
# ESTABLISHMENT AND MAINTENANCE OF THE PUBLIC WARING SYSTEM ABS+

PURCHASE IDENTIFICATION NUMBER:XX2021/XXX

# TEHNICAL SPECIFICATION

5 December 2020

Riga

This document was developed by Corporate Consulting ("Performer") in accordance with the requirements of the agreement "Study on Early Warning Systems Based on Telecommunications Technologies, ECHO/SUB/2019/TRACK1/808194".



### *Authors of the document*

Anastasija Ludženiece, Ivars Solovjovs

### *Changes*

| Date | Version | Description |
|---|---|---|
| 07.12.2020. | 0.5 | Original version of the document |
| 21.12.2020 | 1.0 | The final version of the document, based on the comments received |

# CONTENT

# 1 INTRODUCTION

## 1.1 CONTEXT AND PURPOSE

This document is an annex to the documentation of procurement "Establishment and maintenance of the public warning system ABS +" (procurement identification numberxx2021/xxx (hereinafter "Procurement").

Article 110 of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 on the establishment of the European Electronic Communications Code states that "By 21 June 2022, Member States shall ensure that, when public warning systems regarding imminent or developing major emergencies and disasters are in place, public warnings are transmitted by providers of mobile number-based interpersonal communications services to the end-users concerned".

Meeting the requirements of the Directive in Latvia sets up a public warning system "Early warning system plus" (ABS +), which is intended to warn the public as well as the early identification, assessment and prevention of threats.

The purpose of this procurement is to ensure compliance with the requirements of the Directive by establishing the information system "Early Warning System Plus" (hereinafter referred to as "the System, ABS +").

The System manager and main user will be the State Fire and Rescue Service of Latvia (hereinafter - SFRS). The System owner, the procurer and the party that will sign the contract is the Information Center of the Ministry of the Interior (hereinafter - MoI IC, the Customer).

The purpose of the document is to determine the requirements of the System and the services related to its establishment, which define the scope of the Procurement and are part of the Agreement for the establishment and maintenance of the System.

## 1.2 PROCUREMENT OBJECT

The object of the procurement is **the establishment and maintenance of the public warning system ABS +** in accordance with the requirements laid down in this technical specification.

## 1.3 USE OF THIS DOCUMENT

The requirements described in this technical specification define the functional and non-functional requirements of ABS + and define the scope of services associated with the establishment of ABS +.

The requirements determine the essential characteristics of the System to be developed and the main conditions for the provision of services. It is expected that the Applicant will offer solutions in the tender, as well as during the implementation of the project, which best ensure the achievement of the objective of the respective requirement.

The determining criteria in the fulfillment of a requirement is the achievement of the objective of the respective requirement. In the event of contradictions, the requirements of the Procurement are prevailing.

Each requirement has the following structure:

- **Requirement number**: is the three-digit number indicating the serial number of the specific requirement in the technical specification. The index numbering is arranged in ascending order starting with 001 and allows for the easy identification of each specific requirement defined in the technical specification, with a aim to facilitate reading and quicken orientation of the technical specification (quick finding the specific requirement, linking the technical specification to the regulation, etc.).
- **Requirement name**: is the heading of a specific requirement that provides information on the content of the requirement. All requirements are listed in the "Requirements Index" at the end of the document;
- **Description of the requirement** - is a description of the specific executable requirement, which is sufficiently detailed to allow the Customer to assess the compliance of the Tenderer's technical offer and the system supplied by the Contractor with the objectives and tasks of the tender regulations, in turn for the Contractor (Applicant) to determine the complexity of the implementation of the requirements, thus forecasting the required workload for the implementation of the requirements and technical specification overall.
- **Priority of the requirement** — Priority of the implementation of the relevant requirement according to the following scale:

| | |
|---|---|
| **Mandatory** | The minimum requirements must be implemented during the 1st phase of the System implementation. The Customer reserves the right to reject those tender applications which will not ensure the fulfillment of the minimum requirements. |
| **Optional** | The optional requirements may not be included in the scope of the tender; however, their implementation will be considered as added value and the Tenderer may include a proposal for its implementation in the tender.<br>The implementation of System requirements must be compatible with the Optional requirements for the development of the System in perspective. The implementation of System minimum requirements must not conflict with the optional System requirements. The requirements of the System must be implemented in such a way that in the future it is not necessary to perform complete System rebuilding. |
| **Future** | The implementation of future requirements is not envisaged within the framework of this procurement. They must be taken into account, as they are planned to be implemented in the next phases of the System development. The System must be designed and developed in such a way that, in order to meet future requirements, the System's existing software could be modified as little as possible. |
| **Informative** | Might describe, for example, the expected approach or load and complexity to use the System. This information should be taken into account when planning the architecture of the system and the technologies to be used, but validation of this requirement is not intended at the time of acceptance of the System. |

If the requirement does not have the specified priority, this requirement shall be perceived as **Mandatory.**

## 1.4 RELATION WITH OTHER DOCUMENTS

**Table 1. Relation with other documents.**

| No. | Document Name | Date |
|---|---|---|
| [1] | ABS + architecture description and implementation plan | 07.12.2020. |
| [2] | Evaluation of ABS + technological solutions | 15.10.2020. |

## 1.5 DEFINITIONS AND ACRONYMS

**Table 2. Definitions and acronyms.**

| Term, abbreviation | Explanation |
|---|---|
| ABS + | "Early warning system plus" (*latvian - "Agrīnās brīdināšanas sistēma plus"*). Information system ensuring public warnings in Latvia |
| HTML | Hypertext Markup Language is the standard markup language designed for documents and other information to be displayed in a web browser |
| Procurement | Purchase "Establishment and maintenance of the public warning system ABS +", identification number -xx2021/xxx |
| ICT | Information and communication technologies |
| IS | Information system |
| IT | Information technologies |
| Supplier | Company that as a result of the Procurement has entered into an agreement on the establishment and maintenance of ABS + |
| The Applicant | The company that has submitted a tender in the Procurement |
| Emergency event | An event in which the public needs emergency assistance from the state (operational services). Emergency events may vary in impact on the general public. In the event of an emergency event with a significant impact on public safety, the State warns the public about the emergency event and the necessary action. |
| Exceptional situation | A special legal regime during which the Cabinet of Ministers has the right to restrict the rights and freedoms of state administration and local government institutions, natural and legal persons, as well as to impose additional obligations on them in accordance with the procedures and to the extent specified by law. Law "On Emergency Situation and State of Exception" |
| Warning | Information on the emergency event and the necessary action |
| CAP | Common Alerting Protocol |
| CPDML | Civil Protection and Disaster Management Law CPDML |
| CB | Cell Broadcasting (English-*Cell broadcast*) |
| CBC | *Cell Broadcast Center*. Part of the PWS solution integrated with mobile operator mobile communications equipment providing warning messages |
| CBE | *Cell Broadcast Entity*. Part of the PWS solution enabling dispatchers to prepare warning messages and initiate their transmission |
| Directive | Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code |
| EEN | European Emergency *Number Association* |
| ECM | Electronic Communications Merchant |
| ETSI | European Telecommunications Standards Institute |
| MoI | Ministry of the Interior |

| Term, abbreviation | Explanation |
|---|---|
| GUI | Graphical User Interface |
| GDPR | General Data Protection Regulation |
| MoI IC | The Information Centre of the Ministry of the Interior |
| LB-SMS | Location-based text message (*Location-based SMS*) |
| LEGMC | State limited Liability Company "Latvian Environment, Geology and Meteorology Centre" |
| LMT | SIA "Latvijas Mobilais telefons" |
| MBS | Mobile base station |
| Regulation No. 440 | Republic of Latvia Cabinet Regulation No. 440 Adopted 8 August 2017 "Procedures for Establishing, Operating and Financing the National Early Warning System" |
| MNO | Mobile network operator |
| OTT | *Over-the-top* |
| OMD | Operational Management Division of SFRS |
| PMECN | Public mobile electronic communications network |
| Project | Scope of the "Study on Early Warning Systems Based on Telecommunications Technologies, ECHO/SUB/2019/TRACK1/808194" |
| PWS | Public warning system. A set of procedures and solutions enabling public authorities to warn the public to direct or threatening emergency situations and disasters through a variety of communication channels, including mobile facilities, web solutions (social networks, etc.), radio, television, sirens, specialized communication equipment, etc. |
| System | Public warning system ABS + |
| SLA | Service Level Agreement, Service Quality Indicators agreed by the Parties before the service is provided/received |
| PUC | Public Utilities Commission |
| SASL | State Administration Structure Law |
| SFRS, Customer | State Fire and Rescue Service |

# 2 SYSTEM OVERVIEW

Objectives of setting up the public warning system ABS + (System):

- To provide an opportunity for State institutions to warn the public about direct or imminent emergency events and disasters on mobile phones
- To provide support to the responsible State institutions in connection with the threats to the society, to ensure timely notification of public in the area of their responsibility.

The ABS + is planned to be implemented gradually in several phases:

- Phase 1: provide public warning through mobile communication equipment based on cell broadcasting technology (ensuring compliance with the requirements of the Directive);
- For future phases[1]: providing additional functionality (use of other warning channels, threat identification and notification support, integration with other warning systems, etc.).

This procurement is about 1st phase implementation of the ABS +.

## 2.1 BASIC PRINCIPLES

According to industry standards, the public warning solutions consists of two parts:

- CBC (*Cell Broadcast Center*), a part of the solution, which is integrated with the mobile communication equipment of mobile operators and which provides the transmission of warning messages;
- CBE (*Cell Broadcast Entity*) - the part of the solution that provides the possibility for SFRS dispatchers or other authorized users to prepare, confirm warning messages, send messages, monitor the status / results of messages sent, etc.

ABS + shall be developed on the basis of the following principles, which determine the general approach to the development of the System and shall be taken into account when preparing tender offers.

### *P1: Use of Cell Broadcast technology*

The public warning using mobile communication devices in Latvia is going to be created primarily by using Cell Broadcast technology. The proposed solution must be expandable in the future with the LB-SMS option, but it is outside the scope of this Procurement.

### *P2: Centralized CBC architecture*

ABS + is designed according to the centralized CBC architecture, that is - one CBC node is created, which is connected to the RAN equipment of mobile network operators (Figure 1).

[1]ABS + future development planning is outside the scope of this work and is not reflected in this document.

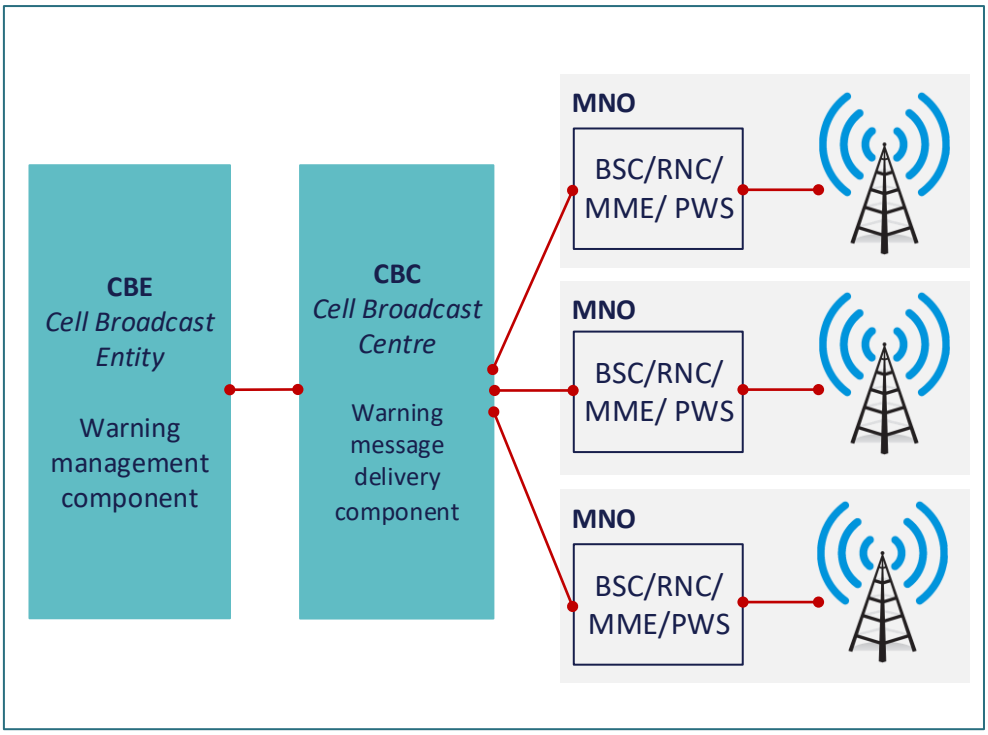


**Figure 1. General System Architecture.**

***P3: Unified procurement of CBC-CBC software, operation of the System is Customer's responsibility***

Both CBE and the CBC are purchased as a single, integrated solution, avoiding the risks of CBE-CBC integration.

In order to minimize the risks of accessibility, availability and other risks, software (**perpetual licenses**) as well as implementation and maintenance services are purchased within the framework of this procurement. The infrastructure necessary for the operation of the System is provided by the Customer in the data centers already at its disposal.

***P4: System development opportunities outside the scope of the procurement***

The Applicant's offered solution must provide an opportunity to provide important functional opportunities in the future without significant changes to the System, which are outside the scope of this procurement, including:

- **Ability to send warning messages through multiple channels.** The public warning system must be designed with the possibility to add other delivery channels in the future, such as sirens, mobile applications, social communication options, etc.
- **Integration with other State authorities**. When developing ABS +, it should be possible for other reporting authorities to prepare information not only in the ABS + system, but also to send warning messages directly from their information systems to ABS +.
- **Public portal**. The possibility for warning message recipients to obtain additional information about the emergency situation and CB activities on a dedicated website (portal).

- **Application not only in case of emergency**. Potentially ABS + could be used not only in emergency situations but also in other situations of public interest (e.g., searching for missing children).

***P5: ABS + manager - SFRS, ABS + owner - Information Centre of the Ministry of Interior***

The following roles are identified in relation to the ABS +:

- SFRS — ABS + manager:
  - define the requirements of ABS +, participate in the implementation of the System, accept the deliverables and System implementation as a whole;
  - directs necessary legislative amendments, justifying the need for ABS +;
  - directs national cooperation with MNO in the implementation of ABS +, determining the expected SLA with MNO;
  - plans ABS + functional development, adding new notification channels to ABS +;
  - as user - prepares, approves and sends public warning messages using ABS +;
  - authorizes user rights for ABS + users;
  - ensures the attraction of funding for the development, implementation and operation of ABS +.
- The Information Centre of the Ministry of the Interior - ABS + owner:
  - responsible for ABS + funding process management and project implementation documentation;
  - performs ABS + procurement, enters into an agreement on the implementation and maintenance of ABS +;
  - manages the ABS + deployment project, coordinates the involvement of the involved parties (MNO, ABS + Supplier, SFRS, etc.);
  - provides the necessary infrastructure for operating ABS +;
  - provides CBE/CBC connection with MNO networks;
  - monitors the fulfillment of MNO services according to SLA;
  - ensure that ABS + is up and running (administration, monitoring, etc.);
  - plans technical development of ABS +, integrations, architecture of public warning systems.

## 2.2 SYSTEM USERS

ABS + users according to the intended ABS + procurement are:

- SFRS OMD – ensured the creation, processing and transmission of warning messages using the ABS + CBE component.
- SFRS management – ensured access to ABS + operational and historical activity reports.
- MoI IC IT administrators - provide technical support for ABS + operations.

The development of ABS + (e.g., integration with 112 platform and LEGMC system, adding new warning channels) may in addition lead to necessity to add new users according to functional scenarios, such as rescue managers, therefore it must be possible to add new users and user groups in ABS + in the future.

## 2.3 FUNCTIONAL UNITS

Figure 2 contains the logical architecture of the System to be created (functional blocks).

The ABS + solution consists of two main parts:

- CBE (Cell Broadcast Entity) - ABS + part enabling SFRS dispatchers or other authorized users to prepare, confirm warning messages, send messages, monitor the status/results of sending messages, etc.
- CBC (Cell Broadcast Center) - ABS + part that is integrated with MNO mobile communications equipment and supports warning message transmission.

In order to introduce the functionality of determining the density of mobile device users in the emergency event impact area, which requires the registration of user devices (*passive geolocation*) at the base station, a necessary MNO component also should be provided.

The System should ensure the following main functional blocks (they may not be the same with the modules of the specific solution and are used to group functional requirements):

- **CBE**
  - E1. Message creation;
  - E2. Message approval;
  - E3. Message sending;
  - E4. Monitoring and reports;
  - E5. Administration;
  - E6. Notification channel gateway;
  - E7. Incoming message gateway;
  - E8. Public portal;
- **CBC**
  - C1. Message processing;
  - C2. Accounting;
  - C4. Area processing;
  - C4. Interfaces with mobile devices (RAN);
  - C5. Administration.

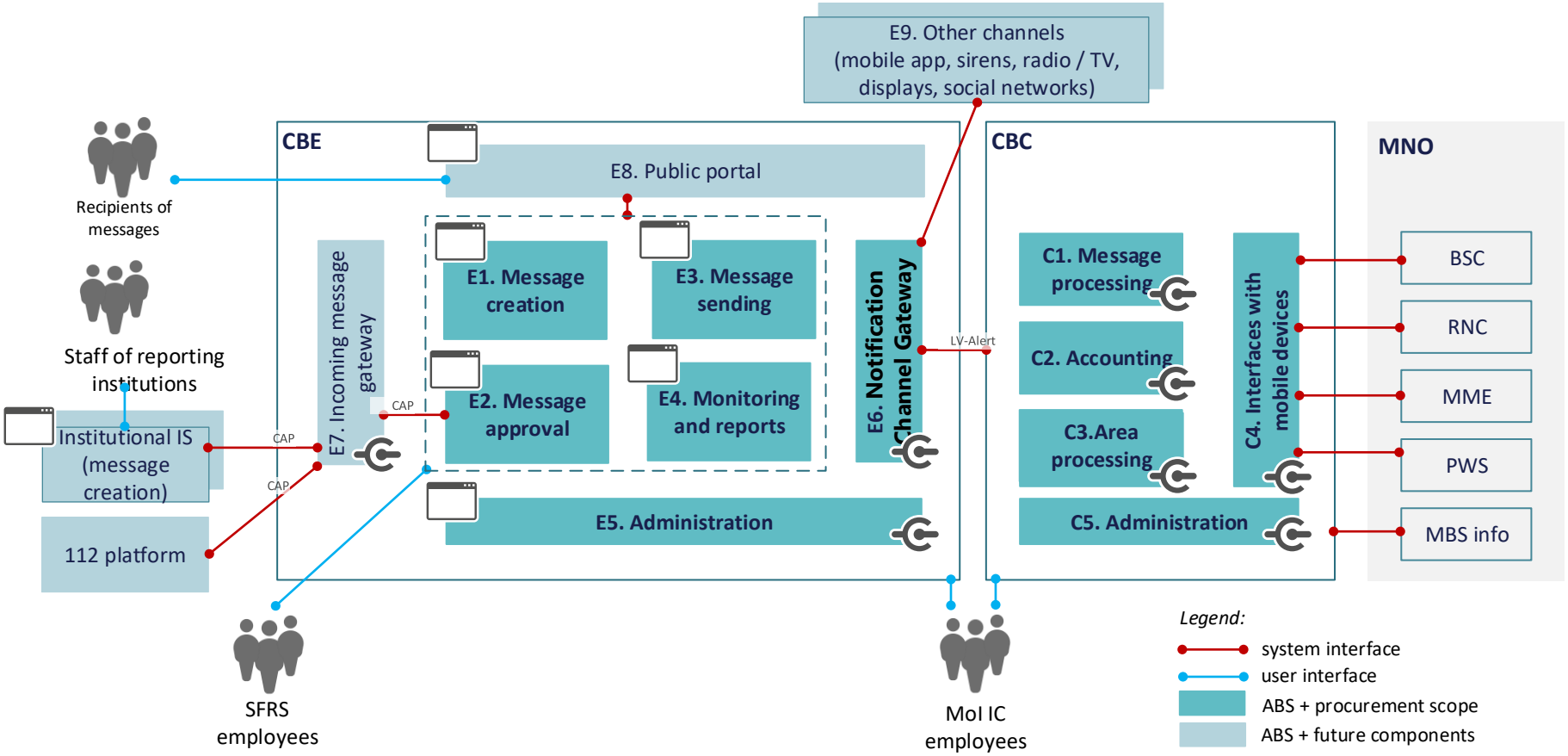


**Figure 2. ABS + functional units.**

# 3 FUNCTIONAL REQUIREMENTS

## 3.1 CBE

### 3.1.1 E1. Message creation

**(FP-001) Create a message** **(Mandatory)**

The System must provide user interface for preparing and storing warning messages.

The user interface must be designed in a way that intuitively, step-by-step allows the user to enter warning message information.

It must be possible to browse the content of the prepared message and return to the previous steps and make corrections if necessary.

It must be possible to save the created message and continue its preparation after a while (before sending).

**(FP-002) CAP, EU-Alert Support** **(Mandatory)**

It is necessary to ensure that content items from the CAP and EU-Alert[2] standard are included in warning message.

The Supplier must ensure that EU-Alert content items are adapted to the specific needs of Latvia (LV-Alert) by preparing and harmonizing the relevant clarifications with the Customer.

**(FP-003) Language** **(Mandatory)**

It is mandatory to ensure preparation and sending of messages at least in Latvian, Russian and English.

**(FP-004) Preforms**

It should be possible to create warning message templates by giving them names.

The use of pre-made warning message templates should be available when creating new messages.

It must be possible to browse, edit, and delete templates.

**(FP-005) Multi-channel support** **(Mandatory)**

It must be possible to specify the sending channels (one or more) for the message.

The cell broadcast channel is used as the default channel.

[2] *"Technical specification ETSI TS 102 900 V1 .3 .1"* https://www.etsi.org/deliver/etsi_ts/102900_102999/102900/01.03.01_60/ts_102900v010301p.pdf

### (FP-006) Sending Time
**(Mandatory)**

It must be possible to select the time at which the message should be sent (immediate or scheduled) as well as the retransmission feature (indicating the frequency and / or interval of transmission, times / end times, etc.).

### (FP-007) Specify notification area
**(Mandatory)**

When creating warning messages, it must be possible to indicate the notification target area in at least the following ways:

- Manually marking the area (polygon) (by connecting lines) on the map;
- Indicating the buffer area around the point or line on the map;
- Specifying the names of the administrative territorial units (selecting them from the list);
- By selecting predefined areas.

It must be possible to combine several areas.

### (FP-008) Defining notification areas
**(Mandatory)**

It must be possible to prepare and maintain predefined notification areas and to save them by giving them a name.

It must be possible to browse, edit, and delete stored notification areas.

### (FP-009) Housing and population density information **(Mandatory)**

It is mandatory to ensure that housing and population density information is loaded and visually displayed on the map.

Housing and population density information in 1 x 1 km and 100 x 100 m cells provided from Central Statistical Bureau of Latvia (available via open data portal)

When specifying and defining the areas for sending messages, the total number of housing and/or population in the area must be calculated.

### (FP-010) County population/number of households information
**(Mandatory)**

When creating notification areas, it should be possible to calculate the total number of inhabitants / households in the specific area (using a geodata layer with the number of inhabitants / households in 1x1km and 100x100m grid cells).

### (FP-011) Mobile User Density Information **(Optional)**

If the information (cache) of registered mobile subscribers is collected, then this information should be visualized on the map, and the total number of messages should be calculated by indicating or defining the sending areas.

**(FP-012) Mapping support** **(Mandatory)**

The browsing and processing of cartographic information related to the sending of warning messages and emergency events must be ensured, including:

- Connection of various external and Customer's basic map raster layers (using WMSTS and / or WMS services), including but not limited to:
  - Openstreatmap,
  - Googlemap,
  - Balticmaps (http://balticmaps.eu);
- Connection of various external and raster layers of vector layers available to the Customer (using WFS service);
- Representation of various sets of external and Customer's objects using geodata vector file formats, such as SHP, KML, etc.;
- Import and search of addresses and names (residential areas, territorial units, streets, houses, etc.);
- Direct and reverse geocoding possibility must be provided.

At least import/integration of the following layers must be ensured:

- Location, ownership and status of MNO base stations;
- Meteorological information;
- Objects of increased hazard.

At least the following map browser functionality must be provided:

- Zoom,
- Measuring distances,
- Automatic determination of the size of the area marked;
- Identification of objects;
- Manage the layers of map;
- Create, format, and save vector sites (point, line, area).

Licenses and availability for the use of geodata specific to Latvia will be provided by the Customer. Licenses for the use of globally available geo-data, if used, must be provided by the Supplier and these costs must be included in the Supplier's offer (e.g., GoogleMap, Mapbox, etc.).

### 3.1.2 E2. Message approval

**(FP-013) Confirmation of message** **(Mandatory)**

It must be possible for the responsible SFRS OMD employee to get acquainted with the parameters of the prepared warning message (message text, notifiable area, message sending time, notification channels, etc.) and at the same system interface window to approve or reject the sending of the warning message.

In case of rejection, the system must allow the user to add a comment on the reason for the rejection of the message (if the author of the message is another user and the workflow requires its approval).

**(FP-014) Message approval workflows** **(Mandatory)**

It must be possible to define workflows for the preparation and validation of messages, indicating the sequence of steps in which authorized users accept messages before they are sent.

**(FP-015) Approval workflow depending on message type** **(Mandatory)**

It must be possible to assign a specific workflow to certain types of messages (for example, before sending a message of the highest importance category, its sending must be confirmed by the SFRS management representative).

**(FP-016) Approval workflow for message author** **(Mandatory)**

It must be possible to assign a specific workflow to certain message authors (for example, if the message has been prepared by an external user (for example, LEGMC), then it is validated and approved by the responsible SFRS employee before sending it).

**(FP-017) Registration of approvals** **(Mandatory)**

When approving a warning message, it is necessary to ensure the creation of an appropriate audit record, which shows: who agreed; time; message text; possible corrections, reasons for rejection, etc. information.

### 3.1.3 E3. Message sending

**(FP-018) Manual message sending** **(Mandatory)**

It must be possible to manually initiate the sending of an approved warning message by sending it to the CBC for further transmission to the public.

**(FP-019) Automatic message sending** **(Mandatory)**

Automatic sending of approved messages according to the defined parameters (time, repetition rate, frequency, etc.) must be ensured.

**(FP-020) Resend in case of error** **(Mandatory)**

In the event of failed message transmission, the notification should pop up accordingly and the possibility of re-sending the message to the CBC (manually or automatically) must be provided.

**(FP-021) Notification Gateway** **(Mandatory)**

The functionality of the notification gateway must be provided, which could be used in the future to connect other notification channels.

At least the possibility to add LB-SMS and siren channels must be provided.

The Supplier must include in their offer a detailed description of the additional channel connection.

### 3.1.4 E4. Monitoring and reports

**(FP-022) Browsing messages** **(Mandatory)**

It must be possible to browse through warning messages that have been prepared but have not yet been sent, as well as already sent messages.

**(FP-023) Select and search messages** **(Mandatory)**

It must be possible to select and search for messages by various parameters, including:

- time of preparation and/or sending;
- user who created message;
- message type,
- message status;
- notification area;
- etc.

**(FP-024) Status of sent messages** **(Mandatory)**

It must be possible to browse through the detailed status of sent a message, including

- in how long time the message was sent;
- how many of the selected MNO towers have transmitted a warning message;
- etc.

**(FP-025) Reporting** **(Mandatory)**

It must be possible to produce on-screen and printable reports (at least 10 reports), such as:

- the number of messages grouped by different parameters over a specified time period;
- SLA performance report regarding message transmission;
- etc.

The exact content of the reports will be defined and agreed upon during the implementation of the System.

### 3.1.5 E5. Administration

**(FP-026) User Management** **(Mandatory)**

A user interface must be provided for managing user accounts (adding, editing, deactivating, deleting, browsing and exporting the user list).

**(FP-027) User Authentication** **(Mandatory)**

The Supplier must provide two-factor user authentication according to the principle - "something to know, something, to have".

**(FP-028) User groups** **(Mandatory)**

User rights management based on user groups must be ensured.

At least the following user groups must be provided:

- Administrators
- Message creator;
- Message validator;
- Message sender;
- User who can access reports;

One user can belong to several groups. The rights of the groups in this case add up.

A user interface must be provided for managing user groups and including users in groups.

**(FP-029) User Rights Management** **(Mandatory)**

The user interface for assigning rights to specific users or user groups must be provided.

A user interface must be provided for assigning rights to specific users or groups of users. Rights are granted for certain activities (e.g., sending messages, browsing audit logs, etc.).

**(FP-030) Classifiers** **(Mandatory)**

A user interface must be provided to maintain the classifiers and reference data used by the System.

### 3.1.6 CBE optional functionality

**(FP-031) Connecting other notification channels** **(Optional)**

It must be possible to connect other notification channels to the System in the future (Notification Gateway functionality), where the same CBE component would be used for message preparation (indicating other channels during message preparation), e.g.:

- LB-SMS (mandatory);
- sirens (mandatory);
- mobile app;
- radio;

- television;
- social networks;
- web sites;

The tenderer must provide in the technical and financial offer a description of possible additional channel solutions and their costs (at least for LB-SMS and siren channels).

Connection of additional channels is an option that can be used by the Customer.

**(FP-032) Integration with other State institution information systems** **(Future)**

It must be possible for the System to receive messages sent in the future automatically from the information system of other State institution (Incoming message gateway functionality).

The Applicant must provide in the technical and financial proposal a description of this integration solution (both in terms of technical and data exchange content).

**(FP-033) E8. Public Portal** **(Future)**

It must be possible to supplement the functionality of the System in the future with a public portal (website), where the public (inhabitants) will be able to obtain additional information about each warning message, as well as information on the necessary action in case of danger.

The public portal provides automatic displays warning messages after they are sent. It must be possible to place more detailed information about each warning message on the portal, as well as to provide additional information on the required action.

## 3.2 CBC

### 3.2.1 C1. Message processing

**(FP-034) Standards** **(Mandatory)**

Cell broadcasting must be provided in accordance with the following standards::

- 3GPP TS 22 268, PWS Requirements;
- 3GPP TS 23.038 version 9.1.1 Alphabet and language-specific information;
- 3GPP TS 23 041, Technical realization of Cell Broadcast Service (CBS);
- 3GPP TS 25 419, UTRAN Iu-BC Interface: Service Area Broadcast Protocol;
- 3GPP TS 29 168, Cell Broadcast Centre interfaces with Evolved Packet Core;
- 3GPP TS 48 049, Base Station Controller - Cell Broadcast Centre (BSC-CBC) interface specification;
- 3GPP TS 29.528 specifications for AMF (5G) service based interface Namf (N50);
- ETSI TS 102 900 V1 .3 .1 (2019-02) EU-ALERT using the Cell Broadcast Service;
- ATIS-0700008 - CBE-CBC Interface Spec.

### (FP-035) Mobile network operators (Mandatory)

Cell broadcasting must be ensured using the networks of 3 mobile network operators operating in Latvia:

- x towers, y cells, z RAN machines.

Information about MNO equipment manufacturers is provided in x. Annex.

### (FP-036) Notification areas (Mandatory)

The following notification areas must be defined for messages:

- cell or list of cells
- mobile base stations (MBS) or MBS list;
- the entire mobile network;
- area coordinates (set of polygons).

If the notification area is specified as polygon coordinates, then their conversion to the cell / MBS is provided by the CBC.

### (FP-037) Message format (Mandatory)

The message can be in text or binary form from 1 to 15 82-byte octet form.

The message encoding must meet the 3GPP standards.

### (FP-038) Notification throughput (Mandatory)

A throughput of at least 1 message per minute must be provided, with the possibility to expand it to 30 messages per minute.

### (FP-039) CBE interface (Mandatory)

The CBE interface must ensure that commands received from CBE are automatically executed.

The interface must be implemented using the HTTP protocol and the XML or JSON data format.

At least the following calls must be provided:

- CBC Login
- CBC Logout
- Change Password
- Create New Message
- Create Message Using Predefined Area
- Change Message Contents
- Kill Message
- Kill Message Cell
- Kill All Message Cell
- Message Information
- Predefine Area

- Remove Predefined Area
- Command Information
- New Message Cells
- New Message Cell Controllers
- New PLMN-wide message
- Retrieve Areas
- Network Availability
- Message Network Cell Count
- Retrieve Information Providers
- Index Message

The Applicant must provide a detailed description of the CBC-CBE interface in the tender offer.

**(FP-040) Number of CBE** **(Mandatory)**

An interface with at least 1 CBE should be provided with the possibility of extending it to 5 CBE in the future.

**(FP-041) Prioritization of messages** **(Mandatory)**

It is necessary to ensure that priority messages are transmitted outside the que (by discontinuing other non-priority messages, then restoring them).

**(FP-042) List of banned names** **(Mandatory)**

A list of banned words that are not allowed in the message text must be provided.

### 3.2.2 C2. Accounting

**(FP-043) Recording of messages** **(Mandatory)**

Records of at least the following broadcasting events must be kept:

- message,
- message type,
- cells/RAN devices,
- source/author of message,
- message status,
- time,
- other attributes of the message received from CBE.

**(FP-044) Broadcast data recording** **(Mandatory)**

Log events must be recorded to reflect message status or status changes.

Possible message statuses:

- planned,
- starting,
- running,
- killing,
- Finished,
- skipped;

Possible status of network elements:

- enabled,
- disabled,
- unlocked,
- locked.

**(FP-045) Reports** **(Mandatory)**

The following reports must be able to obtain (in CSV or analogue format):

- Number of successful incoming test messages;
- Number of successful incoming heart beat messages;
- Number of successful incoming normal messages;
- Number of files incoming test messages per error cause;
- Number of files incoming heart beat messages per error cause;
- Number of files incoming normal messages per error cause;
- Number of status report requests for test messages;
- Number of status report requests for heart beat messages;
- Number of status report requests for normal messages;
- Number of 2G cells addressed to broadcast test messages;
- Number of 2G cells addressed to broadcast heart beat messages;
- Number of 2G cells addressed to broadcast normal messages;
- Number of 3G, 4G, 5G cells addressed to broadcast test messages;
- Number of 3G, 4G, 5G cells addressed to broadcast heart beat messages;
- Number of 3G, 4G, 5G cells addressed to broadcast normal messages;
- Number of 2G cells actually have broadcasted test messages;
- Number of 2G cells actually have broadcasted heart beat messages;
- Number of 2G cells actually have broadcasted normal messages;
- Number of 3G, 4G, 5G cells actually have broadcasted test messages;
- Number of 3G, 4G, 5G cells actually have broadcasted beat messages;

- Number of 3G, 4G, 5G cells actually have broadcasted normal messages;
- Number of test messages fileed to broadcast per error cause type;
- Number of heart beat messages fileed to broadcast per error cause type;
- Number of normal messages fileed to broadcast per error cause type;
- Number of enquire message status requests;
- Number of replace message request;
- Number of cancel requests.

**(FP-046) Reports in geodata format** **(Mandatory)**

It must be possible to obtain the above report information in KML or analogue format, which would allow visualization of the GIS as a layer.

### 3.2.3 C4. Area processing

**(FP-047) Calculation of notification areas** **(Mandatory)**

The CBC should provide the conversion of notification area received from CBE to the list of cells/RAN equipment in the cellular network, based on information about the mobile base stations.

**(FP-048) Information on cellular base stations** **(Mandatory)**

It must be ensured that information on mobile base stations (coordinates, status, etc.) is received from the MNO.

The format and manner of receipt of this data will be specified in the course of the work.

**(FP-049) Number of subscribers registered** **(Future)**

It must be possible to obtain and update the number of subscribers registered in each cell from the MNO.

The Applicant must provide a description of the relevant solution in the tender, as well as the required information from the MNO.

### 3.2.4 C4. Interfaces with mobile devices (RAN)

**(FP-050) 2G (GSM), 3G (UMTS), 4G (LTE) support** **(Mandatory)**

Cell broadcast warning messages must be broadcasted according to the following technologies:

- 2G (GSM);
- 3G (UMTS);
- 4G (LTE).

**(FP-051) 5G aid** **(Optional)**

It should be possible to provide cell broadcasting in *5G non-standalone* technology.

**(FP-052) Notification volumes** **(Mandatory)**

The solution must ensure that the following amounts are reported:

- At least 2000 RAN (BSC, RNC, etc.) equipment with the possibility to expand up to 2500 equipment;
- At least 200,000 cells with the ability to expand to 5,000,000.

**(FP-053) Capacity Management** **(Mandatory)**

The CBC must take into account the technical constraints of RAN and cell load, including:

- One cell broadcast message can be sent at a time;
- Limits on the number of active messages on RAN devices.

The solution must provide protection against exceeding the load limits.

**(FP-054) Status of cells and RAN devices** **(Mandatory)**

The CBC should ensure the storage/updating of information on the status of cells and RAN devices (BSC, etc.), including:

- Usage state: idle, active or busy;
- Administrative state: unlocked, shutting down or locked;
- Operational state: enabled or disabled;
- The air capacity in use (for cells);
- The storage capacity in use;
- The rate of commands sent to BSC.

**(FP-055) Mobile network error handling** **(Mandatory)**

The CBC should ensure the identification and processing of public mobile electronic communications network (PMECN) errors, including:

- CBC-RAN configuration errors
- CBC-RAN connection errors;
- RAN error messages.

### 3.2.5 C5. Administration

**(FP-056) User Management** **(Mandatory)**

It must be possible to manage CBC users.

**(FP-057) Administration User Interface** **(Mandatory)**

A user interface must be provided in the web browser to perform CBC administration and configuration tasks, including:

- Switching on/off CBC components;

- Input, browsing, changes to CBC configuration parameters (including CBE connections, CBC-RAN connections, etc.);
- Monitoring the operation of the CBC.

**(FP-058) Command line user interface** **(Mandatory)**

A command line interface must be provided to enable CBC administration and configuration tasks.

**(FP-059) SNMP interface** **(Mandatory)**

It must be possible to monitor the operation of the CBC using the SNMP protocol.

In case of errors, SNMP alerts must be sent.

**(FP-060) Backup Copies** **(Mandatory)**

CBC data must be backed up with the option to restore the CBC operation in the event of an emergency.

**(FP-061) Audit records** **(Mandatory)**

CBC performance audit records must be created and it must be possible to review these audit records.

# 4 NON-FUNCTIONAL REQUIREMENTS

## 4.1 USERS AND LICENSES

### (NP-001) Rights of use (Mandatory)

The Supplier must ensure the possibility to use the System without restrictions within 5 years from the acceptance (implementation) of the System delivery and commissioning of the System to the specified number of users.

The Supplier must ensure that the State of Latvia (in the person of the Customer) receives non-exclusive rights to use the System software for a specified number of users for an indefinite period of time.

The Customer must be able to copy and use without restrictions for his own needs, as well as, if necessary, modify the documentation related to the System (including software requirements specification, user manual, administrator's manual, System design description, etc.), as well as read and copy information stored in the System.

### (NP-002) Total number of users (Mandatory)

The estimated total number of users (*named users)* is:

- SFRS OMD dispatchers - 10;
- Reporting users - 20;
- External users (users from other authorities) - 30;

The expected number of simultaneous (*concurrent*) users is:

- SFRS OMD dispatchers - 3;
- Reporting users - 2;
- External users (users from other authorities) - 3.

### (NP-003) Licensing of New Software (Mandatory)

All software code created within the procurement (including installation scripts, configuration templates, etc.) is licensed under *the European Union Public License* (EUPL) v 1.2[3] license.

The Applicant's previously created components, as well as commercial third-party products used in the solution, must be logically and physically separated from the software created within the Project.

If the solution to be developed within the Project includes a components based on a components previously created by the Applicant (by modifying or supplementing it within the Project), then it is licensable with an EUPL license.

If the solution includes commercial third-party paid products, they must be included in the financial offer in accordance with the defined maximum requirements for the use of the solution.

## 4.2 ARCHITECTURAL REQUIREMENTS

### (NP-004) System architecture (Mandatory)

The solution must consist of separate logically and physically separable components (modules) and defined interfaces.

The solution must comply with a 3-level architecture – user interface, application server/business logic, database.

The Applicant in their offer must provide a description of the architecture of the proposed solution, which includes a breakdown of components (modules) - a description of their functionality and implementation, the main interfaces and their description.

The applicant must submit an infrastructure-level scheme showing all servers or other infrastructure components, their network connections and protocols.

User functionality must be provided through a web browser, providing multi-user access.

### (NP-005) High Availability Support (Mandatory)

The proposed solution's architecture must support the use of two geographically separated data centers and be able to operate in high-availability, component deployment and load-sharing scenarios (including ensuring that all key components are made redundant).

The Applicant must describe in their offer the proposed approach for the provision of high availability component deployment and load sharing scenarios.

The solution's architecture must ensure:

- continuity of System operation in case of failure of one data center and related components;

[3]https://joinup.ec.europa.eu/collection/eupl/eupl-text-11-12

- Continuity of user session in these scenarios;

The financial offer must include all related costs to ensure high availability.

**(NP-006) Use of ready-made solutions and technological capabilities (Mandatory)**

The Applicant must, where possible and appropriate, offer the use of ready-made solutions and technologies.

Ready-made solutions can be combined with the original design to optimally meet the requirements, including - functionality, usage rights, openness, etc.

**(NP-007) Using Open Solutions (Optional)**

The Applicant must offer a solution that is based as much as possible on the principles of open-source software or a technology-neutral solution that minimizes the risk of dependence on one supplier / manufacturer.

**(NP-008) Use of the web interface (Mandatory)**

The system must ensure that the user's functionality is available in a web browser (exceptions to the administrator's functionality are possible).

The system must be available on the following platforms: MS Windows workstations using the latest versions of Google Chrome, Mozilla Firefox, Microsoft Edge and Safari.

**(NP-009) Accessibility from Mobile Devices (Optional)**

The System must ensure that the main functionality is available on mobile devices (with Android and iOS).

**(NP-010) Interface language (Mandatory)**

The user interface must be in Latvian (the administration may be in English).

If the System is not currently in Latvian, the Applicant must include a description of the works needed to carry out to make System in Latvian, indicating the necessary involvement of the Customer.

## 4.3 SAFETY AND COMPLIANCE

**(NP-011) Compliance with safety regulatory enactments (Mandatory)**

The System must meet the following requirements of security standards and regulations:

- Compliance with the recommendations and guidelines included int the standard "*LVS ISO/IEC 15408 "Informācijas tehnoloģija – Drošības tehnikas – IT drošības novērtējuma kritēriji" 2.daļā "Drošības funkcionālās komponentes*" (Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components. ISO/IEC 15408-2. Third edition 2008-08-15) and formulating and implementing security requirements for specific systems within the framework of the Agreement;
-

- Regulations of the Cabinet of Ministers of 19 June 2012, No. 421 "Requirements for the Protection of State Information System Interoperates and Integrated State Information Systems";
- Regulations of the Cabinet of Ministers of 15 October 2005, No. 764 "General Technical Requirements of State Information Systems";
- Regulations of the Cabinet of Ministers of 28 July 2015, No. 442 "Procedures for the Ensuring Conformity of Information and Communication Technologies Systems to Minimum Security Requirements";
- Regulations of the Cabinet of Ministers of 18 January 2019, No. 15 "Regulations Regarding the Security Incident Relevance Criteria, Reporting Procedures, and Content of Report";
- Regulations of the Cabinet of Ministers of 19 January 2019, No. 43 "Regulations Regarding the Conditions for the Determination of Significant Disruptive Effect of a Security Incident and the Procedures by which the Status of an Operator of Essential Services and Essential Services are Granted, Reviewed, and Terminated";
- Requirements included in other regulatory enactments applicable to the security of information systems, which are adopted and enter into force during the development of the System.

### (NP-012) General security requirements (Mandatory)

The System must be designed in such a way that it is not possible to bypass authentication and authorization procedures and unauthorized use of the System's functionality, access to its data or files, exceeding the amount of access rights granted.

Users may not access information stored on the System by bypassing security control programs, such as at the operating system, files, or database level.

The System architecture must be designed in such way to minimize potential security risks. Sufficient controls must be in place in the System to ensure that confidential information entrusted to the System, both during transmission and storage, is not disclosed to unauthorized persons or software.

### (NP-013) Authentication, authorization and audit (Mandatory)

The System identification, authentication, authorization and audit procedures must meet the following requirements:

- The principle of authorization must be used, according to which anything that is not directly allowed is prohibited;
- All activities must verify the authorization to perform the activity. The verification should take place at the level of each request;
- Protection against verification of the user existence (the System must not show whether the user exists or not before authentication attempts);
- Any unsuccessful authorization or authentication attempt must be logged in the System log;

- The System must block the user account if several (configurable amount) unsuccessful authentication attempts are made;
- In the System, all actions performed by users and administrators must be identified (it must be known which person performs each action);
- The principle of authorization must be used whereby everything not directly authorized is prohibited;
- All transactions must verify the authorization for the operation. The test must be carried out at the level of each request;
- Ensure protection against the verification of the presence of users (The system must not be detected or the user exists or not prior to successful authentication);
- Any failed authorization or authentication attempt must be recorded in the system log;
- The system must lock the user account if more than one (configurable size) failed authentication attempt is made.
- All activities performed by users and administrators in the system must be identified (be known which person is executing each activity);
- The System must have a technical solution that automatically terminates inactive sessions after "n" minutes (where "n" is a configurable parameter, assuming a default value of 15 minutes);
- The System must include a notification mechanism that informs the user of the inactivity of the session and the termination of the session "n" minutes before the session expires (where "n" is a configurable parameter, assuming a default value of 2 minutes);
- The System must contain a control that prevents the reuse of an existing session identifier for the creation of a new session.
- The System must be able to limit the access of administrators to one or more Internet Protocol address areas. By the Internet Protocol address area here is meant the IPV4 or IPV6 address interval.

### (NP-014) Information transmission encryption (Mandatory)

The System must ensure that information is encrypted by transmitting it over the data transmission network. TLS 1.2 or later protocols must be used to encrypt information.

### (NP-015) Compliance with web application security requirements (Mandatory)

The system software must be designed in accordance with the generally accepted security requirements of web applications (see OWASP guidelines, https://owasp.org/www-project-top-ten/).

Independent external security testing of the System must have been done. In their offer, the Applicant must provide proof and information on the performance of such testing.

### (NP-016) Compliance with GDPR requirements (Mandatory)

The System must comply with the requirements of the General Data Protection Regulation (GDPR)[4].

### (NP-017) Audit records (Mandatory)

The System must ensure that audit trails are kept of at least the following events:

- Successful/failed authentication user authentication;
- User account changes;
- Data processing - reading, editing and deleting;
- Sending messages.

It must be possible for the Customer to search and download System audit records.

### (NP-018) Monitoring (Mandatory)

It must be possible to collect real-time system availability and load monitoring information and transfer it to the monitoring software "Zabbix" used by the Customer.

## 4.4 Performance and Accessibility

### (NP-019) Performance and accessibility requirements (Mandatory)

The Applicant must offer solutions that, from an architectural design point of view, ensure the maximum performance and availability requirements specified below, ensuring the functional and non-functional requirements specified in the technical specification, including:

- Number of simultaneous users, see (NP-002) requirement;
- Mobile network parameters – see (FP-035) requirement.

The offer must also include the ICT infrastructure requirements necessary for the operation of the proposed solution (indicating the required server capacity, memory, etc. parameters).

### (NP-020) Notification performance (Mandatory)

The System as a whole must be able to send messages on all mobile networks:

- 50% of the population - no more than 6 minutes.
- 97% of the population - not more than 10 minutes.

### (FP-062) User interface performance (Mandatory)

The System user interface must meet the following performance requirements (according to the specified maximum number of concurrent users):

- Display of the list window and a separate entry window - no longer than 2 seconds;
- Saving corrected records - no longer than 5 seconds at maximum load;

[4]https://eur-lex.europa.eu/eli/reg/2016/679/oj

- Search / filter - no longer than 10 seconds;
- Report creation - no longer than 20 seconds.

**(NP-021) System Accessibility** **(Mandatory)**

The System must ensure the following accessibility requirements:

- Expected System availability time - 24/7;
- An unplanned breakdown must not exceed 2 hours per month.

**(NP-022) Backup and data restore** **(Mandatory)**

It must be possible to make backup copies of the data without stopping the System.

The Applicant's offer must describe the proposed approach for backing up data and restoring data.

**(NP-023) Business Continuity and Recovery Plan** **(Mandatory)**

A Business Continuity and Recovery Solution must be provided.

As part of the implementation, the Supplier must supply a draft backup and recovery plan (including a description of all necessary procedures and activities related to ensuring the continuity of the system and restoring its operation)

## 4.5 Infrastructure and operation

**(NP-024) Available ICT infrastructure** **(Information)**

The following ICT infrastructure provided by the Customer is available to operate the System,

- Two physically remote Tier-3 compliant data centers;
- VMWare virtualization platform vSphere High Availability capability;
- 100Gb redundant connections between data centers and VPN connections to MNO ICT infrastructure using public data transmission networks;
- Windows Server software.

**(NP-025) Required ICT infrastructure** **(Mandatory)**

In order to ensure the implementation and operation of the System, the Applicant may count on the ICT infrastructure referred to the requirement (NP-024).

The Applicant must indicate in their offer what virtual ICT infrastructure resources are needed to ensure the operation of the System, including virtual machines, CPU/kernel, RAM, memory, network throughput etc.

If additional ICT infrastructure (including software) is needed in addition (NP-024), then the Applicant's offer must contain a description/specification of such ICT infrastructure and in the financial offer must include the costs related to its purchase.

# 5 REQUIREMENTS FOR THE SERVICES TO BE PROVIDED

The subject of the procurement includes the provision of the following services:

- System implementation
  - Customer needs analysis, specification requirements;
  - System customization, configuration;
  - Integration with other systems;
  - Training;
  - Deployment, testing and acceptance;
- System maintenance (for 5 years)
  - Free warranty (1 year);
  - User support (level 3 support);
  - Delivery of system updates;
  - Providing updates;
- Implementation of change requests, provision of additional support

## 5.1 General service requirements

**(PP-001) Project management** **(Mandatory)**

The Supplier must appoint a project manager who must ensure the management of the execution of the procurement works by the Supplier throughout the implementation of the procurement and must be the main contact person in connection with the execution of the procurement works.

Project management should be ensured in accordance with the generally accepted project management approach.

The Applicant must provide a description of the proposed project management approach in their offer.

**(PP-002) Project kick-off meeting** **(Mandatory)**

Within 5 working days after signing the contract, the Supplier must organize a kick-off meeting, during which at least the following issues must be considered:

- Project participants, roles;
- Understanding of project goals and critical success factors;
- Project scope and implementation approach;
- Project time schedule;
- Project communication.

### (PP-003) Project management plan (Mandatory)

Within two weeks from the signing of the contract, the Supplier must prepare, present and coordinate with the Customer the project implementation plan, which includes at least the following information:

- Project team, roles and responsibilities of those involved;
- System implementation approach;
- Project implementation time schedule;
- Necessary involvement of the Customer;
- Communication plan (incl. Progress meetings, information exchange procedures, etc.)
- Quality assurance measures;
- Other information necessary for the successful implementation of the project.

### (PP-004) Progress meetings (Mandatory)

The Supplier must participate in regular progress meetings, during which the progress of the project implementation is monitored and work issues related to the project implementation are addressed.

Progress meetings may be organised remotely.

### (PP-005) Supervisory Board (Mandatory)

The representatives of the Supplier's management must participate in the meetings of the Project Monitoring Board (not less than once every three months) upon invitation from the Customer.

### (PP-006) Language (Mandatory)

The working language of the project is Latvian or English (communication, meetings, protocols, etc.).

The Supplier must ensure the translation of the materials to Latvian, which concerns the end user.

### (PP-007) Sharepoint environment (Mandatory)

The Supplier must use the Customer's Sharepoint environment for information exchange and delivery of deliverables.

## 5.2 Implementation of the system

### (PP-008) Implementation stages (Mandatory)

Implementation of the System must be performed in the following steps:

- Customer needs analysis, clarification of requirements
- System customization, configuration
- Integration with other systems
- Training

- Deployment, testing and acceptance.

The Applicant must provide in their offer a detailed approach and plan for the delivery (implementation) of the System, ensuring that the requirements of the steps are met.

If the steps of the project approach proposed by the Applicant differ from the above-mentioned implementation steps, then the Applicant must provide a mapping of these steps with the steps specified in this requirement description.

**(PP-009) Deadlines** **(Mandatory)**

Delivery (implementation) of the System must be ensured within a maximum of 8 months from the moment of signing the contract (time of acceptance of the implementation of the System and fully operational System).

**(PP-010) Customer needs analysis, clarification of requirements** **(Mandatory)**

The Supplier must perform a detailed analysis of the Customer's needs and a clarification of the requirements, specifying the way in which the requirements set out in the Technical Specification will be ensured.

The applicant must offer a methodology for analyzing the customer's needs and documenting the detailed requirements.

**(PP-011) System customization, configuration**
**(Mandatory)**

The Supplier must customize and / or configure the System to ensure that the technical specifications of the procurement and requirements specified during the Customer needs analysis are met.

**(PP-012) Integration with other systems** **(Mandatory)**

Ensure that the system is integrated with MNO related systems, i.e.:

- MNO RAN components (BSC, etc.);
- Import and update of MNO mobile base station information.

**(PP-013) Training** **(Mandatory)**

Suppliers must provide the following training (may be provided remotely):

- Training of instructors (*train the trainer*) - 10 trainees, at least 6 hours;
- Training of system administrators: 2 trainees, at least 6 hours.

Training materials and test environment for training in Latvian or English must be provided for training.

The training content must be adapted to the Customer's situation and the planned System usage scenarios.

**(PP-014) Deployment, testing and acceptance** **(Mandatory)**

The Supplier must perform the deployment of the System in the production environment, ensuring its availability to all users of the System.

Successful implementation of the System is confirmed by acceptance testing, within which the compliance of the System with the initial requirements of the procurement and specified requirements during the implementation phase is validated.

System availability testing includes a single data center failure scenario.

System security testing will be performed by the Customer.

System testing is performed after System deployment using data and configuration corresponding to actual operation of the system.

After the System has been accepted, the System's operation is initiated.

The Applicant in their offer must describe the proposed System testing and acceptance approach.

**(PP-015) Documentation** **(Mandatory)**

The Supplier must provide at least the following documentation of the deliverables:

- The System user's guide in Latvian (may be electronic, e.g., in wiki format);
- System Administrator's Manual (may be in English).

**(PP-016) Contextual assistance** **(Optional)**

The system should provide contextual help - the ability to activate explanatory information from a specific window. User assistance integrated in the user interface must be provided:

- on screen forms for each interface element (field, selection list), an explanation for filling the field;
- on application pages, the ability to open an explanation about the purpose of using a specific page. May contain links to external documentation;
- general instructions for use of the application - a brief description of the purpose of use of the application, principles of use, processes. May contain links to external documentation.

**(PP-017) On-site visits** **(Mandatory)**

During the implementation of the System, the Supplier should provide at least two on-site visits (e.g., when carrying out an analysis of the needs of the Customer at the beginning of the project and at the final step of the project when providing training for users), in compliance with applicable travel rules and restrictions.

All travel costs, etc., should be included in the financial offer.

## 5.3 SYSTEM MAINTENANCE

**(PP-018) Off-site support** **(Mandatory)**

As part of operating the System, the Supplier must provide off-site support (via e-mail or other electronic means of communication), which includes:

- Provision of help desk services in 24/7 mode;

- Availability of supplier specialists during regular testing of the System (planned 2x per year);
- Consultations and answers on issues related to the use of the System;
- System error ticket registration, classification and free error fixing.

The Applicant must provide a detailed description of the proposed support services in their offer.

**(PP-019) On-site support** **(Optional)**

The Supplier must provide on-site support for the system.

The Applicant must provide in their offer a detailed description and conditions of the offered on-site support service (if it is available).

**(PP-020) Provision of a free guarantee** **(Mandatory)**

The Supplier must provide a free guarantee for 12 months after the System implementation (after signing the System Transfer-Acceptance Act).

During the warranty period, the Supplier must for free perform elimination of system defects and delivery of corrections to the Customer. Defects are considered to be non-compliance of the System with the requirements of the Technical Specification, requirements agreed during the execution of the contract, conditions of the contract and regulatory enactments in force at the time of System implementation. In case of conflict, the requirements of this Technical Specification shall prevail.

**(PP-021) Delivery of System updates during System maintenance period** **(Mandatory)**

The Supplier must ensure the delivery and installation of System updates (functional and security) during maintenance at no additional charge.

**(FP-063) Error Request Management** **(Mandatory)**

The Supplier must ensure the possibility for certain users of the Customer to report System errors.

The Supplier must provide the ticketing (error, etc.) management environment / tools.

The Applicant in their offer must provide information on the procedures for managing error tickets and the tools used.

**(PP-022) Support Response Times** **(Mandatory)**

When providing System Maintenance Support, the Supplier must ensure at least the following response times:

- Ticket registration, classification and providing initial information on the potential time of troubleshooting):
  - 1 hour in the event of an accident,
  - 8 hours in other cases on working days and during working hours from 9:00 to 18:00 Latvian time).

### (PP-023) Error categories and troubleshooting times (Mandatory)

When providing System Maintenance Support, the Supplier shall provide at least the following troubleshooting times:

- Category 1 (accident paralyzing software operation) -3 hours;
- Category 2 (an error that cannot be bypassed: a problem that affects one of the software functions and cannot be performed using another component of the System) – 8 hours;
- Category 3 (error that can be bypassed: problem, but unlike category 2, this shortcoming can be bypassed) - 5 working days;
- Category 4 (inaccuracy: problem that does not directly affect working with software) – 20 working days;
- Category 5 (request for change: problem when software needs changes that were not previously defined) - by agreement;
- Category 6 (consultation on the use of software) - 1 working day.

### (PP-024) Implementation of change requests, provision of additional support (Mandatory)

The Customer by mutual agreement with the Supplier may order additional works (for example, in connection with integration or the provision of specific additional support) within the framework of this agreement.

The Applicant in their financial offer must include information about an hourly rate for additional works.