IPA/2017/039-816/01/ME/Transport - Country Action Programme for Montenegro (2017):
Support to the Transport sector in Montenegro

Contract title: Establishment of a National Maritime Single Window (NWSW)

Identification number: NEAR/TGD/2020/EA-RP/0069

ANNEX 2

Technical Specification of

Data Centre Hardware, Network System Software, Administrator's Workplace, Education Centre, Requirements Of Information Security, Disaster Recovery, Business Continuity, Compliance, Electronic Signature, and Intellectual Property Protection

Funded by the
European Union

Disclaimer

This document was produced with the financial support of the European Union. Its contents are the sole responsibility of Business and Strategies in Europe, S.A. (B&S Europe) and do not necessarily reflect the views of the European Union.

Table of contents

1. Initial assumptions of MSW development

1. No public *cloud* solution is allowed for data storage or servers;
2. As a consequence of the first assumption, no *hybrid* solution is allowed either;
3. As the only exception, *cloud* components may be allowed if it is justified and impossible to use the on-premise solution, if the provider of services has physical resources used for *cloud* service deployment available on the territory of Montenegro, if the development and integration would not be possible without cloud solution, or if the cloud solution for a particular solution is explicitly allowed by this document;
4. The required overall solution is represented by on-premises hardware, system software and network components, constituting a private *cloud* solution under physical and logical control of MSD;
5. The initial technical solution is composed of:
    a. Hardware components;
    b. Network components, and
    c. System software components.

Timeline: Estimated viable project execution timeframe is two (2) years, starting from the project award. This timeframe includes hardware and network installation and system integration, creation of the functional MSW specification and application development services. The hardware, network components and system software should be installed right after the functional specification is created and just prior to rolling out the first MSW module for testing and acceptance, as well as before transporting it to the initial production work (marking the beginning of the exploitation of MSW).

After two years of the creation of the functional specification, installation of hardware, network components and system software and development, the second phase begins and lasts for one (1) year, where the Contractor provides system exploitation and assistance, ensuring uninterrupted system functioning.

System exploitation and assistance, after the rollout of the first functional module and until end of the development of MSW, includes:

1. *Helpdesk services* for the network and system hardware. This includes, but is not limited to system monitoring, patching etc;
2. *Monitoring and adjustment of ongoing correct functioning of the developed modules*. This activity cost refers to e.g. adjustments of the existing system, incorporating legal requirements and ongoing hardware and system software checks, but without changes in modules and functionality.

The proposed layout is vendor-agnostic and does not determine or suggest any technologies, vendors, or their products. Mentioning that the technologies, vendors or products are indicative and not conclusive. The outlined proposal is a conservative, common layout used in the maritime sector for the port, regional and national single windows using *on-premises* private cloud. Required components constitute a minimum of acceptable technical specifications.

2. Indicative MSW architecture

2.1 Basic assumptions

Required layout for on-premises integrated MSW solution is shown in *Figure 1* on the next page. There are four distinctive and separate physical modules, that are instantly identifiable (from left to right):

1. **MSW administrator's office** – physically separated from the hardware and network equipment (noise, EM emissions and cold environment do not allow persons permanently working in data centres). Wi-Fi solution for connectivity is preferred. Office space, heating, cooling, furniture and electrical connections are provided by the Client;
2. **Data centre #1** (location #1) – contains all hardware and network equipment required to operate MSW and the equipment required for staged data backup to hard drives and then tapes. Physically, it is a separated and overseen (e.g. CCTV) small data centre or a part of a larger data centre that accommodates Web service servers, database servers, backup server, and network infrastructure. This has to be connected to the Internet using a separate media data link and a logical tunnel, connecting it to Data centre #2 over the Internet. Data centre space, cooling, furniture and electrical connections are provided by the Client. The physical address of the data centre #1 is Maršala Tita 7, 85000 Bar, Republic of Montenegro.
3. **Data centre #2 (location #2)** – contains a redundant set of hardware and network equipment able to take over MSW functionalities, in case of failure of location #1 caused by any reason. In function and layout similar to location #1, but it does not contain backup server, as data and server backups are executed only in location #1. This has to be connected to the Internet using separate media data link and a tunnel connecting it to Data centre #1. Data centre space, cooling, furniture and electrical connections are provided by the Client. The physical address of the data centre #2 is Montenegro VTMIS centre, Dobra Voda, 85000 Bar, Republic of Montenegro.
4. **Education/presentation centre** – physically separated from other locations, may use existing facilities. It is a location where meetings, nomad work of consultants and third parties and education sessions could be performed. It has to be a networked office environment with an overhead projector, a wireless multifunctional printer/scanner and a group of all-in-one workstations for the stakeholders. Wi-Fi solution for connectivity is required.

Catastrophic failure of a single location (e.g. earthquake, break-in and vandalism, robbery, rogue employee's action, fire or flooding), causes complete system and data loss of a critical national infrastructure that can not be overcome if backup server and tapes reside on the same location. The backup server protects only against logical data deletion, and even then, only in the case that the backups run properly and correctly executed and periodically tested.

Considering that guidelines for EMSW also anticipate the creation of a redundant site as a consequence of the required SLA, and the same is simultaneously a professionally identified requirement, Montenegrin MSW requires two locations in active-active mode.

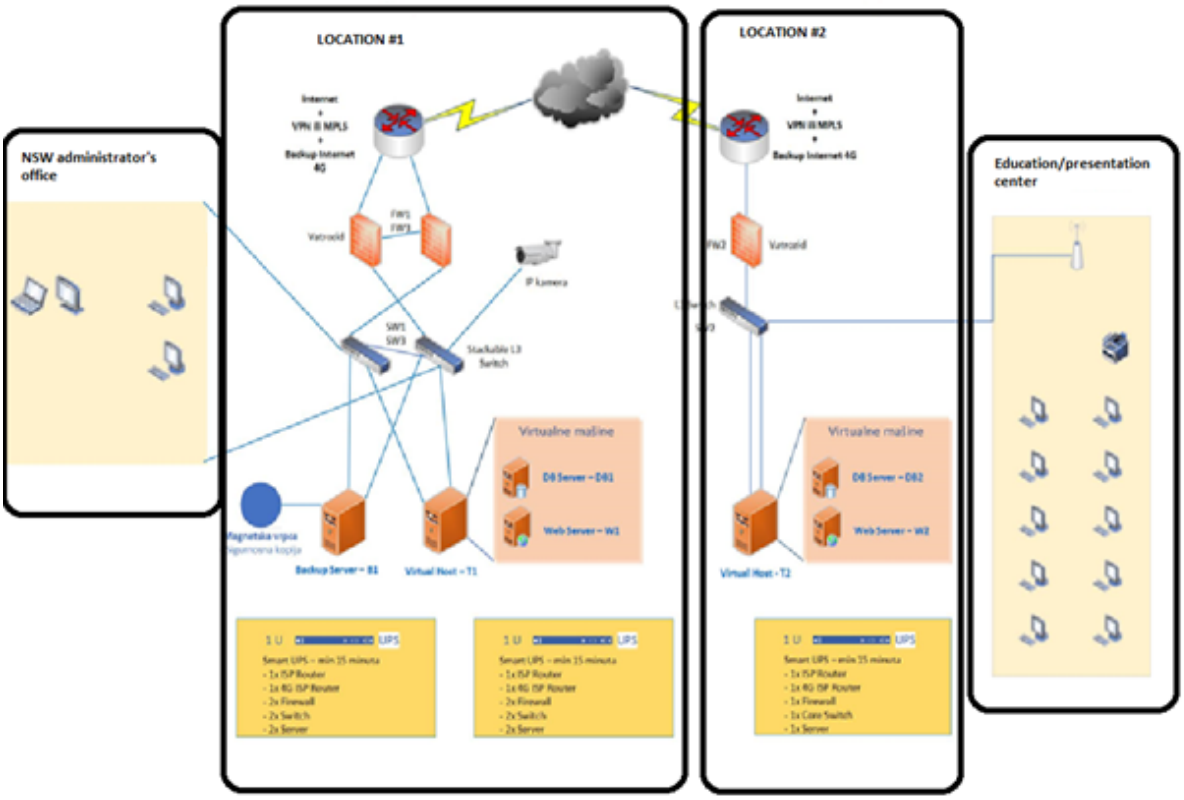

Figure 1: MSW design proposal

MSW will form a part of the *Critical National Infrastructure* after accession to EU, and since *go-live,* it will formally be its part. No MSW setup without two locations under these conditions is acceptable. Other scenarios may include *cloud-cloud* or *on-premises-cloud* solutions, but at least two locations, physical or virtual (and in this case physical), are *de facto* industry standard.

The third location, physical or logical, may be included in the architecture. This location does not have to contain physical hardware (exceptionally, it may be a dedicated *cloud* service), and it could be used as an arbiter to determine which (or both) of the two data centre locations are „up" (alive). This service may have the form of an external load balancer with included required functionality, also may be an already existing part of the state-controlled infrastructure.

Prerequisites for the physical placement are environmentally controlled suitable venue for data centres #1 and #2, following the usual system requirements (oversight, CCTV, physical access control, electricity, cooled environment, temperature indicator, UPS) and they are provided by the Client. One such separate room per location (approx. 12 m2) with access control is provided by the Client. Alternatively, MSW equipment may be joined to already existing racks if sufficient space is available. Two Internet links towards Internet are required (one per each location), and two data centres need to be connected between them using the optical connection and at least 4 x 10 GB aggregated links using a single-mode optical cable.

2.2 Network layout

This chapter describes only very basic concepts and outlines the proposed network layout.

Network architecture requires a pair of devices for UTM (*Unified Threat Management*), combined firewall capabilities in all applicable locations in Active-Passive cluster and full mesh configuration connected internally towards three network switches. This avoids the network's single point of failure in the primary location and ensures HA (*High Availability*). Secondary location requires a single UTM device and a pair of access switches. LAN switches need to have an adequate number of 10 GB SFP ports.

Primary and secondary locations are directly connected using at least 4 x 10 GB aggregated links using a single-mode optical cable. IPSEC tunnel using WAN links could be used as a heartbeat witness for the VSAN cluster.

Both locations require a permanent data link while ISP CPE equipment should have 4G SIM cards for the over-the-air backup or use other physical media for primary link failover. Dynamic OSPF routing protocol throughout the network should be implemented. The primary location has higher priority, therefore does all the traffic routed through it. UTM has configured IP SLA that performs ISP link quality of service and in case of packet loss of higher latency, UTM device does not advertise a default route to OSPF, so it becomes active on the secondary location and all Internet traffic exits on that side, rendering the secondary site as active, without any interruption of the service for the end-users. In the case of primary site recovery, the situation is reverted back. Recovery in both directions must be automatic, without the administrator’s intervention.

Considering that the same network will be used in both locations, the VRRP protocol should be set on core switches. Except for the two physical IP addresses, it should have a single virtual address shared by stacks of the primary and secondary location. Virtual gateway is anticipated in the primary stack location, caused by higher priority.

An indicative layout of a proposed network for primary and secondary locations is shown in Figure 2 on the next page.

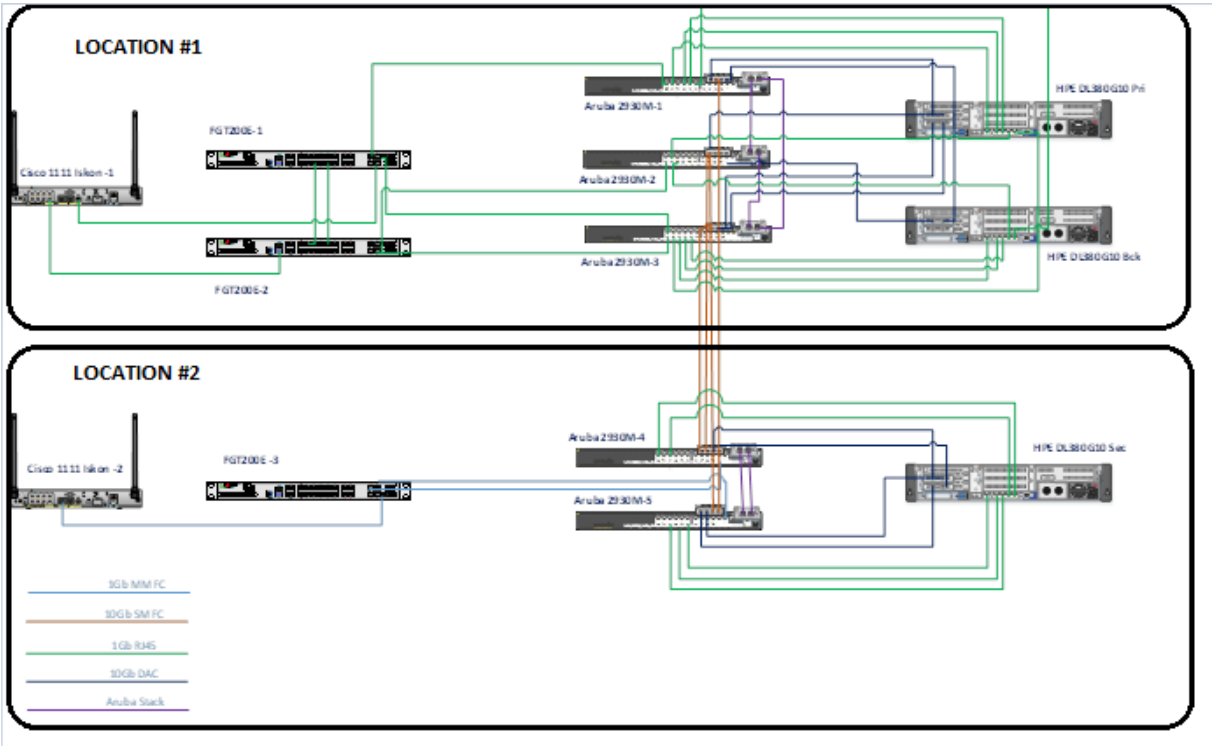

Figure 2: MSW network design proposal

As a part of the project, structural cabling needs to be ensured by the Contractor in both data centre locations, and towards the administrator's workplace and the education centre. It includes, but it is not limited to:

1. ISP cabling of links on both locations (optical connection);
2. Internal UTP cabling of the data centres #1 and #2;
3. The optical connection between data centres #1 and #2, and
4. UTP cabling of the MSW administrator's office and education/presentation centre.

UTP cables need to be CAT 6A, RJ-45 connections, which would be used and tested with report needs to be done using a verifier device (e.g. Fluke MS2-100 tester, or similar). All cables need to be tested for length, wire map capability and 1 Gbps speed. Also, speed and latency need to be tested for the Internet link on both locations and optical links between locations and appropriate sign-off reports created.

Some possible network technology vendors include: *Cisco, Fortinet, Hewlett Packard Enterprise, Aruba,* or *Ubiquity*. The list is not exhaustive or limited.

2.3 Data centres layout

In both locations, a physical server needs to run virtualization capabilities. SAN (*Storage Area Network*) storage/appliance is expected, either in form of a physical SAN or logical (software) SAN. Furthermore, the first location also anticipates an additional physical server for backup purposes. The required backup policy is that newer data and recent changes are offloaded to slower and cheaper local hard drives (repository) connected to the backup server, while according to the retention rules, older data is offloaded for more long-term storage – high capacity tapes. The backup policy has to meet the required SLA.

The administrator should periodically (at least weekly) hand-carry tapes to remote storage away from the primary location, and insert fresh backup tapes, in order to ensure at least 1-week restore capability in case of destruction of the primary or both locations.

Some possible examples of data centre technology vendors for the layout shown in *Figure 3*. may be as follows:

1. Virtualization – *Microsoft (Hyper-V), VMWare, Oracle*;
2. Software-defined SAN – *Starwind, Nutanix, RedHat*;
3. Backup software – *Veeam, Symantec, Microsoft,* and
4. Servers – *Hewlett-Packard, Dell*.

The list is not exhaustive or limited.

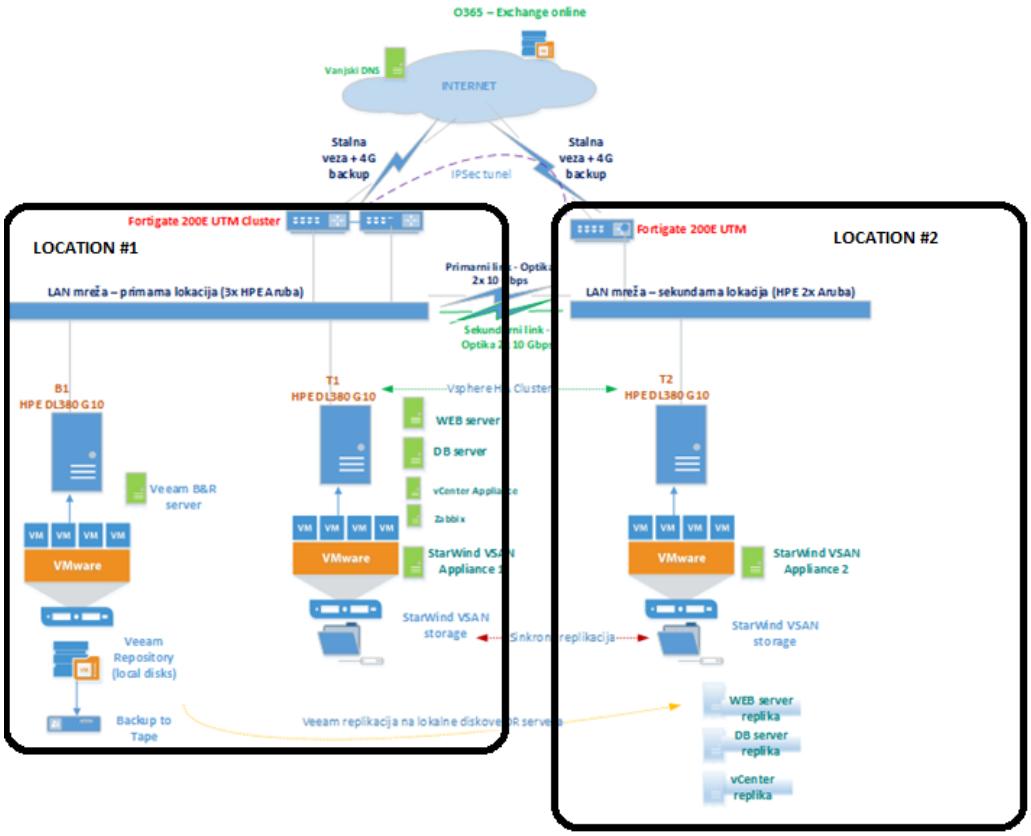

Figure 3: MSW data centres' design requirements

The required layout may be described as the *on-premises private cloud* as it utilizes virtualization technologies in order to achieve scalability, cost savings, and ensure high availability across single and a pair of locations.

Servers in the data centre need to have the adequate capacity (storage, memory, and processing power) in order to support initial and intermediate MSW development. Capacity needs to be dimensioned in order to allow for at least **two separate environments**: test (Quality Assurance/User Acceptance Testing) and production, which need to be strictly divided. The contractor will develop and internally test functionalities in their own development environment, and when they are sufficiently internally tested, they will be transported to QA/UAT environment. After testing, when appropriate modules are tested and functionalities acknowledged by the end-users and/or Technical Assistance (if applicable), they will be transported to a production environment that serves end-customers (stakeholders from the target groups). Appropriate testing procedures and sign off documents according to the usual best practices need to be maintained. The installed capacity of any resource (memory, hard drives, network) also needs to ensure easy scalability and extension when any capacity measure that is systematically overseen reaches 70 %.

Hard drives in local software-defined storage (or separate SAN (if chosen)) need to use an adequate RAID configuration, in order to balance between speed, high availability, and capacity. The same is valid for system and other hard and flash drives in physical servers.

A minimum set of servers for base MSW development and mid-term operations required is:

1. ESXiSRV-T1 or similar physical server (data centre #1);
2. ESXiSRV-T2 or similar physical server (data centre #2);
3. ESXiSRV-B or similar physical server (data centre #1, backup server);
4. vCenter or similar virtualization control server;
5. Microsoft SQL Enterprise or similar database server (ensures encryption of *data-at-rest* and *data-in-transit* and *one-time fee* purchase without additional annual maintenance), and
6. Management server for software-defined SAN (if used).

It is expected that this infrastructure will, within a scope of the project, initially serve a dozen or more virtual servers supporting integral MSW operations. Some of them are enumerated, as follows (the list is not final). Therefore, the Contractor should plan and install the capacities accordingly:

1. Application server;
2. Database server;
3. Web services server;
4. Reporting server;
5. Digital signature server;
6. Software-defined SAN server (if used);
7. Logging server;
8. System server instances (DNS, DHCP, heartbeat), and
9. Other (e-mail – SMTP server etc.).

Most of the servers run on instances in both locations.

Except described top-level required services, this hardware is also used to operate smaller system components required for full functionality as:

1. Anti-virus;
2. Load balancing;
3. Message brokering;
4. PKI (private key) management, and
5. Others.

Data centres may use already existing centralized UPS system, however, one mountable UPS unit per delivered rack is required, that will ensure sufficient enough autonomy in order to gracefully ensure shutdown in case of lack of external power supply. In case of availability of the external fossil fuel-powered generator hooked up to a centralized UPS system, the Contractor will connect delivered MSW hardware and network equipment to the existing fossil fuel-powered generator, as it is a preferred long-term configuration for power supply, in case of operative *Critical National Infrastructure*.

3. MSW development, maintenance, and operations

3.1 Development phase

For purposes of this document, „*development phase*“ is the phase during which the contractor is performing the following activities (the list is not final and depends on the contractor selected technology and methodology):

1. Creating a detailed functional and technical documentation for MSW, including process, document, and data analysis up to the level of the individual data element;
2. Creating final architecture of the hardware and network equipment to be delivered, including system software to be used with them, in order to develop and operate MSW;
3. Creating a detailed parts list for hardware, network and system software to be delivered (Bill of Material);
4. Delivery, installation of the network and data centre hardware;
5. Installation of the supporting system software on the data centre hardware, Development Services („*programming*“) for MSW;
6. Training services for the stakeholders from the target groups;
7. Drafting a related set of project documentation.

This is a minimum required set of activities to be performed within the scope of the MSW development project, for a minimum viable MSW project. All activities need to be performed for a successful MSW roll out to end-users and should be funded, as a part of the underlying contract.

3.2 System exploitation and assistance phase

For purposes of this document, „*system exploitation and assistance phase*“ is the phase during which the Contractor is performing at least the following activities (the list is not final):

1. Monitoring the system for proper operation;
2. Performing security and other patches on the servers and network equipment;
3. Checking logs of the servers, network and all physical and virtual servers including virtualization platform for errors applying remedial actions;
4. Accepting service desk/helpdesk requests from end-users, classifying them according to priority and acting on them to full resolution (examples may range from simple actions like account closing or opening up to more complex issues of troubleshooting);
5. Monitoring accessory systems for proper functioning, both from the technical and administrative viewpoint (examples: 2FA SMS gateway is properly functioning and the contract is valid; external Internet link is functioning and the contract is valid; subscriptions for various hardware and network equipment are ongoing and valid);
6. Verifying backup consistency and performing periodical restore tests with success log signoff;
7. Ensuring that the system, on the whole, is functioning properly in other aspects, and
8. Based on gained experience with the system, identifying improvement opportunities, and escalating them to the MSW governing authority, in order to evaluate whether they are candidates for improvement (*RFE – Requests for Enhancement*) and to budget them timely on behalf of MSD.

A distinctive and separate part of the maintenance and operations is further development. MSW developed according to the initial specifications is not, and will never be a completed system, as there are always numerous expected future changes in the environment, legislation, stakeholders, or project orientation.

Most of these activities need to start and be executed roughly mid-to-late- development phase, and not after the end of the subject contract. For example, as soon as the hardware is installed, all described activities need to be performed by the selected MSW integration services vendor, up until the end of the development.

In order to avoid misunderstandings, many hardware and software components carry with them inherent need to purchase and maintain so-called „*subscription*“, „*maintenance packs*“, „*maintenance service*“ or „*care packs*“. These are software-enabled options that maintain full capability and usability of the system softer, hardware and network components during their exploitation; they are initiated at the moment of the installation. Typically, they need to be renewed annually and carry the financial form of the operative cost. Some examples are:

- Antivirus software definitions for servers – maintenance usually needs to be paid annually after the first year;
- Unified Threat Management firewall network devices – definitions usually need to be renewed annually;
- Servers, physical SAN storage – care packs that enable patching and extend warranty usually need to be renewed annually;
- 2FA SMS gateway – incurred SMS sent for authentication need to be paid, usually purchased in quantity packs;
- The digital signature component could be a one-time fee or an annual subscription;
- Database – in some cases, needs to be paid annually;
- Office 365 for e-mail accounts etc. – usually needs to be paid monthly;
- Other system components like load balancers, integration system software etc. – usually one-time paid and then maintenance is paid annually.

The Contractor shall provide full functionalities or all used database, system software and integration components for the duration of the contract.

3.3 Data centres

3.3.1 Activities to perform – network installation

The Contractor should pass redundant optical cable fibres from ISP equipment to network equipment of the MSW system and minimum STP Cat 6e cable from the switch to MSW administrator's workplace and the education centre.

The Contractor should pass electric cables from the distribution box to the server and network equipment.

The Contractor should perform other civil works required to ensure the functionality of the procured server, network and system software in two locations, and ensure physical and logical security of the equipment used to operate the MSW system.

The Contractor should clean the space after installation and civil works and take care of remaining waste and packaging in an ecologically acceptable manner.

Both data centres need to be connected using a separate data link using optical media having a speed of at least 100/100 Mbps. Two data centres need to be connected using the speed of at least 4 (fibers) x 10 Gbps in link aggregation and using redundant LAN switches in a primary location, so the system function does not rely on a single fiber. In case that all four fibers fail, synchronization between data centres stops working, but the primary location continues serving the clients without interruption including backup in the primary location.

The Contractor should use IPsec tunnel using two Internet links as an additional data connection between locations. The tunnel is always up and active for purposes of SAN or VSAN heartbeat witness. IPsec tunnel should use Internet link tunnels to be redundant.

Redundancy of the Internet links in both data centres needs to be achieved by data connection using different media than the primary one (e.g. 4G over-the-air connection or different physical media link). Failover from the primary to the secondary link should be automatic and without administrator's intervention.

For each data centre, at least two of each public static IPv4 and IPv6 addresses should be provided by the Contractor, one for each firewall and one for each web server, until the end of the contract.

3.3.2 Firewall specifications

Firewalls delivered by the Contractor should have at least the following specifications:

1. Minimum 1x GE RJ45 Management/HA port;
2. Minimum 2x GE RJ45 WAN ports;
3. Minimum 2x GE RJ45 ports;
4. Minimum 4x GE SFP connection;
5. Minimum 1x USB port;
6. Possibility of 4G USB connection;

7. IPv6 support;
8. IPSec VPN between sites (*site-to-site*) capability;
9. Client SSL-VPN connection capability for minimum 200 simultaneous users having a minimum throughput of SSL-VPN connection at 600Mbps;
10. Minimum required services: standard UTM, IPS, Web server protection, antivirus protection, IPv6 support, SSL VPN service, DHCP and DNS services;
11. Entries history minimum 30 days retroactively until the current date;
12. Minimum throughput under IPS load 2 Gbps;
13. Minimum throughput under full load 1 Gbps;
14. Licenses need to cover all required services until the end of the contract;
15. Service should include installation in the rack.

3.3.3 Network switches specification

The network switch is a hardware device providing basic interconnection of all devices in the LAN infrastructure, connects it to the firewall and data link, and should have as a minimum the following technical characteristics:

1. Minimum 20x 10/100/1000 connections (IEEE 802.3, IEEE 802.3u, IEEE 802.3ab);
2. Minimum 4x 10G / 1G SFP+ connections;
3. Switching capacity minimum 200Gbps;
4. Support for IPv4 and IPv6 data traffic;
5. VLAN support;
6. PoE support;
7. Layer 3 protocol support;
8. Managed switch;
9. Service should include installation in the rack.

To connect network devices (ISP router – firewall – switch, multi-fibre optical cables need to be used (multimode). All required equipment to connect them using optical cables needs to be installed in the rack (optical patch panel).

3.3.4 Servers specification

First (T1) and second (T2) servers in data centres need to be physical on-premise servers. Each server needs to be a host for virtual machines running on VMWare vSphere, or similar virtualization platform. VMware vSphere Hypervisor (ESXi) Essentials Plus, or similar software needs to be installed. Minimum technical requirements for the first and second servers T1 and T2 are as follows:

1. Minimum 2x 300GB SAS SSD for installation of the virtualization server software;
2. Minimum 8x 1,8TB SAS SSD to store virtual machines configured in RAID 1+0 system (total storage capacity is minimum (8x1.8 TB)/4;

3. Minimum 2 processors, 12 cores each;
4. Minimum 128 GB RAM;
5. Minimum 4x10 Gbit network cards, at least one of them on a physically separated module inside the same server;
6. Capability to upgrade the server with additional RAM and disk space (internal disk array should have at least 8 slots and the size of the external disk RAID should be at least 16 slots);
7. At least one spare SAS SSD drive capable to replace one previously outlined disk used to store virtual machines with appropriate capacity (minimum 1.8 TB);
8. Minimum 2 (two) Power Supply Units (PSU);
9. Service should include installation in the rack.

For the first server T1, minimum of two physically separated network cards need to be connected to a separate network switch using at least STP CAT 6a cable or similar.

For the second server T2, a minimum of two physically separated network cards needs to be connected to the same network switch using at least STP CAT 6a cable or similar.

The Contractor should deliver complete service of installing and configuring the server and network equipment and installation of the system and driver software, including all consumables and spare material required for rack installation, up to the level of fully functional, integrated system.

3.3.5 Virtualization server specification

Virtualization server (hypervisor) needs to be installed on SSD hard drive with SAS interface and size of at least 300 GB set configured in at least RAID 1. Virtualization server should have at least the following characteristics:

1. Virtual machine encryption;
2. Capability to synchronously replicate virtual machines to the secondary location

Virtual machine storage must be on a separate hard disk array with a minimum capacity of 3 TB.

3.3.6 Virtual machines on the first server specification

3.3.6.1 Web Server - W1

The web server must be installed on a Linux operating system (the latest available production version at the time of configuration) or equivalent that supports a minimum of the two most common web server platforms, such as Apache, nginx, IIS or similar.

User access to the web server, i.e. the content on the webserver (website) must be supported by a license agreement that provides for an unlimited number of users and devices that are able to access the MSW system.

The web server must have at least the following feature:

• Possibility of mirror synchronous replication (mirroring) of all web data to another location.

3.3.6.2 Database Server - DB1

The database server must be installed on a Linux operating system with associated licenses or on an equivalent operating system. The Contractor must use MySQL Enterprise database software with associated licenses or MSSQL database software with associated licenses, or equivalent enabling on the fly encryption and encryption of the static content. Licenses to use the database software must not limit the number of users who will access them or require additional licenses for additional users. The latest

available version of the database software must be used at the time of configuration. The database should follow the „full initial payment“ model, meaning that no annual maintenance or annual payments are allowed after the initial database provision.

The database software must be configured in a way that is not directly accessible from the Internet, i.e. it must be located behind a firewall.

3.3.7 Virtual machines on the second server specification

3.3.7.1 Web Server - W2

Web server W2 is the synchronous replication of Web server W1 from the first location. Its main purpose is to take over the functionality of running the entire MSW system in case the first Web server W1 has an outage for any reason.

User access to the web server, i.e. the content on the webserver (website) must be supported by a license agreement that provides for an unlimited number of users and devices that must access the MSW system.

Additionally, another web server must be directly accessible from the Internet using a name associated with a public IP address intended exclusively for it.

3.3.7.2 Database Server - DB2

A DB2 database server is the synchronous replication of a DB1 database server. Its main purpose is to take over the functionality of running the entire MSW system in case the first database server has an outage for any reason.

The licenses used to operate the system must not limit the number of users who will access the MSW system or require additional licenses for additional users who will use the system's functionality in the future.

It must be possible to install and run additional virtual machines that are not explicitly listed on each physical host if they are needed for testing, upgrading and smooth operation of the MSW system.

3.3.8 Data Backup Server - B1

The backup server must be installed as a physical server and be located in the first datacenter. It must be installed and configured with Veeam Backup & Replication software (Veeam Backup and Replication Enterprise, current production version at the time of configuration) or equivalent software that must be downloaded from the official website of the manufacturer in the production version valid at the time of installation.

Minimum technical specification of the backup server, B1 should be as follows:

- Minimum 1 processor with 12 cores;
- Minimum 96 GB of RAM;
- Minimum 2 x 300GB SAS SSD for operating system installation;
- Minimum 6 x 6TB disks for data backup storage in hot-swap mode and RAID 1 disk configuration;
- Minimum 2 network cards;
- Minimum 2 power connectors;
- Configured magnetic tape device as an additional medium for backing up the minimum capacity without compression 6250GB, plus a minimum of two magnetic tapes of appropriate capacity (Example: HPE LTO-6 Ultrium 6250 tape or equivalent) and one tape for mechanical cleaning of the head of the tape device.

Data backup software must have at least the following features:

- The possibility of backing up virtual machines and returning to the original host or another one;
- The possibility of recovering individual data (documents, application files, etc.);
- The ability to recover an individual Oracle database or Microsoft SQL database type or equivalent;
- The ability to record data on magnetic tape;
- The ability to encrypt the data contained in the backup.

All critical parts of the MSW system must be backed up, in accordance with the standards of required service levels.

4. Other equipment and services

4.1 UPS

Three Smart-UPS devices are required (two in the first, one in the second server room), which could power all network and server devices in the server room under full load for a minimum of 30 minutes.

Smart UPSs must be equipped with network cards that allow autonomous and "clean“/“graceful“ shutdown of all virtual and physical servers and other equipment in the event of a power outage on the external power source that supplies the entire system.

The system must be configured in such a way as to achieve the described server shutdown in the event of a power failure and a test (simulation) of such a scenario must be performed, of which a record must be made.

The supplier must document the procedure and procedure for restarting the system.

The supplier must deliver all installation and consumable materials as well as the service of installation in the server racks and connection to an external power source. All power cables must be properly connected to the device to which they are connected.

4.2 Rack and Patch panels

Both server rooms must be equipped with server cabinets with a minimum size of 42 standard units to install components of the planned system and subsequent system expansions according to the needs and requirements of the customer for further system upgrades. Each server cabinet must be equipped with grounded electricity outlets for all devices that can be placed in the server cabinet. Cabinets must be equipped with a side and rear side, a shelf for the purpose of placing the monitor and a front door with a physical or digitally actuated key.

4.3 Data cables

The optical data connection must be made at least to the network switch in both server rooms. The Contractor must provide a minimum of Category 6a STP cables in those locations for which this is indicated by the professional rules for connecting computer and server equipment to the network equipment of the system.

4.4 DNS

The local (internal) DNS service must be able to associate local (internal) server and device names with the corresponding IP addresses for easier communication and setup. The DNS service must be set up on the firewall or as a separate service on the virtual machine.

The external DNS service must be able to associate public (external) IP addresses with the associated server and device names, and vice versa. The external DNS service could be registered with the third party and included in the service, as well as the rights to access the information and configuration must be retained only by the Client. For high availability, DNS records for external addresses need to be configured with at least two different DNS service providers.

4.5 DHCP

DHCP service is required for devices that will not use static IP addresses and must be able to communicate with the rest of the system. DHCP service can be configured on a firewall, network switch, or as a service on a separate virtual machine.

4.6 Antivirus software

Antivirus software must be installed on each physical and virtual server in the MSW system and each delivered workstation. Antivirus software must have support for Windows and Linux server operating systems. Its management console must be in a cloud environment and must not require an additional server on the local system. Antivirus software licenses must be valid until the end of the contract.

4.7 Mailboxes

A minimum of 10 IMAP and/or Exchange email accounts with a minimum capacity of 5GB per account in a cloud environment (Office365, Google, ZohoMail, or equivalent) must be leased for reporting from various applications, system monitoring and logging work orders, and communication between system administrators. The lease must last until the end of the contract.

4.8 Ticketing system

The ticketing (helpdesk) system could be installed on an additional virtual machine on the Linux operating system or equivalent, or using a public cloud service, which will be accessible regardless of the type of device, sending direct (push) notifications of occurrence and changes per working account. If the system is used and configured on a virtual machine, it is necessary to provide access from the Internet, a public IP address for the server and DNS records for access to the server using a domain name. Data traffic to and from the server must be encrypted, and the web interface secured with a username and password. An example of such a system is the Spiceworks Help Desk, GLPI or equivalent system which is free for commercial use at no extra charge. No software in the commercially paid model should be used.

4.9 Classroom/Test Center

For the needs of the classroom and test centre, the supplier must deliver and configure the following equipment:

1. 8 (eight) computers, each with the following features:

- All-in-One computer model;
- Minimum 23.8 " screen size in FHD resolution;
- Minimum with features of Intel i5-8600U processor, AMD Ryzen 5 2600X, or equivalent;
- Minimum 8GB of RAM;
- Minimum 240GB SSD;
- Minimum 1x 10/100/1000 Ethernet (RJ-45) input;
- Minimum 802.11b/g/n Wi-Fi connectivity;
- USB keyboard + USB mouse.

2. 1 (one) multifunction printing device with the following features:

- Black and white printing, laser technology;
- Multifunction device (printing, copying, scanning, ADF tray);
- Network connectivity (minimum Ethernet (RJ-45) and Wi-Fi 802.11b/g/n).

3. 1 (one) wireless access point with the following features:

- Minimum 1x LAN port 10/100Mbps;
- Minimum 802.3u Ethernet standards;
- Minimum Wi-Fi standards: 802.11a/b/g/n/ac;
- Minimum Wi-Fi speed: 450Mbps;
- Supported protocols: IPv4 and IPv6;
- Ensure connectivity of the Wi-Fi AP device with the switch in another room using a cable of at least STP Cat6 model.

4. 5 (five) mobile smartphones, with the following features:

- Minimum 6.1" display;
- OS Android 10 One UI 2.5 or iOS 14.1;
- Minimum 128 GB memory;
- Camera minimum 12 MP front/10 MP rear;
- Minimum WiFi 802.11b/g/n WiFi;
- Minimum 4G.

5. 5 (five) tablets with the following features:

- Minimum 10,2“ display;
- OS Android 10, One UI 2.5 or iOS;
- Minimum 128 GB memory;
- Camera minimum 8 MP;
- Minimum WiFi 802.11b/g/n WiFi;
- Minimum 4G.

4.10 System administration equipment

4.10.1 Computer equipment for system administration

For system administration purposes, the vendor must deliver and configure the following equipment:

1. 2 (two) desktops, each with the following features:

- All-in-One model;
- Minimum 23.8 " screen size in FHD resolution;
- Minimum with features of i5-8600U processor, AMD Ryzen 5 2600X or equivalent;
- - Minimum 8GB RAM;
- - Minimum 240GB SSD + minimum 500GB HDD;
- Minimum 1x 10/100/1000 Ethernet (RJ-45) input;
- Minimum 802.11b/g/n Wi-Fi connectivity;
- USB keyboard + USB mouse;
- The warranty on the device must be until 31.12.2020.

3. 1 (single) laptop, with the following features:

- Minimum with features of Intel i5-8600U processor, AMD Ryzen 5 2600X or equivalent;

- - Minimum 8GB RAM;
- - Minimum 256GB SSD;
- Minimum 17 " screen in FHD resolution;
- Minimum 1x 10/100/1000 Ethernet;
- Minimum 802.11b/g/n Wi-Fi;
- The warranty on the device must be until 31.12.2020.

4. 1 (one) screen + 1 (one) mouse + 1 (one) keyboard + 1 (one) port replicator for laptop, with the following features:

   - LED technology;
   - Minimum 16: 9 23.8 " screen size in FHD resolution;
   - Minimum 1xDVI, 1xHDMI, 1xDisplay input;
   - Possibility of height adjustment;
   - USB keyboard + USB mouse;
   - Port replicator with at least Ethernet (RJ-45), USB 3.0, HDMI connectors.

4.10.2 Other equipment for office space and system administrators

1. Wi-Fi AP device for wireless internet access (Wi-Fi device previously intended for the classroom and test centre can be used when it is no longer needed there);
2. Printer with laser technology and black and white printing (a printer from the classroom and test centre can be used when it is no longer needed there);
3. Equip each workstation with a minimum of two Ethernet (RJ-45) ports (connected to the main network switch in the first server room with at least STP Cat6e cables);
4. The workspace must be equipped with at least one Smart-UPS power supply system for all devices of the system administrator (minimum 2x desktop computer, 1x laptop, 1x Wi-Fi AP, printer) that can supply power to the devices for at least 15 minutes from the moment of primary power supply interruption.

2 (two) screens + 2 (two) keyboards + 2 (two) mice, one set for each server room with the following features:

- LED technology;
- Minimum 16:9 19 " screen size in FHD resolution;
- Minimum 1xDVI, 1xHDMI, 1xDisplay input;
- Possibility of height adjustment;
- USB keyboard and USB mouse;
- Possibility of placing in the server cabinet on a shelf.

4.11 Application and Operating System Licenses

1. 11 Microsoft Windows 10 Professional licenses with installation service on delivered computers;
2. 11 Libre Office packages, minimum version 6.0 or equivalent with the installation service on delivered computers.

5. MSW system security policy requirements, PKI and IPR

5.1 Mandatory data storage security policy

The Contractor has to design, develop and deliver MSW system respecting the following requirements of data storage security policy:

1. The system platform on which the system runs must ensure high reliability and efficiency through multi-layer architecture (Multi-layer/Multi-tier);
2. The system, hardware and communication components of MSW systems must be designed and integrated so that in case of interruption of some of the system components other system components continue to record changes and transactions, and function independently until the full operational functionality of the system as a whole is restored;
3. The system, hardware and communication components of MSW systems must be designed so that after the re-establishment of the availability of systems or services that have recorded interruptions, there is an automatic exchange of data generated during operation of correct system components and those that have recorded interruptions, as well as within them, without special additional intervention by the system administrator;
4. Within the design of the MSW system, the Contractor must envisage at least double, redundant and location-separated physical platforms of key components of the MSW system, at the level of hardware (software), software (software) and service (Web interface);
5. The data media on which the systems and data of the MSW system are stored must be configured at least in the RAID modes guaranteeing redundancy and system coherency in case of malfunction of a single data media;
6. The Contractor must envisage the creation of user groups in accordance with the common rights of users, and support the gradual (granular) management of user rights at the level of groups and individual users, at least Administrator, Authorized users and Guests/Public access;
7. MSW system must contain three integrated subsystems for monitoring and subsequent review of system operation, in relation to monitoring the internal performance of the system at the level of hardware (hardware), in relation to the exchange of system data and messages with the environment and other systems (software), and in relation to tracking and recording user actions of users;
8. The minimum parameters that the system must record during operation in relation to the internal performance of the system are the power state of the system server, the use of working memory, disk space usage and their occupancy, the state of network connectivity and the use of processor resources and their correctness;
9. At the software level, the MSW system must minimally record events (log files), audit events and access to objects (auditing events), the state of communication with other systems, the state of application processes and related services required for the proper functioning of the MSW system;
10. In addition to the MSW system, the Contractor must supply and install and integrate user monitoring system that monitors and records user actions when using the MSW system, which is an integral part of the MSW system and must not be performed as additional commercial software.
11. The system must also record activities related to the storage, delivery, automatic processing and transmission of data within the MSW system, between its components and during the exchange of data with external systems that use its services (logging, journaling).

12. The system for recording automatic data processing and transmission activities must be adjustable with regard to different levels of recording (in a minimum of two envisaged levels).
13. In relation to all three subsystems, the MSW system must have an integrated ability to report to system administrators in accordance with predefined levels of critical events that trigger the notification process, at least for the levels of hardware, software and initiated or performed user actions.
14. Notifying the administrator of critical events must be done automatically, at least by means of the e-mail.
15. Data stored in MSW system databases including digital content, audio, video, streaming data, text, etc. must be encrypted with AES-128 technology or equivalent professional standard technology of comparable or higher encryption strength, both during storage within the MSW system, transmission and during the exchange of that data via computer and data networks and communication channels.

5.2 Business Continuity Planning (BCP)

The Contractor has to design, develop and deliver MSW system respecting the following requirements of Business Continuity Planning:

1. The MSW system must be designed to be a complete solution for electronic data exchange between all involved stakeholders in a flexible way that is easily adaptable to foreseeable future requirements (e.g. inclusion of a new stakeholder, concessionaire or new customs procedures), which allow continuity of operations and operations MSW system that is the subject of the offer;
2. The design of the MSW system must support the possibility of uninterrupted operation, taking into account the target mode of availability of MSW services 24/7 and the annual availability of all MSW services (SLA - Service Level Agreement) to all involved users of 99.8% of the total time fund in the year;
3. The design of the MSW system must provide for a total allowed annual interruption of service delivery to customers due to unforeseen failures of software and hardware components of the MSW system of 8 hours per year, with each individual unforeseen interruption (RTO - Recovery Time Objective) must not exceed 4 hours;
4. The design of the MSW system must provide for a total duration of preventive (announced) system maintenance of a maximum of 10 hours per year, each individual instance of preventive maintenance may not exceed 4 hours, with one maintenance event allowed in each of the four annual quarters;
5. The design of the MSW system must be such as to allow the greatest temporary data loss in the event of a system component failure within 15 minutes (RPO - Recovery Point Objective);
6. The MSW system must be designed in such a way that in case of planned or unforeseen interruption of service delivery, and immediately after the return of the MSW system to its nominal state, ensure its return to a consistent state, by incorporating data and information generated in other systems during component failure, to achieve consistency of systems and processes and data contained in MSW databases;
7. In case of the need for preventive (announced) maintenance of the system, it must ensure the availability of redundant logical platforms and services at separate physical locations in the possession of the client;

8. Data backup storage must include all data and metadata contained in the MSW system modules and databases required to restore the system to a consistent state in the event of data deletion or other unforeseen catastrophic events;
9. The Contractor must document the MSW system continuity policy within the MSW system documentation regardless of the existence and content of the Client's business continuity policy, and this document must contain at least the following chapters: envisaged bodies (authorities, instances) for continuity policy implementation, primary and secondary location description for data storage and processing, telecommunication (network) architecture between sites, the methodology of data replication between primary and secondary location, required minimum architecture of applications, data and services, minimum technical and organizational requirements for secondary location, and recommendations for implementation, testing and maintenance.
10. The developed policy of the continuity plan of the MSW system must be formally accepted and certified by the Client.

5.3 Disaster Recovery Policies (DR)

The Contractor has to design, develop and deliver MSW system respecting the following requirements of Disaster Recovery:

1. The Contractor must design the backup system of all data received in the MSW system and deliver all hardware, network and software components required for this backup activity;
2. The Contractor must document the disaster recovery policy within the documentation of the MSW system, regardless of the existence and content of the recovery policy of other parts of the Client's information system, and this document must contain at least the following chapters: a list of return service priorities, a return service strategy, and disaster recovery plan testing criteria;
3. The Contractor must perform a test simulation of the return of the MSW system to the nominal condition in accordance with the occurrence of one possible catastrophic event, which is the complete loss of the database from the first physical location, with the return of database contents from backups from hard drives, magnetic tapes or other physical location, on which it must submit to the Client a report in accordance with the prepared documentation of disaster recovery policy, which contains minimum information on the occurrence of events, actions taken and their sequence and the final outcome of system recovery with an indication of system consistency in relation to required Service Level Agreements;
4. The developed disaster recovery policy must be formally accepted and certified by the Client;
5. Data backup must be performed in accordance with the required levels of service availability, with a minimum of using a physical server to back up data, hard drives on which copies of data are stored and then copied to magnetic tapes.

5.4 Compliance requirements

Defining requirements related to professionally required information security rules:

1. The Contractor must design the MSW system in compliance with part of the rules defined by the professional standard ISO/IEC 27002: 2013, at least in relation to the following provisions of the standard: information security architecture, access control security, use of cryptographic techniques and technologies (encryption), application of measures physical security of the system, application of operational security measures (minimum protection against malicious and harmful software, application of measures to manage technological vulnerabilities of MSW systems, the proposal of information security audit plan of MSW systems), application of network and computer communications security measures within MSW systems, the anticipation of the necessary security requirements for the procurement, development and maintenance of MSW systems in relation to suppliers, and managing security incidents that occur during the use of the MSW system;

2. The design and manner of achieving compliance with part of the rules of the standard ISO/IEC 27002: 2013 must be documented within the documentation of the MSW system, which contains at least the chapters described in the previous point of requirements related to compliance with the relevant professional standard;

Defining the required specific functionalities of the system related to the EU General Data Protection Regulation:

1. The Contractor must ensure compliance of the delivered MSW system with at least the EU General Data Protection Regulation (hereinafter EU GDPR 2016/679), the Act on the Implementation of the General Data Protection Regulation (OG 42/2018), regardless of compliance with the said Regulation. other business processes of the Client and compliance of entities and stakeholders involved in the exchange of data with MSW;

2. The delivered MSW system must comply with all requirements of the EU GDPR and related Montenegrin legislation for personal data privacy and information security at the time of delivery of the system;

3. In addition to the implementation of the functionality of software and hardware that ensure compliance with GDPR, the Contractor must document what was done within the system documentation in a separate document dedicated to GDPR compliance;

4. The document dedicated to GDPR compliance must contain a chapter describing the data processing in the MSW system - hereinafter, RoPA (Record of Processing Activity);

5. The minimum content of the document dedicated to GDPR compliance consists of a table of entities, stakeholders, departments or organizational units that perform data processing in accordance with GDPR within the MSW system, function, process name, type of data processing activities, details of data processing with description, who is responsible "processor", whether there is an external "processor" outside the organization, the purpose of processing, the macro purpose of processing, what is the legal purpose of data processing, what category of data is processed, who are the recipients of data processing results, what is the rule of data retention whether the data are in electronic form or in the form of a physical document, which technical and organizational security measures have been applied, and whether the processing is carried out in a third country or international organization, to which and why;

6. The chapter dedicated to RoPA must contain an expert analysis of the risk of impact on privacy for each data processing activity envisaged by it, which is performed within the MSW system;

7. The GDPR compliance document must contain the procedure to be followed in the event of a breach of privacy within the MSW system, or in the event of a privacy incident;
8. The GDPR compliance document must contain a description of the procedures related to the rights of data subjects (including electronic forms, internal documents and various models of response to the request of the subjects whose private data are processed);
9. The Contractor must incorporate standard privacy clauses in accordance with the requirements of the GDPR into the interface of the MSW system presented to users, as well as in other messages including e-mails;
10. Where applicable, the Contractor must incorporate into the MSW interface, as well as other messages including e-mails, standard clauses related to external "processors" of data that are presented to MSW system users as needed;
11. Among the functionalities of the MSW system, the Contractor must include the possibility of creating information privacy notices, and where applicable, data processing consent forms, in accordance with the requirements of the GDPR;
12. The functionality of the MSW system must include the creation, presentation and distribution of information notices to users on the privacy of information, as well as forms of consent to data processing, in accordance with the GDPR;
13. The design of the MSW system must include functionalities by which the system administrator can achieve the fulfilment of the fundamental privacy rights of users provided by the GDPR, namely the right of access, correction, right to forget (delete) and right to transfer (transfer) private data, including submission and processing requests for the stated rights, by using predefined functionalities from the graphical interface and not by additional queries and processing over the contained data;
14. Functionalities related to achieving basic GDPR rights of users and the possibility of their transfer to the administrator must be performed simply, by inquiry or action of protection of rights in relation to a person, persons or types of data processing in accordance with documented RoPA, automatically, without the need for additional refinements and system queries. professional methods of connection and export from databases;
15. The system must support the export of private data to a minimum of CSV (Comma Separated Value), TSV (Tab Separated Value), XML, XLS, DOCX and PDF formats.

5.5 Public key system and electronic signature

The Contractor has to design, develop and deliver MSW system respecting the following requirements for a public key system and electronic signature:

1. System login and public key infrastructure connection (PKI infrastructure) must support two-factor login (authentication) via username and password and additional security modules, such as hardware security modules (HSM), smart cards (Smart Cards), software modules (Soft Tokens), SMS, e-mail, or equivalent technology solutions that do not require additional payments for end-users;

2. The use of an electronic signature solution in the *cloud* is only acceptable for use on portable devices that cannot be connected to and use hardware security modules (eg tablets, smartphones and similar access devices). For electronic signatures using computers that can be connected to and used in connection with hardware security modules (eg laptops, desktops and similar access devices), physical devices must be used to authenticate the user when using the electronic signature. In the event that the user of the MSW system already uses a physical device to use an electronic signature that can be used for the purposes provided by the MSW system, he must be able to support such devices without the need to add a new physical device;

3. The MSW system must provide access to data and services only to those entities that are authorized to process such data and authorizations are granted by the system administrator;

4. The system must be designed so that access to the administrator account is assigned by the super administrator and the activities of the administrator account are recorded in separate access and action log;

5. The system must allow verification of the level of access to the subject (authentication) in accordance with the verifiable identity of the subject trying to access;

6. The system must be designed in such a way that information is not disclosed to unauthorized entities, which must be achieved using professionally standard technologies, such as SSL (Secure Socket Layer) or equivalent protocol and HTTPS or equivalent protocol;

7. The MSW system must be harmonized with all legal regulations governing the electronic delivery of documents to state administration bodies;

8. All documents exchanged, processed or stored in the MSW system must be treated in accordance with the rules relating to the electronic document or electronic document, and this division of used documents on the day of delivery must be documented by the Contractor within the delivered written system documentation;

9. The MSW system must enable the verification of documents by means of an electronic signature, which replaces in one the stamp and the handwritten signature, both in relation to electronic documents and in relation to electronic documents;

10. The MSW system must provide for the possibility that in case the signature only identifies the author of a document and does not produce other legal effects, the use of electronic signature can be replaced by using a user login system, with adequate information security measures to ensure integrity, confidentiality and availability of data on the person who used the appropriate computer system, i.e. application of best practices of information security, and especially related to the preservation of computer system access logs, ie logs of receiving and exchanging documents via MSW system, as well as other applicable access logs;

11. The option from the previous requirement of the technical specification must be performed as a selection option for a particular group of users or an individual user by the MSW system administrator;
12. The options from the previous two points of the technical specification must be documented on the day of delivery within the delivered written system documentation;
13. All documents exchanged through the MSW system must have traceability of receipt within the system and support the sending of feedback to the sender on receipt (or delivery status) of the document, and provide electronic records of letters received in accordance with this Regulation;
14. The system must support sending notifications to the sender about the incorrect expected document format or incorrect electronic signature, in case this is the case, and sending a link to the stakeholder's server with instructions related to the correct expected electronic document format and, if applicable, rules and methods for the correct use of an electronic signature;
15. The system must ensure that the time of receipt of the electronically signed message and other legally prescribed data is recorded in the access logs;
16. The system must ensure the verification of the signatures of service providers from EU countries in accordance with the Electronic Signature Act.

5.6 Protection of intellectual property, design and delivery of program source code to the Client

The Contractor has to design, develop and deliver MSW system respecting the following requirements for the protection of intellectual property, design and delivery of program source code to the Client:

1. The Contractor must provide the Client with a license for access, use and finishing of the MSW system, including all innovations, design, trademarks and trademarks created during the development of the MSW, which are necessary for the smooth and complete use of the MSW system;
2. The Contractor must guarantee to the Client that the MSW system does not violate and will not violate the intellectual property rights of any third party during the handover in its delivered, installed, tested and accepted condition, its use, as well as copying of software and materials procured by the Client. and to obtain at its own expense all necessary written contracts, consents and transfer of ownership from its employees or other participants whose services were used in the development of the MSW system;
3. The license from the previous point of the technical specification must be non-exclusive (non-exclusive), irrevocable, must be valid for the territory of the Republic of Montenegro, and the price of its use is considered fully paid under the contract without additional costs for the Client;
4. The license for the delivered MSW system must allow the unlimited operational use of the MSW software package on all computers and other devices of the Client and stakeholders for which it is developed or may need to use it;
5. The MSW license must give the Client the right to further develop, decompile, integrate and combine with other software, by the Client and its suppliers, including implementation by other interested stakeholders;
6. In addition to the license, the Contractor must deliver to the Client in digital form all program code is not obfuscated form generated during the development of MSW system, including drawings, database design and tables, flowcharts, metadata and schematics, system architecture documentation, user and administrator documentation, user accounts, passwords, and other information necessary for the smooth and complete use of the MSW system.