintain templates the users can use in their everyday life to generate specific content.** • **Capability to prepare documents in a visual online rich text editor capable of combining static text and metadata in a dynamic template.** • **Ability to manage documents in workgroups (multiple author participation), to facilitate document control, auditing, editing and timeline management.** • **Capability to sign, seal, store and transfer selected electronic documents using a qualified electronic certificate and qualified electronic time stamp.** • **Capability to identify, accept and exchange signed messages with certification authorities (CA) registered in National Register of**	Mid-term

Qualified Trust Service Providers. • **Capability to automatically check the validity of electronic signatures and electronic seals.** • **Ad-hoc Reports & Statistics (Tools for ad hoc analysis that can be used to create a non-predefined report or to drill deeper into a static report to get details about case data, transactions, or records).**	
Design and develop data encryption functionality in the DMSA database	Mid-term
Establish compliance of the front-end of the asset declaration system with WAI (Web Accessibility Initiative) level A1 – accessible by people with disabilities.	Mid-term
Interoperability infrastructure and data exchange with the relevant national registries and databases	
Perform customization of the DMSA backend system in order to enable calls to appropriate web services to enable retrieval of data from other relevant electronic registers once these registers are published and made available via GG.	Short-term**
Creation and sharing of web service authentication parameters, testing calls to web services and putting them into production	Short-term**
Implement functionalities that will enable direct retrieval and import of data in machine-readable format from external systems that can then be leveraged to perform automatic asset verification routines under pre-defined rules.	Short-term
IT governance, information security, data protection	
Improve human resources capacities in the APK to manage Information System and provide user support and training by employing additional staff member(s) and improve their labour status in terms of salaries and other financial and non-financial benefits.	Short-term
The IT expert cannot provide any recommendations related to improvement of the IT Governance, Information Security framework and implementation of technical measures for personal data protection, since APK was not able to share relevant information on the current state in this aspect due to confidentiality of such data.	N/A

* Depends on the legal incorporation of the Treaty into national legislation.

** Depends on existence of the legal basis and availability of interoperable electronic database from which to retrieve data.

7.2.2.4 Moldova

Recommendations	Priority
IT infrastructure	
From the IT infrastructure point of view, there are no obstacles to establishment of asset declaration data exchange.	N/A
Deploy an additional firewall in clustered mode with the existing device in order to achieve high-availability and redundancy of network security functions performed by these firewalls.	Short-term
Electronic system for collection, verification and exchange of asset declaration data	
The e-Integrity information system meets minimum functional and architectural requirements to act as the national backend system that can receive and process asset verification requests from other jurisdictions and send responses to other Focal Points.	N/A
Design and implement ASDEVEDEX Gateway and Connector for e-Delivery of data and messages between Focal Points.	Mid-term*
Further improve the information system to ensure: • **Capability to identify, accept and exchange signed messages with certification authorities (CA) registered in National Register of Qualified Trust Service Providers.** • **Capability to automatically check the validity of electronic signatures and electronic seals.** • **Comply with WAI (Web Accessibility Initiative) level A1 – accessible by people with disabilities.** • **Datawarehouse & Business Intelligence (Datasets included into DW/BI).**	Mid-term
Interoperability infrastructure and data exchange with the relevant national registries and databases	
Perform customization of the e-Integrity information system in order to enable calls to appropriate web services to enable retrieval of data from other relevant electronic registers once these registers are published and made available via the Mconnect GSB.	Short-term**
Creation and sharing of web service authentication parameters, testing calls to web services and putting them into production	Short-term**
IT governance, information security, data protection	
From IT governance point of view, there are no obstacles to establishment of asset declaration data exchange.	N/A
Improve human resource capacities in the NIA to manage the information system and provide user support by employing additional staff and improve their labour status in terms of salaries and other financial and non-financial benefits.	Short-term
Obtain ISO/IEC 27001 certification to finalize the Information Security Management activities performed to date	Mid-term

* Depends on the legal incorporation of the Treaty into national legislation.

** Depends on existence of the legal basis and availability of interoperable electronic database from which to retrieve data.

7.2.2.5 Montenegro

Recommendations	Priority
IT infrastructure	
Renew outdated hardware, network and network/application security equipment in the data centre (i.e. storage systems, FC SAN Switch, core/aggregation switches, internal firewalls) by establishing scalable high-availability infrastructure for processing and storage of asset declaration data and underlying IT services	Short-term
Establish the disaster recovery location and related business continuity management policies. The preferred, cost-efficient solution would be to reuse the state disaster recovery centre, if it exists. If it does not exist, consider planning of disaster recovery location in coordination with the Ministry of Public Administration.	Short-term
Electronic system for collection, verification and exchange of asset declaration data	
The new information system meets minimum functional and architectural requirements for the national backend system that can receive and process asset verification requests from other jurisdictions and send responses to other Focal Points.	N/A
Put the new asset declaration and verification information system into production	Short-term
Design and implement ASDEVEDEX Gateway and Connector for e-Delivery of data and messages between Focal Points.	Mid-term*
In addition to functionalities supported by the existing system, the new information system should be capable to: • **Perform data encryption within the database** • **Datawarehouse & Business Intelligence (Datasets included into DW/BI)**	Mid-term
Establish compliance of the front-end of the asset declaration system with WAI (Web Accessibility Initiative) level A1 – accessible by people with disabilities.	Mid-term
Interoperability infrastructure and data exchange with the relevant national registries and databases	
Perform customization of the information system in order to enable calls to appropriate web services for retrieval of data from other relevant electronic registers once these registers are published and made available via the national GSB or secure peer-to-peer connection (public officials account balances at commercial banks).	Short-term**
Creation and sharing of web service authentication parameters, testing calls to web services and putting them into production	Short-term**
Implement functionalities that will enable direct retrieval and import of data in machine-readable format from external systems that can then be leveraged to perform automatic asset verification routines under pre-defined rules.	Short-term
IT governance, information security, data protection	
Improve capacities of the Department for Analytics and Information Technology to manage the information system and provide user support and training by employing additional staff and improve their labour status in terms of salaries and other financial and non-financial benefits.	Short-term
Establish a working group as the Change Management Advisory Body for	Short-term

further development and improvement of the IS.	
Design and implement Service Desk (Ticketing) software or call centre to track all relevant information related to submission and resolution of support and change requests.	Mid-term
Establish the Information Security Management framework by adopting the Information Security Policy and other accompanying policies, such as Business Continuity Plan, Information Security Incident Management, to regulate organizational aspects of information security and data protection.	Mid-term
Data protection officer duties should be assigned to specific positions outside the IT Sector in the new organisational structure.	Short-term

* Depends on the legal incorporation of the Treaty into national legislation.

** Depends on existence of the legal basis and availability of interoperable electronic database from which to retrieve data.

7.2.2.6 North Macedonia

Recommendations	Priority
IT infrastructure	
Renew hardware and network equipment in the data centre by establishing scalable high-availability infrastructure for processing and storage of asset declaration data and underlying IT services	Short-term
Implement a backup policy based on specialized backup software and dedicated backup storage device.	Short-term
Establish a disaster recovery location and related business continuity management policies. The preferred, cost-efficient solution would be to reuse the state disaster recovery centre, if it exists. If it does not exist, consider planning the disaster recovery location in coordination with the Ministry of Information Society and Administration.	Short-term
Electronic system for collection, verification and exchange of asset declaration data	
The information system meets minimum functional and architectural requirements to act as the national backend system that can receive and process asset verification requests from other jurisdictions and send responses to other Focal Points.	N/A
Design and implement ASDEVEDEX Gateway and Connector for e-Delivery of data and messages between Focal Points.	Mid-term*
Further improve the Information system to be capable to: • **define, create and maintain templates that shall be used by the users in their everyday life for generating specific content.** • **In addition to the predefined, system-wide templates, capability to prepare documents in a visual online rich text editor capable of combining static text and metadata in a dynamic template.** • **sign, seal, store and transfer selected electronic documents using a qualified electronic certificate and qualified electronic time stamp.** • **identify, accept and exchange signed messages with certification authorities (CA) registered in National Register of Qualified Trust Service Providers.**	Mid-term
Design and develop data encryption functionality within Information System database	Mid-term

Establish compliance of the front-end of the asset declaration system with WAI (Web Accessibility Initiative) level A1 – accessible by people with disabilities.	Mid-term
Interoperability infrastructure and data exchange with the relevant national registries and databases	
Perform customization of the information system in order to enable calls to appropriate web services for retrieval of data from other relevant electronic registers once these registers are published and made available via the national GSB (CITIZEN PERSONAL STATUS REGISTER - birth, marriage, death, Register of ships, aircrafts, Social welfare register).	Short-term**
Creation and sharing of web service authentication parameters, testing calls to web services and putting them into production	Short-term**
Implement functionalities that will enable direct retrieval and import of data in machine-readable format from external systems that can then be leveraged to perform automatic asset verification routines under pre-defined rules.	Short-term
IT governance, information security, data protection	
Improve the capacities of the IT Department to manage the information system and provide user support and training by employing additional staff and improve their labour status in terms of salaries and other financial and non-financial benefits.	Short-term
Establish a working group as the Change Management Advisory Body for further development and improvement of the IS.	Short-term
The IT expert cannot provide any recommendations related to improvement of the information security framework and implementation of technical measures for personal data protection, since SCPC was not able to share relevant information on the current status of this aspect due to confidentiality of such data.	N/A

* Depends on the legal incorporation of the Treaty into national legislation.

** Depends on existence of the legal basis and availability of interoperable electronic database from which to retrieve data.

7.2.2.7 Serbia

Recommendations	Priority
IT infrastructure	
From the IT infrastructure point of view, there are no obstacles to establishment of asset declaration data exchange.	N/A
Finalize activities related to establishment of the disaster recovery location. IT infrastructure at the disaster recovery location should be designed in such a way to provide additional compute/storage resources or load-balancing features to IT services deployed at the primary location.	Short-term
Electronic system for collection, verification and exchange of asset declaration data	
The information system meets minimum functional and architectural requirements to act as the national backend system that can receive and process asset verification requests from other jurisdictions and send responses to other Focal Points.	N/A
Design and implement ASDEVEDEX Gateway and Connector for e-Delivery of data and messages between Focal Points.	Mid-term*

Interoperability infrastructure and data exchange with the relevant national registries and databases	
Perform customization of the information system in order to enable calls to appropriate web services for retrieval of data from other relevant electronic registers once these registers are published and made available via the national GSB or secure peer-to-peer connection (Real Estate Register, Register of Securities, Tax Administration registries, Central Bank Register of Commercial Bank Accounts).	Short-term**
Creation and sharing of web service authentication parameters, testing calls to web services and putting them into production	Short-term**
Implement functionalities that will enable direct retrieval and import of data in machine-readable format from external systems that can then be leveraged to perform automatic asset verification routines under pre-defined rules.	Short-term
IT governance, information security, data protection	
From IT governance point of view, there are no obstacles to establishment of asset declaration data exchange.	N/A
Adopt a new organisational structure that envisages separation of IT and General Affairs so that the new IT Sector management can concentrate solely on strategic and operational planning of IT-related activities.	Short-term
Improve the capacities of the future IT Sector to manage the information system and provide user support and training by employing additional staff and improving their labour status in terms of salaries and other financial and non-financial benefits.	Short-term
Consider engaging OITeG to take over the maintenance of specific IT infrastructure components and provision of specific IT services to achieve a higher level of service and cost-effectiveness due to limited funds in the APC's budget.	Mid-term
Establish a working group as the Change Management Advisory Body for further development and improvement of the IS.	Short-term
Establish the Information Security Management framework by adopting the Information Security Policy as the cornerstone act to regulate organizational aspects of information security and data protection.	Mid-term
Data protection officer duties should be assigned to a specific position outside the IT Sector in the new organisational structure.	Short-term

* Depends on the legal incorporation of the Treaty into national legislation.

** Depends on existence of the legal basis and availability of interoperable electronic database from which to retrieve data.

7.2.3 Technical concept for data exchange

7.2.3.1 Compliance with the European Interoperability Framework

The European Interoperability Framework for Pan-European e-Government Services (hereinafter: EIF) serves to support the interoperability of different system components. The EIF supports cross-border and cross-sector interoperability and guides public administrations in reaching this objective. It also supports the integration of various National Interoperability Frameworks (hereinafter: NIF) by indicating common elements such as principles, policies, guidelines, recommendations and standards. EIF can be considered as a 'meta framework' that establishes generic principles in

common between several NIFs which are, in general, more detailed and often prescriptive. The EIF promotes and supports the delivery of European public services by fostering cross-border and cross-sector interoperability and guiding public administrations in their work to provide European public services to businesses and citizens. It also complements and ties together the various National Interoperability Frameworks at European level.

National Interoperability Frameworks of Parties of the Treaty, where existing, are also based on the EIF.

Technical concept is envisaged to adhere to the following principles and recommendations of the European Interoperability Framework 3.0:

Openness

Recommendation 3: Ensure a level playing field for open source software and demonstrate active and fair consideration for use of open source software, taking into account the total cost of ownership of the solution.

Recommendation 4: Give preference to open specifications, taking due account of the coverage of functional needs, maturity and market support and innovation.

Transparency

Recommendation 5: Ensure internal visibility and provide external interfaces for European public services.

Reusability

Recommendation 6: Reuse and share solutions and cooperate in the development of joint solutions when implementing European public services.

Recommendation 7: Reuse and share information and data when implementing European public services, unless certain privacy or confidentiality restrictions apply.

Technological neutrality and data portability

Recommendation 8: Do not impose any technological solutions on citizens, businesses and other administrations that are technology-specific or disproportionate to their real needs.

Recommendation 9: Ensure data portability, namely that data is easily transferable between systems and applications supporting the implementation and evolution of European public services without unjustified restrictions, if legally possible.

User-centricity

Recommendation 10: Use multiple channels[77] to provide the European public service, to ensure that users can select the channel that best suits their needs.

[77] A multi-channel service delivery approach means the availability of alternative channels, physical and digital, to access a service, as users may prefer different channels depending on the circumstances and their needs.

Recommendation 11: Provide a single point of contact in order to hide internal administrative complexity and facilitate users' access to European public services.

Recommendation 12: Users should be asked to provide only the information that is absolutely necessary to obtain a given public service.

Recommendation 13: As far as possible under the legislation in force, ask users of European public services once-only and relevant-only information.

Inclusion and accessibility

Recommendation 14: Ensure that all European public services are accessible to all citizens, including persons with disabilities, the elderly and other disadvantaged groups. For digital public services, public administrations should comply with e-accessibility specifications that are widely recognised at European or international level.

Security and privacy

Recommendation 15: Define a common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses.

Multilingualism

Recommendation 16: Use information systems and technical architectures that cater for multilingualism when establishing a European public service. Decide on the level of multilingualism support based on the needs of the expected users.

Administrative simplification

Recommendation 17: Simplify processes and use digital channels whenever appropriate for the delivery of European public services, to respond promptly and with high quality to users' requests and reduce the administrative burden on public administrations, businesses and citizens.

Preservation of information

Recommendation 18: Formulate a long-term preservation policy for information related to European public services and especially for information that is exchanged across borders.

Assessment of effectiveness and efficiency

Recommendation 19: Evaluate the effectiveness and efficiency of different interoperability solutions and technological options considering user needs, proportionality and balance between costs and benefits.

7.2.3.2 Reuse of best practices from similar European projects

This technical concept is designed to leverage best practices and solutions implemented in similar European cross-border data exchange projects such as e-Codex. e-CODEX is the main European tool for establishing an interoperable, secure and decentralised communication network between national IT systems in cross-border civil and criminal proceedings.

e-CODEX offers a European digital infrastructure for secure cross-border communication in the field of justice. The EU co-founded project strives to improve the exchange of cross-border legal information and enhances the access of citizens and businesses to legal means in Europe.

The project provides easy access to judicial information and boosts judicial cooperation by improving the interoperability between legal authorities within the European Union.

7.2.3.3 Technical concept – background information

Technical concept on the exchange of data for the verification of asset declarations is in further text referred as acronym **ASDEVEDEX**. Technical concept is designed to cope with different legal systems of Parties of the Treaty and include a methodology for mutual equal interpretation of legal terms. All solutions are based on the principle of subsidiarity, so that national IT-solutions can be preserved and reused to the maximum extent possible.

ASDEVEDEX is conceptualized to enable smooth implementation of the International Treaty on Exchange of Data for the Verification of Asset Declarations and help achieving its purpose to prevent corruption by providing for a direct administrative exchange of information concerning asset declarations between Parties of the Treaty.

The ASDEVEDEX aims at providing more effective, an easier and safer electronic exchange of data for the verification of asset declarations between Parties of the Treaty through common standards and greater interoperability of information systems.

The ASDEVEDEX aims to improve interoperability between national asset declaration verification systems of Parties of the Treaty with minimum impact on existing national ICT solutions. In this context transport of data and documents is a key element of the solution. Any functionality to be developed for a cross-border exchange of asset declaration verification requests and responses means transport of information from one country to another. The ASDEVEDEX translates national standards of documentation to the ASDEVEDEX standard through mapping to ensure reliable transportation of the data.

More specifically and from a technological perspective, ASDEVEDEX is a multilateral, content agnostic e-delivery infrastructure. It uses best practices gathered around similar EU projects related to electronic data exchange in cross-border judicial cooperation. It is interoperability layer for exchange of data for verification of asset declarations among Parties of the Treaty. This e-delivery infrastructure intends to take into account experience with standards coming from previous EU large

scale projects and reuse existing building blocks established by the Connecting Europe Facility (CEF) projects.[78]

The ASDEVEDEX architecture enables the interconnection of Party's Focal Points through national Gateways and Connectors. No central component is involved in the communication.

While asset declarations verification procedures provide a certain level of standardisation across the region, their functioning relies on national organisations, procedures as well as technologies and specific frameworks (e.g. e-identification, e-signature etc.). When electronic communication crosses national borders, mutual trust and acceptance of the national systems that manage such communication is needed.

Memorandum of Understanding / Protocol needs to be established to recognise exchanged electronic information with a minimum level of organisational requirements needed for operational and technical matters related to, or in connection with, asset declarations verification among Parties of the Treaty.

7.2.3.4 Actors involved in ASDEVEDEX

Actors involved in the future design and implementation of the ASDEVEDEX data exchange concept are:

Focal Points of Parties of the Treaty

Focal Points of Parties of the Treaty will be responsible for:

- Reception of the digitally signed electronic message with accompanying electronic documents (request for data verification) from the Focal Point of other jurisdiction and verification of the sender
- Registration of the electronic message in the national asset declaration and verification IT system (hereinafter: national backend IT system)
- Sending of data exchange (query) from national backend IT system towards competent national electronic register (based on the requested data from other jurisdiction) using already established data exchange mechanisms (i.e. web service) between respective endpoints in accordance with applicable legislation.
- Reception of the electronic response from competent national electronic register in the national backend IT system
- Forwarding of the electronic response from the national backend IT system to the Focal Point of other jurisdiction using ASDEVEDEX technical interoperability components (national Gateways and Connectors) based on mutually agreed semantic interoperability documents.
- Registration of the request for data verification in the national backend IT system and sending of the digitally signed electronic message with accompanying electronic documents to the Focal Point of other jurisdiction using ASDEVEDEX technical interoperability

[78] CEF project funded by the European Commission is devoted to stimulate and support projects of common interest for the deployment and operation of digital service infrastructures.

components (national Gateways and Connectors) based on mutually agreed semantic interoperability documents

- Reception of the electronic response from the Focal Point of other jurisdiction and registration in the national backend IT system using ASDEVEDEX technical interoperability components (national Gateways and Connectors) based on mutually agreed semantic interoperability documents

Public administration or other institutions/organizations competent for national registers/databases containing data subject of cross-border data verification:

Public administration or other institutions/organizations competent for national registers/databases, containing data that is subject to cross-border data verification will be responsible for:

- Reception of data exchange (query) from the national backend IT system (based on the requested data from other jurisdiction) using already established data exchange mechanisms (i.e. web service) between respective endpoints in accordance with the applicable legislation.
- Sending of the electronic response to the national backend IT system.

Regional Working Group for Technical and Semantical Interoperability of the ASDEVEDEX

The Regional Working Group for Technical and Semantical Interoperability of the ASDEVEDEX should consist of representatives of each Party of the Treaty. Each Party of the Treaty (Focal Point) should designate at least two representatives, one lawyer and one IT professional.

The working group will be responsible to prepare, validate, adopt and update the Protocol and its implementing annexes. The Protocol and its annexes will regulate the legal, organizational, semantical, technical and security aspects of ASDEVEDEX data exchange between the Parties of the Treaty. The Protocol should also provide a mechanism for recognition of information exchanged across borders between Parties of the Treaty.

7.2.3.5 ASDEVEDEX architectural guidelines

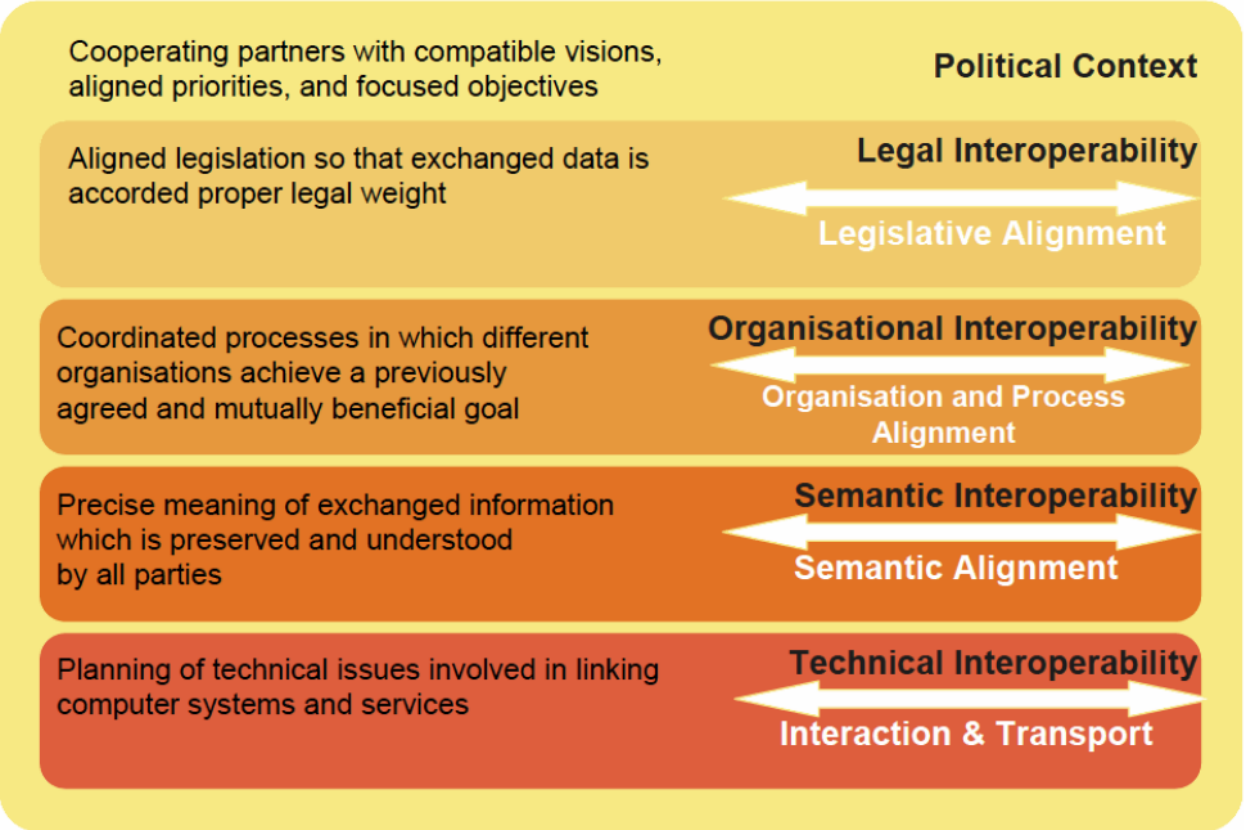
ASDEVEDEX should rely on the EIF in order to support the interoperability of different systems' components. The ASDEVEDEX should focus on four EIF layers of intervention: legal interoperability, organisational interoperability, semantic interoperability and technical interoperability.

Reaching legal interoperability refers to the reduction of incompatibilities between legislation in different Parties of the Treaty regarding data exchange in asset declarations verification. Moreover, the Treaty itself deals with the issue of legal interoperability establishing that Parties providing data and documents via ASDEVEDEX may trust each other in terms of confidentiality, e-Identification and e-Signature. Other more specific Memorandums of Understanding or Protocols deriving from the Treaty may be agreed upon by the Parties of the Treaty to regulate organizational, technical and semantical interoperability aspects of the data exchange.

Organisational interoperability refers to the cooperation between Focal Points of Parties of the Treaty to achieve mutually agreed goals and implies integrating related data exchange.

Semantic interoperability aims at ensuring that the precise meaning of information that is shared between Parties of the Treaty is understood and preserved throughout these exchanges. **Therefore it consists of developing a vocabulary to describe data exchanges and ensuring that all communicating parties understand data elements in the same way.**

Technical interoperability refers to technical aspects of linking information systems. It includes aspects such as interface specifications, interconnection services, data integration services, data presentation and exchange.



EIF Interoperability layers

It is strongly recommended to design the ASDEVEDEX architecture following the Architecture Guidelines for Trans-European Telematics Networks for Administrations, Version 7.1 (IDABC) and the ISA guidelines. The fundamental requirements of this use case specify a decentralised architecture and interoperability between heterogeneous systems.

First, decentralised responsibility that allows Focal Points to organise their national IT backend systems, networks and the technological approach in a way best suited to their practices and legal framework. Decentralised responsibility also means autonomy of the Focal Points to select the architecture of their own IT solutions, service providers, policies and legal framework. On the basis of this principle, Parties of the Treaty maintain their current national systems and connect them to the ASDEVEDEX architecture, which has the main aim of “translating” data from national standards

to the ASDEVEDEX standards. At the same time, the Focal Points' architectural and technological solutions must adhere to ASDEVEDEX interoperability standards, while policies and legal framework must match the Treaty and national asset declaration verification regulations aligned with the Treaty.

Second, the use of a web service model as the key technology for setting up interoperable services based on standard interfaces and protocols that any application, running on any web-enabled infrastructure, can be designed to support.

Third, the guidelines also support reusability of components, which brings economy of scale and shorter implementation time. In the ASDEVEDEX environment this supports both the "reuse" of national systems already implemented, which will be kept unchanged (unless a Focal Point decides to build its system from scratch) and also the ASDEVEDEX components which are reused and adapted from other EU and open source projects mentioned earlier.

Fourth, the guidelines indicate the advantages to opt for a multilateral solution instead of bilateral solutions.

Architectural guidelines tend to choose design leading to a reduction in modification of national IT backend systems, the conversion to ASDEVEDEX standards performed by National Gateways and a system based on the existing and future Parties' of the Treaty full trust in confidentiality, e-Identification and e-Signature.

ASDEVEDEX architecture is also based on the use of multilateral solutions. Interoperability partners should establish a common technical platform for the implementation of the Treaty instead of implementing bilateral arrangements, because this would create the need for maintenance of a multitude of solutions and agreements.

The ASDEVEDEX should rely on the **TOGAF (Open Group Architecture Framework)** guidelines as an architecture development method.

7.2.3.6 ASDEVEDEX Architectural Components

ASDEVEDEX is a multilateral, content agnostic e-delivery infrastructure that uses building blocks from previous large scale projects to develop a single interoperability layer to support cross-border exchange of data for verification of asset declarations among the Parties of the Treaty.

The main components of the ASDEVEDEX architecture are the National Gateways and Connectors, which constitute the e-Delivery infrastructure. Once the Gateways and National Connectors are up and running, they provide the e-Delivery functionalities required to implement the data exchange. **In a nutshell, the main function of the Gateway is to exchange messages with other Gateways, while the National Connector carries out the adaptations required by each Focal Point's corresponding national backend IT system, which in return enables the reading and creation of the messages by a user.**

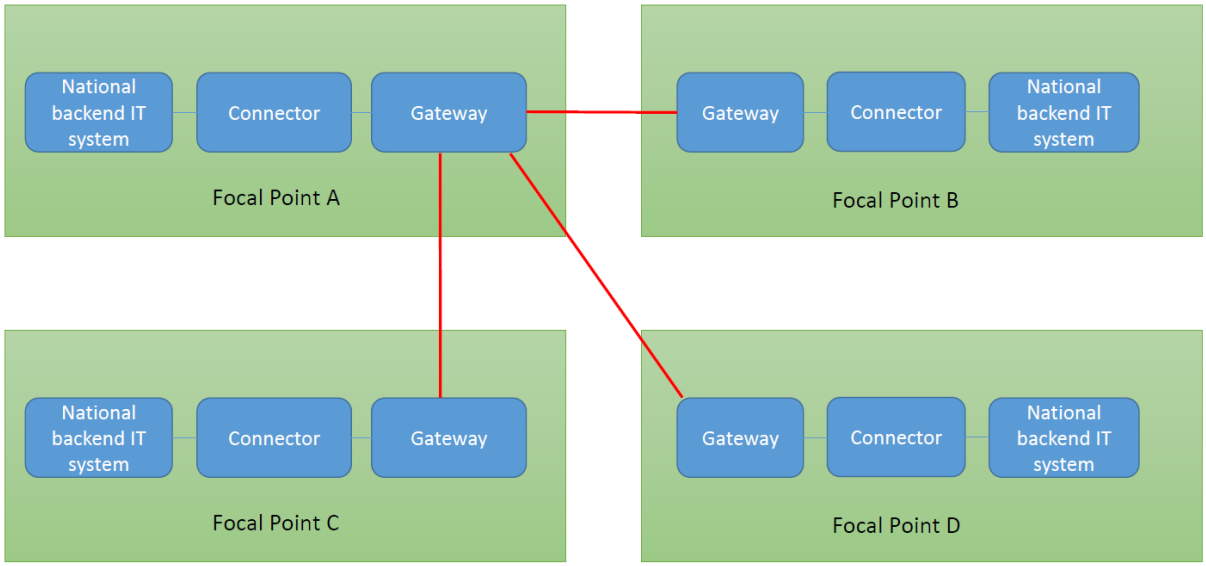
Interface with the e-Delivery infrastructure is provided by a national backend IT system, maintained by the Focal Point of a Party of the Treaty. User interaction is foreseen only in the national backend

IT systems connected to the ASDEVEDEX components. In addition, ASDEVEDEX should develop a default implementation of the Connector framework that works 'out of the box' and without any further adaptations.

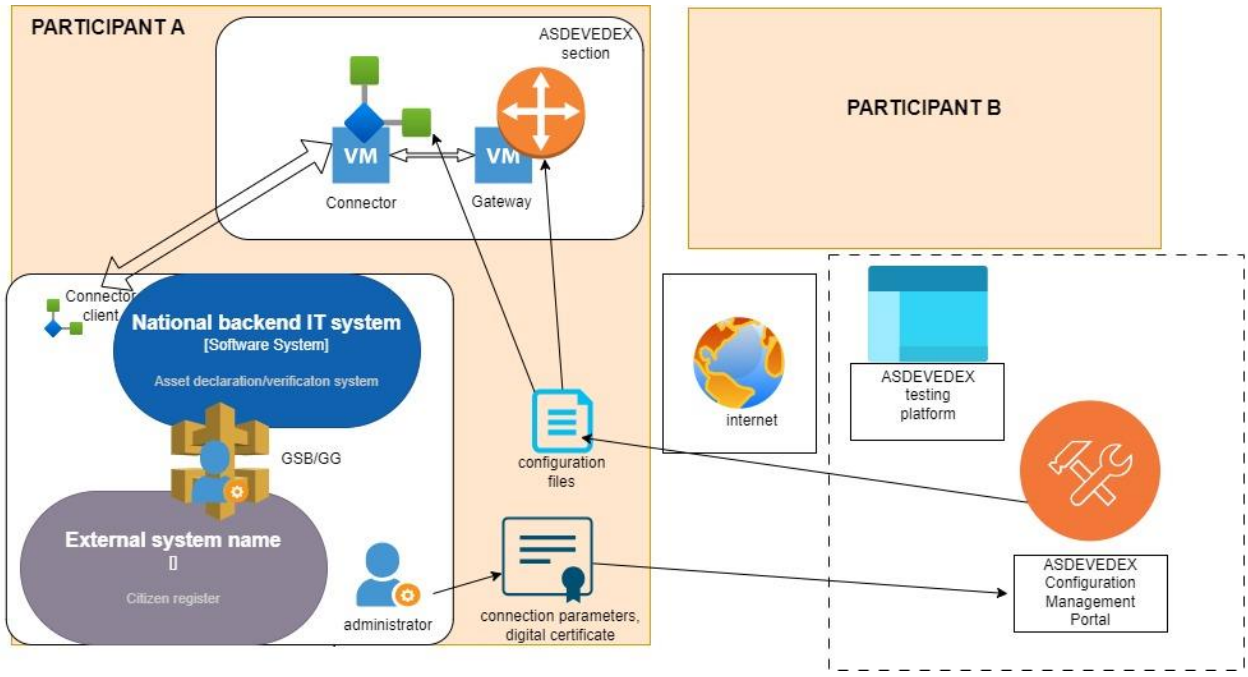
Organisational, legal and semantical issues that arise due to connections between different national asset declaration verification systems are framed by the Treaty and will be further regulated by implementing MoUs/Protocols (hereinafter: Protocols) that will be concluded between Parties of the Treaty. Protocols should provide a mechanism for semantical standardization of data and recognition of information exchanged across borders between Parties of the Treaty.

ASDEVEDEX technological components and its corresponding Protocols will need to change with time in order to adapt to external changes and to improve.

ASDEVEDEX high level architecture overview



ASDEVEDEX High-level architecture overview



High-level overview of ASDEVEDEX components

7.2.3.7 Gateway

The basic functionality of the Gateway is e-Delivery, which is the exchange of messages between Focal Points of the Parties of the Treaty.

The Gateway should perform the following tasks and support the following functionalities:

- Compliance with a set of standards:
  - ebMS 3.0 standard: Gateway interchange messages complying with the ebXML standard. Message transformation will take place at another component: the Connector. The Connector then forwards the content to the Gateway (Web service or JMS interface). The Gateway then creates an ebMS message, which is in ebXML format.
  - Latest version of the standard ETSI-REM TS 102 640-2 for the implementation of messages exchanged between Gateways.
  - Core Components Technical Specification (CCTS) meta models and rules necessary for describing the structure and contents of conceptual and physical/logical data models, process models and information exchange models.
- p-modes configuration[79] to define the way ebXML messages are sent and processed between two Gateways.
- Security: The Security module should sign and encrypt communication between different Gateways.
- Reliability: The Reliability module should implement configuration options for Reliability and Quality of Service (using AS4).

[79] P-Mode parameters are used to set values in the ebMS message header and determine how and where to send the message.

- Logging: the Logging module should enable the administrator to configure log levels and choose the log medium to be used (database or file).
- Web service interfaces: The Backend interface for communications with the national Connector will be implemented in the web service interface. Web service or Java Messaging Service interface will be leveraged for communication between each National Connector and Gateway.

7.2.3.8 National Connector

Each ASDEVEDEX participant of the Treaty must perform some adaptations to the messages sent to other Focal Points and received from other Focal Points. The Connector Framework provided by ASDEVEDEX should be a generic set of modules which aims to provide the common functionality which is needed by every Focal Point. Specific parts of Focal Points' national backend IT systems will need some specific and dedicated implementation using well-defined interfaces.

The Connector framework implements two workflows, one for sending messages from the national backend IT system to the Gateway (outgoing workflow) and the other one for receiving messages from the Gateway and forwarding them to the national backend IT system (incoming workflow).

The Connector consists of a controller that should implement and control the whole workflow between the components. The connection of the Connector to the national backend IT system should be provided by the Party of the Treaty. A small database will be needed for internal use, such as storing message IDs.

The incoming workflow consists of the following steps:

1. The Connector queries pending messages from the Gateway and downloads them.

2. Then the Trust-Ok token of the incoming message is validated and a piece of evidence is created and sent back to the Gateway to inform whether the message has been accepted or rejected. The Trust-OK token is a document in PDF (human readable) and XML (machine readable) format that is included in the ASICs envelope and that indicates the result of Connector’s validation of the sender signature and certificate or information regarding the authentication process of the advanced electronic system used. The result of the validation (trustworthy - not trustworthy) is indicated in the Trust-OK token document. The message is sent independently from the result of validation. The idea behind the Trust-OK token is to provide the possibility for the receiving party (e.g. receiving Focal Point’s authorized officer) to recognise documents that have been filed by using a trustworthy advanced electronic system based on signature or authentication. By using the token in accordance with the adopted MoU/Protocol, the receiving party does not need to validate the signature and the certificate itself. Regardless of the signature assessment by the Trust-OK token, the receiving party still has the right and is granted the means to revalidate the signature independently.

3. Afterwards, the content is transformed (if necessary) to the national format and the message is sent to the national backend IT system.

4. How the Connector checks if the message has been delivered to the national backend IT system is specific to each Focal Point. A timer starts and when it expires with no news from the national backend IT system it considers that the message has not been delivered.

5. The real retrieval of the message by the end recipient is also expected and the result is also sent back as an additional piece of evidence (Retrieval/NonRetrieval) to the Gateway. A second timer analogous to the former is used here.

The outgoing workflow consists of the following steps:

1. The Connector queries the pending messages from the national backend IT system and downloads them.

2. Afterwards the content is transformed (if necessary) to the ASDEVEDEX format based on semantical interoperability documents adopted in the Protocol.

3. The Trust-OK token is created by checking the signed PDF or, in case of an advanced electronic system, by default.

4. The ASiCS container, an electronic envelope containing the form and the attached PDF documents, is also created.

5. A piece of evidence to inform the national backend IT system on the progress of the message is created. In case of errors, evidence of rejection is sent back to the national backend IT system immediately.

6. The National Connector forwards – via the web service – to the Gateway the message content, the ASiCS container and the Evidence. The Gateway collects them and creates the message according to the ebMS 3.0 standard.

7. The National Connector then waits for the acceptance of the message from the Gateway to forward the evidence with the confirmation of acceptance for the national backend IT system. A timer starts and if it expires NonDelivery and NonRetrieval Evidence will be sent to the national backend IT system.

As previously mentioned, a default implementation of the Connector framework should be developed within the ASDEVEDEX project, which works out of the box without any further adaptations. This version should be used by all piloting Parties of the Treaty which do not have any national backend IT system in place to be connected to ASDEVEDEX but still want to participate in ASDEVEDEX, which can be the case for Bosnia and Herzegovina.

7.2.3.9 National backend IT system

A national backend IT system is an application/information system that is maintained by the Focal Point (i.e. the national solution which manages asset declaration and verification which has been adapted to satisfy ASDEVEDEX requirements, or an ad-hoc solution). A national backend IT system must be able to deliver a service in conformity with ASDEVEDEX standards (semantical, technical, security, privacy, etc.) set by the Protocol and be connected to a Gateway through a Connector.

It allows e-filing and reception of documents and data. It can either be an existing application for asset declaration and verification adapted to satisfy ASDEVEDEX requirements or a new application. In order to be able to send/receive messages to/from other Parties of the Treaty, the national backend IT system must be connected to a Gateway through a Connector.

A country can have several Service Providers, as can potentially be the case in Bosnia and Herzegovina.

If the national backend IT system of the Focal Point uses other data structures or XML schemas than the ASDEVEDEX ones, a mapping must be implemented in the National Connector.

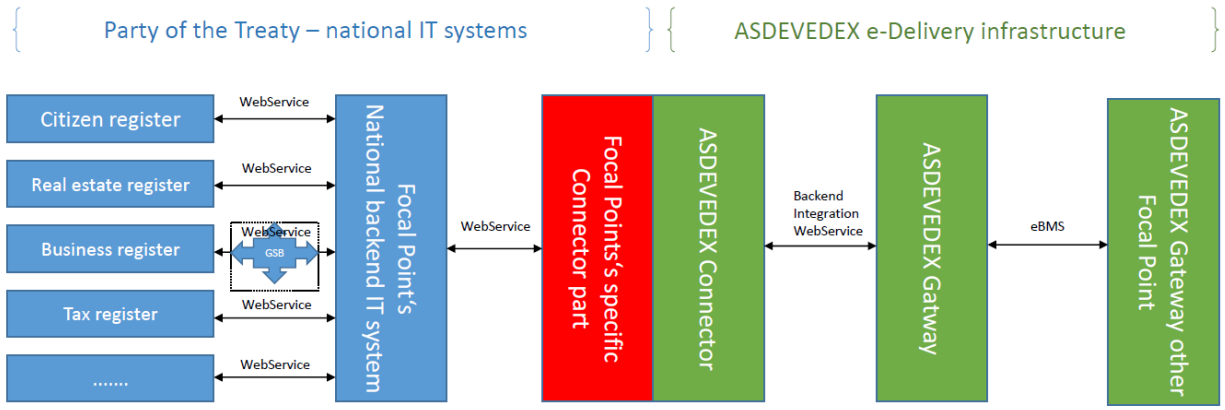
In all cases, the national backend IT system must include support for eSignature or eID solution in accordance with the Protocol.

Its main functions are to create, send and receive documents and data related to verification of asset declarations in accordance with provisions of the Treaty, and allow electronic signing or authentication of the user if an authentication-based advanced electronic system is used. The advanced electronic system can be based on either electronic signature or authentication and must have the following characteristics:

1. The document is uniquely linked to the user;

2. The system is capable of identifying the user;

3. The document is created using means that the user can maintain under his control and any subsequent change of the data is detectable.



Integration of the Focal Point's national solutions into the ASDEVEDEX e-Delivery infrastructure

7.2.3.10 Message structure in ASDEVEDEX

The overall structure of a typical message exchanged between Focal Points in ASDEVEDEX will consist of the following content:

- ebMS messaging envelope: It contains all the necessary information for routing the message, such as original sender and receiver IDs, service, action, conversation ID and also a timestamp.
- ASIC-S Container: It contains all PDF documents (e.g. the signed Main Document and the Trust-OK Token PDF) and also supporting attachments like pictures, etc.. The Trust-OK Token is an intelligible electronic document bearing the results of a legal and technical validation, helping the user to decide whether to accept the document or not.
- XML Schema: It contains the data of the signed Main PDF in an XML Form which can be processed and mapped to national backend IT systems and their needs.
- XML Trust-Ok Token: The Trust-OK Token in an XML Form in order to be able to process the token.
- For non-repudiation purposes, a certain number of evidences should be created for each sent message. ASDEVEDEX should follow the ETSI REM Standard for Evidences in order to identify successful message exchange.

Through the use of a timestamp, the evidence provides information about the different points in time when the message was received at various points (sending Gateway, receiving Gateway, receiving national backend IT system).

For a successful message, four evidences should be generated:

1. SUBMISSION_ACCEPTANCE
2. RELAY_MD_ACCEPTANCE
3. DELIVERY
4. RETRIEVAL

For the receiver of a message, a timestamp will be available in “delivery evidence”. This timestamp from the receiving Party is the one considered to be valid for any legal periods or deadlines relevant for performance of actions in accordance with national regulations.

7.2.3.11 Protocol for legal, organizational, semantical and technical interoperability

Organisational, semantical, legal and technical issues that arise due to connections between different national asset declaration and verification systems will be regulated by the Treaty and implementing Protocol to be signed between the Parties of the Treaty. The Protocol should also provide a mechanism for recognition of information exchanged across borders between Parties of the Treaty.

Protocol and its annexes will be created and adopted to define:

- Mutual recognition of trust services (e-identification, e-signature) between Parties of the Treaty
- Organizational aspects of cooperation of Parties of the Treaty such as ASDEVEDEX governance, minimum service level requirements, release and change management, availability management, incident and problem management including support and escalation procedures, etc.

- Semantical interoperability documents such as data dictionaries, taxonomies, naming conventions, libraries of XML schema documents, etc.
- Technical interoperability aspects of linking information systems including interface specifications, interconnection services, data integration services, data presentation and exchange.
- Minimum technical and organisational measures for personal data protection and preservation of confidentiality, integrity and availability of data and information systems/infrastructure.

When exchanging information across borders, Focal Points in the ASDEVEDEX lack a legal basis to recognise the information exchanged. The Protocol should provide for legal basis by referring to eIDAS implementing acts and MoUs for mutual recognition of trust services between specific WB6 countries to address general and specific conditions for establishing trust and mutual acceptance of national systems. The eIDAS regulation provides for a mutual recognition of e-signatures for national online service offered by or on behalf of a public sector body if the foreign e-signature is of the same security level. The approach could be to establish in the Protocol a mutual recognition of trust service providers and identification providers of Parties of the Treaty for the sole purpose of data exchange in asset declaration verification.

The Protocol should be negotiated in accordance with the provisions of the Treaty. Such a Protocol should then form a firm basis for recognition of information exchanged across borders between Focal Points in ASDEVEDEX. When Focal Points are ready to join the data exchange, they must declare that they comply with the terms of this Protocol. This agreement may become redundant and needs to be amended if a European regulation or other legislation (MoUs of mutual recognition of trust services between WB6 jurisdictions) enters into force.

The concept of the Protocol is simply that if the information is trusted by the Party from which it originates, then it may also be trusted by the receiving Party, subject to certain conditions. The Protocol is understood as the mutual recognition between Parties of the Treaty of electronic data, documents and signatures within the existing legal framework. In order to come under the scope of the Protocol, the document must originate from an advanced electronic system and must be accompanied by a Trust-OK token issued by the Sending Connector, indicating whether the Document is considered as trusted or untrusted in the original country of trust. Both signature-based and authentication-based Advanced Electronic Systems shall be accepted. The specific requirements for electronic documents and the Trust-OK token should be set out in the Protocol and its Annexes.

The establishment of a Protocol shall create the conditions that will allow the Receiving Gateway, upon receipt of a message from the Sending Gateway, to forward the message to the receiving Connector without requesting further authentication from the Sender. The receiving Connector shall process the message in accordance with the laws of the Receiving State. In relation to the sending party, the receiving state shall have no obligation to carry out a verification of the authenticity and integrity of the document(s) but may rely on the information provided by the Trust-OK token.

Traceability and trust is also supported by means of evidences. For each message, each of the Sending Connector and the Receiving Connector shall issue time evidences as it will be further

defined in the Protocol in order to allow the sender and the recipient to identify the points of time that are legally relevant.

Because ASDEVEDEX aims to support electronic data exchange in asset declaration verification procedures with minimal impact on national ICT systems**, it is essential to achieve a shared understanding of the actual transactions and relevant data used by all parties involved in the procedure.** Semantic interoperability aims at ensuring that the precise meaning of the information shared between the Parties of the Treaty is understood and preserved throughout these exchanges. **Therefore it consists of developing a vocabulary to describe data exchanges and ensuring that all communicating parties understand data elements in the same way. It should encompass a dictionary of data retrieved from national registers relevant to asset verification.**

Security and data protection issues are considered very important by Parties of the Treaty. The relevant provisions at the EU level and at the national level have to be respected. This is why the Parties of the Treaty have to make sure that the Protocol envisages the application of all necessary technical and organisational measures to guarantee personal data security and prevent the alteration or loss of, or unauthorised processing of, or access to such data (in particular the authenticity, data confidentiality, traceability, integrity, availability and non-repudiation and security of the messages).

The parties to the Protocol should agree and undertake to use their best efforts to cooperate effectively and in a timely manner to strengthen the functioning of the ASDEVEDEX System. For this purpose, they should appoint Contact Persons (ASDEVEDEX Coordinators) who will be responsible for operational and technical matters related to or in connection with the functioning of the ASDEVEDEX system. ¸

The Protocol should be open for all countries signing or ratifying the Treaty.

It is important to note that the Protocol will be only valid for the purposes of implementation of the Treaty.

7.2.3.12 Process and data modelling for ASDEVEDEX

ASDEVEDEX aims to support electronic data exchange in asset declaration verification procedures with minimal impact on national backend IT systems**, it is essential to achieve a shared understanding of the actual transactions and relevant data used by all parties involved in the procedure.**

Description of the process and data modelling stages in order to enable data exchange at semantical layer is given in the paragraphs to follow.

ASDEVEDEX should follow the ebXML standard to achieve interoperability. Part of the standard is ebBPSS for process analysis. Process analysis requires people involved in handling the cross-border asset declaration verification procedure (in accordance with the Treaty) to participate in describing the process. The basic steps in the process analysis are:

1. Describing the context of the legal procedure (Analysis of the legislative foundation of the cross border asset declaration verification procedure)

2. Scoping of the process

3. Modelling of the process

4. Defining business transactions (Listing the information needed for each transaction to be processed successfully)

5. Reporting on the outcome of the process analysis

As for data modelling, ASDEVEDEX should use a 3-level framework for semantic interoperability. The framework consists of a conceptual model, a logical model and the physical model. Every level of abstraction serves a different objective. Most of all, semantic interoperability serves for alignment of business and IT. The conceptual model will guide and support business and IT to create the foundation for the exchange of information through using previously known and used concepts. For the composition and reusability of concepts, the logical model facilitates the design process by selecting, composing, fine tuning and coding logical elements to use in messages supporting the execution of cross border asset declaration verification procedures. The physical layer is exclusively related to the use case (i.e. exchange of data from the real-estate register).

ASDEVEDEX data exchange will be supported by common electronic business documents in XML format (also called XSDs or XML-Schemas). These schemas will be created after a thorough process modelling exercise. The deployment of these schemas into automated proceeding in national backend IT systems requires mapping between schemas on the ASDEVEDEX layer and the schemas used in national backend IT systems.

Analysing the schemas developed for national formats and procedures should be done by people with combined knowledge of the business procedure, data sets and knowledge of national backend IT systems. A core team of data modellers should be established as the semantical interoperability group in the Regional ASDEVEDEX Interoperability Working Group consisting of representatives from all Focal Points. This body will be responsible for creating, editing, validating and adopting XML schema definitions (XSD). As schemas require maintenance, for instance to reflect a change in legislation, ASDEVEDEX participants should also agree to coordinate updates after new releases of the schemas. These coordinated updates will also allow participants to plan time to amend their mapping and conduct new tests.

Mapping is a transformation[80] process that follows after creation, validation and adoption of XML schema documents. The responsibility for mapping is with the Party of the Treaty. Parties decide when, if and how messages are transformed from the ASDEVEDEX level to the national backend IT systems. As this can be a very time consuming activity, specialists of the Party of the Treaty must be involved in this process as early as possible.

[80] Transforming XML data from one XML format to another XML format.

7.2.3.13 ASDEVEDEX implementation steps for each Focal Point

This chapter entails steps required to join the ASDEVEDEX e-delivery infrastructure and prepare for live data exchange, as follows:

1. Become a partner of the ASDEVEDEX piloting environment in order to get access to the ASDEVEDEX environment to start testing with other Focal Points.

2. Sign the Protocol

3. Set up the Gateway and Connector infrastructure and connect it to its national backend IT system. For the development of the GW and Connector the version control GIT should be used.

4. Development/adaptation/customization of relevant components of the national backend IT system.

5. Conduct tests before going live:

   a. An initial phase of internal tests by developers;

   b. Integration tests of components (Gateway and Connector); business tests of national backend IT systems.

   c. Gateway to Gateway tests and Connector to Connector tests between jurisdictions;

   d. End-to-end tests.

   e. Preparation of documentation for successful test executions

6. Create and maintain the test environment as well as the production environment, i.e. all up and running.

7. Indicate the successful completion of all tests and the documentation of these tests (Quality Assurance) to the Regional ASDEVEDEX Interoperability Working Group.

8. Preparation to go live: install, configure and set up Gateway in a separate production environment and send all necessary information to the Regional ASDEVEDEX Interoperability Working Group.

9. Going live: after providing the necessary configuration files, the new Focal Point is part of the ASDEVEDEX production system. The go live is not necessarily done with all the Parties of the Treaty at the same time. In other words, one Focal Point can continue testing with some Focal Points while being in the production phase with others.

7.2.3.14 Lessons learned from similar data exchange projects in the EU

This chapter lists key lessons learned from similar data exchange projects implemented between EU Member States:

- Create and follow a pilot preparation checklist.
- Focus on starting the pilot with Parties of the Treaty that have a better chance of providing necessary technical preconditions (interoperable national backend IT system)
- Focus on time management and personnel:
    - Assign at least one dedicated person to testing and communication with both external (other Parties of the Treaty) and internal (registries within the jurisdiction connecting to the national asset declaration and verification system).
    - Allow at least two months for testing. No matter how carefully one Party plans its deployment goals, the successful completion of testing highly depends on another Party's time availability.
    - Ensure that proper legal arrangements are made (Protocol for definition of all relevant aspects of legal, organizational, semantic and technical interoperability).
- Use of automatic testing tools, if possible and applicable (a secure website where another Focal Point can request a test message to be automatically sent when needed) for testing the Gateway and Connector.
- Use mutually agreed Schemas & documentation for mapping existing national schemas to ASDEVEDEX (or creating new ones):
- Consult previous end-to-end test files and pre-completed test forms (PDFs accompanied by their respective ASDEVEDEX valid XML files) from Focal Points already in piloting mode during validation process of end-to-end testing.
- Verify the actual practices concerning the off-line procedure, which will be electronically enabled through the use case as they may differ quite broadly from what would be expected reading the law or looking at the experience of other Focal Points.
- Plan local dissemination activities to users well in advance and get direct feedback.
- Not all communication requirements are formally foreseen

Properly managing technological, legal and organisational complexity is the key to success of the project.

7.2.3.15 Information security framework and technical and organizational measures for data protection within ASDEVEDEX

ASDEVEDEX should be a secure system. Security and data protection issues are of particular importance in ASDEVEDEX. The relevant provisions on the network and information security and data protection at the EU level and at the national level have to be respected. Parties must therefore adopt all necessary technical and organisational measures to guarantee personal data security and prevent alteration or loss of, or unauthorised processing of or access to data.

Security by Design

From a technical point of view, ASDEVEDEX should be a transportation mechanism for messages and documents over a network infrastructure. There are different layers relevant for this transportation:

- A network layer provides the basic connection between nodes of the Focal Points.
- A transport layer provides the transport mechanism between those nodes of the network layer.
- A message layer provides the message structure and definition for the messages to be transported via the transport layer.
- A document layer adds documents to the messages of the message layer.

On each of these layers security measures should be applied. The basic approach for ASDEVEDEX should be to rely on well-established and standardised security measures instead of implementing its own proprietary measures. Updated versions of the security components are constantly being provided and just need to be integrated (and tested) in new versions of ASDEVEDEX releases.

Network layer

ASDEVEDEX can be used with different kinds of network layers. It is expected that it will be usually applied on regular Internet connections. Security therefore follows the usual security applications of Internet technology (and is extended by the other layers described below).

For higher security requirements, another network layer could be applied. s-TESTA could also be used as the network for exchange of ASDEVEDEX messages once all jurisdictions in the Western Balkans meet the technical preconditions to use this network. s-TESTA (Secure Trans European Services for Telematics between Administrations) is the European Community's own private, IP-based network dedicated to inter-administrative requirements and providing guaranteed performance levels. s-TESTA has been created to offer a telecommunications interconnection platform that responds to the growing need for secure information exchange between European public administrations.

Transport layer

The transport layer should usually be protected by TLS or mTLS[81]. This is a well-established standard for protecting the transport layer in Internet technologies and applied worldwide on a vast number of services. TLS/mTLS provides for the encryption and authentication of the transport channel. It secures the transportation route between each hub of the transport route. Each hub needs to decrypt (only) the address data to forward the message to the next hub. Before forwarding, each hub encrypts the address data again.

Simple (one-way) TLS is possible and sometime still applied, but two-way-TLS (mTLS) is recommended as it is becoming the current standard of protection for the transport layer.

[81] https://tools.ietf.org/html/rfc5246

Message layer

On the message layer, several standards should be applied by different ASDEVEDEX components:

1. The protocol used for Gateway-to-Gateway transmission (as the message layer) is AS4 which signs and encrypts the messages - depending on the security configuration on the Gateway level.

2. Additional layer of security to the message layer shall be performed using WS-Security for signing and encryption of messages for the web services towards the Gateway and the backend(s). Therefore, a Connector-to-Connector encryption should be applied additionally.

3. Digital certificates should be used for signing and encrypting functionality throughout the ASDEVEDEX systems. Those digital certificates for encryption and signing should be compliant with the X.509 standard. Only certificates that originate from a Certificate Authority listed in the Trusted Services List (TSL) should be accepted.

Document layer

Messages contain documents and attachments. These are packed into a package, called “container”. The container is built according to the ASiC-S standard. The sending Connector signs the ASiC-S container and the signature is validated upon receipt by the receiving Connector.

Access to the ASDEVEDEX configuration

The chapters above indicate how ASDEVEDEX should apply security measures by complying with security standards to the channel from one ASDEVEDEX node[82] to another. However, security breaches do not happen only during message transport. They can also happen when setting up ASDEVEDEX Access Points. The communication between ASDEVEDEX Access Points needs prior configuration. Configuration files contain the addressing data, the applied security policy and other information. They also contain trust stores with the public certificates of all participating ASDEVEDEX Access Points. Such configuration files are created for each Focal Point’s node by a Regional ASDEVEDEX Interoperability Working Group using a Configuration Management Tool. Access to the Configuration Management Tool is provided and restricted to each Focal Point only upon personal and individual request. Administrative access is restricted to the Regional ASDEVEDEX Interoperability Working Group.

Data Protection by Design

It is clear that asset declaration verification data exchange involves transfer of personal data, which is subject to data protection regulations. The GDPR foresees that personal data can be transferred (i.e., processed) if this is based on one of the listed justifications. Further, only personal data that is necessary for serving its purpose needs to be processed (data minimisation). Finally, if personal data is processed, appropriate measures need to be applied to reduce the risk of a privacy breach, with due diligence.

[82] Access point of the Focal Point

ASDEVEDEX should apply such measures as an integral part of its design:

- Encryption should be applied on several layers. Gateway-to-Gateway communication should be done via an encrypted channel and, additionally, Connector-to-Connector communication should also be encrypted for further security. Messages are signed to proof their authenticity.
- Participation in ASDEVEDEX is possible only for mutually acknowledged and authorised Focal Points.
- For the transmission of data, the data needs to be processed. For this processing the data is stored temporarily. Then, after the processing, the data should be automatically deleted. No personal data whatsoever should be stored permanently.
- Temporary storage would be done on the local instances of the ASDEVEDEX Focal Points. By design, there is no central data storage in place as ASDEVEDEX is merely a decentralised, peer-to-peer communication network without any central authority in between.

The high level of various data protection measures in ASDEVEDEX is a good starting point for privacy-compliant data exchange. Still, the final responsibility lies with the Focal Points - operators of national backend IT systems. ASDEVEDEX Focal Points are the data controllers. Therefore, their national backend IT systems and IT infrastructure need to comply with data protection provisions as well. As controllers they have the responsibility to apply further measures on their national instances of ASDEVEDEX Access Points and related systems. Recommendations for technical and operational measures for personal data protection that should be put in place by each Focal Point regarding its backend IT systems and underlying infrastructure are provided in Annex 3.

Still, technical evolution needs to be monitored closely and subsequently adopted into ASDEVEDEX components. The technical environment is changing constantly, and so are the risks of security and privacy breaches. This is a task which does not end at the end of ASDEVEDEX implementation and will need to be taken over by all competent authorities of the Focal Points for the maintenance of such a security- and privacy-designed system.

Finally, it needs to be taken into account that higher security usually comes with a price. Additional security levels do not only demand additional costs (e.g., for qualified certificates). Even more, they result in higher complexity of the system, requiring additional effort and skilled IT professionals to configure, test and maintain the system. Therefore, it needs to be thoroughly considered which security level is appropriate and still efficient for the asset declaration verification data exchange use case.

Annex 1: Questionnaires (provided in the separate file)

Annex 2: List of held interviews

Country	Institution	Type	Tentative meeting schedule
Albania	High Inspectorate of Declaration and Publication of Assets and Conflicts of Interests – Staff responsible for Asset declaration and ICT department National Agency for Information Society (AKSHI)	**On-site**	**5.10.2023**
Bosnia and Herzegovina	Agency for the Prevention of Corruption and Coordination of the Fight against Corruption Central Election Commission of Bosnia and Herzegovina Anticorruption and Quality Management Office of the Sarajevo Canton Civil Service Agency of Bosnia and Herzegovina	**On-site**	**18.09.2023**
Kosovo*	Agency for Prevention of Corruption of Kosovo* – staff responsible for asset declarations and ICT department	**Online**	**19.10.2023**
Moldova	National Integrity Authority of the Republic of Moldova – staff responsible for asset declarations and ICT department	**Online**	**27.10.2023**
Montenegro	Agency for Prevention of Corruption of Montenegro – staff responsible for asset declarations and ICT department Cadastre and State Property Administration	**On-site**	**20.09.2023**
North Macedonia	The State Commission for Prevention of Corruption of North Macedonia – staff responsible for asset declarations and ICT department Personal Data Protection Agency	**On-site**	**4.10.2023**
Serbia	The Agency for prevention of corruption of the Republic of Serbia – staff responsible for asset declarations and ICT department Ministry of Interior	**On-site**	**30.10.2023**

	Central Register of Compulsory Social Insurance Agency for Business Registers Tax Administration Republic Geodesic Authority Central Register of Securities		

Annex 3: Recommendations for technical and operational measures for personal data protection that should be put in place by each Focal Point

Article 32 of the EU GDPR states that taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

This annex contains the list of technical and organizational measures that should be taken in consideration by all involved actors in the asset declaration, verification and data exchange to protect personal data.

Information Security Policies

- Approved security policies aligned to the highest industry standards
  - a policy governing access to data;
  - a policy governing data sharing with third parties; and
  - a process for reporting suspected violations of policies
- At a minimum, annual review of information security policies
- Appropriately detailed data map

Organization of Information Security

- Dedicated information security function responsible for security initiatives and operations
- Designated roles and responsibilities within the security function

Human Resource Security

- Contractually binding confidentiality obligations on all personnel handling confidential and/or personal data
- Security awareness, education and training upon onboarding and at regular intervals
- Background checks for all employees to the extent permitted by applicable laws
- Disciplinary process for policy violations to the extent permitted by internal policy and local applicable law
- Termination or change of employment controls

Asset Management

- Management oversight of assets such as servers, databases and user endpoints
- Assigned ownership for all assets
- Classification and handling of assets

Access Control

- Remote access to the IT systems via VPN tunnels, where appropriate, or other state-of-the-art secure, encrypted connections
- Least privilege and need-to-know basis security concepts embedded into the access management process
- Access authentication program
- Periodic review of access rights (at least annually)
- Access termination within 48 hours for separated users
- Use of multi-factor authentication (MFA) and/or single sign-on (SSO) to access IT systems
- Password complexity and configuration requirements in accordance with best practices and infosec standards

Cryptography

- Encryption of data at rest
- Key management system with applicable security controls

Physical and Environmental Security

- Physical entry controls
- Security of equipment and assets off-premises
- Secure disposal or reuse of equipment
- Appliances for the monitoring of temperature and humidity in data centres
- Redundant power supply units are built into the systems, where appropriate, to help ensure an uninterrupted supply of power to the data centre and storage locations
- Fire/smoke detectors and fire extinguishers or fire suppression system in data centres
- Visitor access and authorization program

Operations Security

- Approved change management process for changes to IT infrastructure and information systems
- An appropriate backup methodology to ensure data integrity and timely restoration of core operational data and systems
- Secure event log preservation
- Annual vulnerability scanning and penetration testing of systems and environment
- Annual audit of system configurations and controls
- Endpoint Detection & Response (EDR) to protect endpoints
- Server and infrastructure components hardening

Communications Security

- Network protection including security intrusion-detection-system, anti-malware software, anti-distributed denial of service software, next-generation firewalls deployed across the environment, etc.
- Segregation of networks into zones

- Network monitoring services in place 24 x 7 x 365 to detect unauthorised activities

System acquisition, development and maintenance

- Secure software development process to enable the creation of software that incorporates security into every phase of the software development life cycle (SDLC). Security is embedded into the code from inception rather than addressed after testing reveals critical product flaws.
- Separation of development and production environments
- Periodic review of open-source and third-party source code libraries
- Static and dynamic scanning of source code.
    - Static scans review the code for vulnerabilities before it is packaged into the front-facing application. These are performed annually to address vulnerabilities in sourced code and compiled applications.
    - Dynamic scans are performed during code changes after the compilation of the code and is to identify run-time errors in the application

Supplier relationships

- Third party risk management program enables ongoing identification, assessment, monitoring and mitigation processes to manage the risks that occur with using vendors, establishing partnerships and outsourcing services.
- Process to respond to regulatory and user requests
- Capability to respond to security and privacy questionnaires from the Focal Point in a reasonable timeframe.
- Vendors/Outsourced partners should possess ISO 27001 or other relevant information security certification for the service provided
- Cloud providers to Focal Points should provide the latest annual 3rd party network and application penetration test summary report

Information security incident management

- Incident management program
- Forensic capability for collecting incident data
- Business Continuity program to ensure redundancy of IT infrastructure and Information systems
- Business Disaster Recovery program to ensure recovery of personnel and infrastructure in the event of a disaster
- Business impact analysis to identify critical systems and processes
- Logging of access and forensic capabilities to preserve logs and evidence for investigations where necessary

REGIONAL
ANTI-CORRUPTION
INITIATIVE

Fra Andjela Zvizdovica 1, B/14
71000 Sarajevo
Bosnia and Herzegovina
Phone: +387 33 296 327/328
E-mail: info@rai-see.org
www.rai-see.org