DECEMBER 2024

EUROPEAN EMERGENCY NUMBER ASSOCIATION

# PUBLIC WARNING REPORT CARD

THIS DOCUMENT IS SPONSORED BY opencode MOBILE NETWORK SYSTEMS

# Table of contents


Foreword 1

Acknowledgements 2

Legal disclaimer 3

Understanding the questions asked from the countries 4

Austria 14

Belgium 23

Bulgaria 34

Croatia 43

Cyprus 54

Czech Republic 61

Denmark 70

Estonia 79

Finland 89

France 96

Germany 107

Greece 119

Hungary 127

Iceland 137

Ireland 145

Italy 146

Latvia 154

Lithuania 162
Luxembourg 171
Malta 180
Netherlands 188
Norway 197
Poland 206
Portugal 214
Romania 223
Slovakia 232
Slovenia 241
Spain 248
Sweden 257
UK 265

# OPENCODE SYSTEMS

With nearly 25 years of global experience in telecommunications, Opencode Systems is the leading provider of Public Warning Systems (PWS), specializing in cutting-edge solutions like Cell Broadcast Centers, Cell Broadcast Entities, Alert Exchangers, and Location-Based SMS (SMS-LB) emergency alert systems. Our patented technology has been deployed across Europe, Asia, the Americas, the Middle East, the Pacific, and the Caribbean.

Opencode's wireless alerting solutions enable governments to deliver mass public warnings across all generations of mobile networks and across all mobile channels. Within seconds, critical safety information can be broadcast to millions of mobile users, targeting specific locations or covering entire countries.

**Today, Opencode Systems is the largest provider of centralized Wireless Public Warning Systems,** helping governments significantly reduce costs, streamline operations and take full control over the broadcast process, while also enabling service providers with the required level of radio data privacy. This groundbreaking solution has set a new standard for nations with populations up to 50 million.

**Opencode's alerting solutions support a wide range of broadcast channels, including:**

- Cell Broadcast
- Location-based Text and Voice Broadcast
- TV / IPTV and Radio Broadcast
- Social Networks Broadcast
- Public and Road Signage Broadcast
- Siren Broadcast
- Satellite Broadcast

The public warning alerts are managed via a user-friendly interface, which features interactive online and offline geographic information system (GIS) maps. Opencode platform enables the visualization of operational and emergency data, supporting both broadcast and crisis management processes. The platform also serves as the administrative hub for government agencies, service providers, and network operators. The interface is equipped with advanced security, access control, and validation functions, ensuring ease of use while maintaining robust protection against breaches or unauthorized activities.

Opencode Systems has delivered telecommunications solutions in over 70 countries, creating substantial value for both telecommunications providers and governments.

Opencode Systems is a privately owned independent company, free of debt and not reliant on any government and venture affiliations.

To explore our product portfolio and for more information about our global offices, please visit www.opencode.com or contact us at sales@opencode.com for any inquiries.

# Foreword

Public warning systems are essential tools for protecting lives and property. They play a crucial role in helping communities prepare for and respond to disasters. In simple terms, public warning refers to the process of sending timely and accurate alerts to people at risk during emergencies—whether through mobile phones, sirens, TV, or other channels—to inform them of immediate dangers and guide their response.

In Europe, recent natural disasters in Spain, Switzerland and Central Europe have brought the importance of these systems into sharp focus. At a global level, initiatives like the United Nations Early Warning For all Initiative remind us that ensuring these alerts reach everyone is more critical than ever.

In the European Union, the European Electronic Communications Code (Directive 2018/1972) has been a major driver in improving public warning capabilities. It requires Member States to implement systems that can send alerts directly to people in affected areas via their mobile phones. But technology is only a small part of public warning. As highlighted during the recent floods in the Valencia region in Autumn 2024, the strategy on how these alerting technologies are used is decisive. It is crucial to define well in advance when an alert is sent, with what message, by who, to whom, to which area, among other things.

The Public Warning Report Card 2024 intends to review the technologies and strategies for every country, highlighting some best practices in European countries, which can be beneficial for any public authority. Drawing on past publications, including the 2019 update on public warning systems, the blog post "8 Recommendations to Get the Most Out of Public Warning Systems", and other relevant publications on this topic, this report emphasises the value of cooperation across countries, industries, and institutions. By learning from one another, we can ensure these systems are not only compliant with EU and relevant national law but are also effective in reaching everyone—especially vulnerable populations who might otherwise be left behind.

The Public Warning Report Card 2024 intends to not only be a collection of data, but rather reflect the collective effort of Europe's emergency services and the broader public safety community to build a safer, more prepared society. As the risks we face grow more complex, robust multi-channel public warning systems will continue to be a pillar of our resilience.

**Benoit Vivier**
Public Affairs Director, EENA
09 December 2024

# Acknowledgements

The Public Warning Report Card 2024 could not have been completed without the contributions and support of many individuals and organisations.

I would like to thank my colleagues at EENA for their invaluable assistance throughout this project. Special thanks to Sanna Antila, who managed the visual aspects of the document and make sure that this document is easy to read, and to Gary Machado, who provided direction and oversight. I am also grateful to Cristina Lumbreras and Freddie McBride for their work on refining the questionnaire, as well as to Peter Lonergan and Annita Elissaiou for their thoughtful review of the document.

My thanks also go to Amélie Grangeat from the International Telecommunication Union (ITU) for reviewing the questionnaire and ensuring the technical and operational relevance of the questions.

I extend my sincere appreciation to all those who participated in interviews and provided insights and data about their countries, as well as those who facilitated connections and shared their expertise during this process. Without their contributions, this document would be empty and without purpose.

Finally, I wish to acknowledge the support of Opencode, the sponsor of this document, for enabling its development while respecting the independence of its content.

Thank you to everyone who contributed to this project.

## LEGAL DISCLAMER

This document is authored by EENA staff members with contributions from representatives of public authorities. This document does not represent the views of individual members of EENA, or any other parties.

This document is published for information purposes only and it does not declare to be a statement or interpretation of EU law or the national law of EU Member States. This document is entirely without prejudice to the views of relevant national statutory authorities and their legal functions and powers, whether under EU law or the national law of their Member State. Accordingly, under no circumstances may reliance be placed upon this document by any parties in compliance or otherwise with any applicable laws. Neither may reliance be placed upon this document in relation to the suitability or functionality of any technical specifications, or any other matters discussed in it. Legal advice, technical advice and other advice as relevant, may be sought as necessary.

This publication is for EENA Members only. It is forbidden to forward this publication to non-EENA members without the approval of EENA. If you are not member of EENA you must not use, disclose, reproduce, copy or distribute the contents of this communication. If you have received this in error, please contact the sender. The information published is based on the information provided by relevant representatives. It is also based on responses to a questionnaire designed by EENA and sent to EENA members in each country described in this document. Interviews were conducted with some of these members.

Possible inaccuracies of information are not under EENA's responsibility. EENA is not liable for any use that may be made of the information contained therein.

For more information, please contact Benoit Vivier at bv@eena.org.

# Understanding the questions asked to the countries

*This introductory section intends to help the reader understand why some questions were asked providing the rationale behind them but also some technical information, which may be necessary for understanding the questions and answers. We will go through the questionnaire section by section.*

## SECTION 1: GENERAL QUESTIONS

This section gathers basic information about the public warning system in each country, including its name, geographical coverage, and governance structure. Knowing the system's name ensures clarity for reference and comparison. Details about coverage help identify whether the system operates nationwide or in specific regions, including overseas territories where implementation may differ. Governance information provides insight into which entity is responsible for the system's oversight, whether a government ministry, emergency management agency, or another authority.

## SECTION 2: PUBLIC WARNING CHANNELS

This section examines the communication channels used for public warning, highlighting the importance of a multi-channel approach. No single channel can guarantee 100% population coverage, so leveraging multiple channels increases the likelihood of reaching everyone, including vulnerable groups or those with limited access to certain technologies.

Mobile phones are particularly effective due to their widespread use, but several technologies can be deployed:

- Cell Broadcast: Broadcasts alerts to all compatible devices in a designated area through cell base stations.
- Location-Based SMS: Sends SMS alerts to devices in a specific area based on real-time or recent location data.
- Registration-Based SMS: Sends SMS alerts to individuals who have opted into a specific service or database.
- National SMS: Sends messages to all mobile users in a country, regardless of location.
- Mobile Apps: Applications specifically designed for public warning can provide alerts alongside additional information, though they require prior download and user registration.
- Apps Designed for Other Use: Apps initially developed for other purposes (e.g., public broadcaster, public transportation apps) can also deliver public warnings to their users.
- Other channels complement mobile-based solutions and ensure broader coverage:
    - Sirens: Provide audible alerts for immediate emergencies, especially in outdoor environments.
    - Fixed-Line Alert Systems: Send voice warnings to landline telephones.
    - Emails: Deliver detailed alerts and instructions sent by email
    - Social Media: Offers rapid dissemination of alerts to tech-savvy and younger populations but lacks reliability during network disruptions.
    - TV & Radio: Long-established channels that provide wide coverage, especially in areas with limited internet access.
    - Billboards & Public Signs: Deliver visual alerts in public spaces, effective for mass awareness in busy areas.

## Common Alerting Protocol (CAP)

The questions in this sub-section focus on the use of the Common Alerting Protocol (CAP) in public warning systems. CAP is a standardised protocol designed to create alerts in a harmonised way so information is disseminated across all channels in a consistent manner.

It enables different systems and technologies to communicate seamlessly, ensuring consistent and efficient delivery of alerts across various channels.

CAP messages are structured to include essential information such as the type of emergency, the affected area, and recommended actions. This standardisation reduces delays in disseminating warnings and minimises the risk of miscommunication during emergencies.

Having a public CAP feed allows other organisations, developers, and even neighbouring countries to access and repurpose alert data, fostering transparency and collaboration. The URL, if provided, gives a direct link to this resource for further evaluation and use.

## Cell Broadcast

Cell Broadcast (CB) is a robust telecommunications technology designed for delivering emergency alerts to mobile devices within a specific geographical area. It is highly reliable due to its ability to broadcast messages over a dedicated channel within the mobile network, ensuring that alerts are delivered even when networks are congested. Unlike other communication methods, CB messages are prioritised within the network, guaranteeing their delivery during emergencies when traditional channels might fail. Its scalability, efficiency, and independence from user registration make it a key tool in modern public warning systems.

The alert process begins with the Cell Broadcast Entity (CBE), an infrastructure used by authorised agencies to create and manage alerts. The CBE is essentially where alert messages are defined, and the geographical target area, and where parameters such as urgency or duration are set. In some countries, there may be multiple CBEs to accommodate regional authorities, sectoral agencies, or diverse organisational needs. For example, regional emergency agencies may each operate their own CBE to address localised incidents, while national authorities may maintain a separate CBE for large-scale emergencies. In some setups, there is one CBE per mobile network operator (MNO). This model allows each MNO to integrate the alert creation process directly with their own infrastructure, potentially simplifying technical implementation but requiring coordination to ensure consistent messaging across operators.

Once the alert is prepared, it is transmitted to the Cell Broadcast Centre (CBC). The CBC is a critical component of the mobile network infrastructure that receives the alert from the CBE and ensures it is broadcast to mobile devices in the defined area. In centralised systems, a single CBC handles dissemination for all mobile network operators (MNOs) in the country. In decentralised systems, each MNO operates its own CBC, which is fully integrated into their network infrastructure and directly handles broadcasting through their respective cell towers.

The broadcast occurs over a dedicated channel that operates independently of normal network traffic. This makes CB particularly effective during emergencies, as it avoids the congestion that can affect voice and data communications. CB is compatible with all network generations, including 2G, 3G, 4G, and 5G, but the planned phase-out of 2G and 3G in many countries has prompted some authorities to roll out CB systems exclusively on 4G and 5G. These newer network generations offer improved capabilities, including faster transmission and enhanced geofencing accuracy.

When a mobile device receives a CB alert, it displays the message prominently on the screen, often overriding other activities. Alerts are typically concise and may include actionable instructions. To ensure attention, the alert is accompanied by a distinctive sound and vibration pattern, designed to be recognisable even in noisy environments. Many systems allow users to opt out of certain levels of alerts. High-priority messages, such as the so-called “presidential alerts” override user preferences, including opt-outs, to guarantee delivery in critical situations. Modern CB systems may also support silent alerts, which allow authorities to broadcast messages without triggering sound or vibration on devices. This feature is particularly useful in sensitive situations, such as active shooter incidents, where noise could endanger individuals.

## Location-based SMS

Location-Based SMS (LB-SMS) is a widely adopted technology for disseminating public warnings by targeting mobile devices within a specific geographical area. It relies on mobile network operators (MNOs) to identify devices in the target zone using location data, either in real time or based on their last-known location. Once identified, SMS alerts are sent directly to these devices, ensuring that individuals in the affected area receive timely and relevant emergency notifications.

LB-SMS operates across all mobile network generations (2G, 3G, 4G, and 5G), ensuring compatibility with the broadest possible range of devices. However, the delivery mechanism may vary depending on the network. Messages on 4G and 5G networks can either "fall back" to 2G/3G for transmission or be sent over the IP Multimedia Subsystem (IMS). This dual capability ensures continuity, but as many countries plan to phase out 2G and 3G networks, some authorities are focusing on optimising LB-SMS for 4G and 5G to future-proof their systems. An important characteristic of LB-SMS is its dependence on the operator's core network capacity for rapid dissemination.

Once a warning is sent, LB-SMS messages are received on devices as standard SMS alerts. These messages often contain clear, actionable instructions. Their format and appearance are consistent with regular SMS notifications, making them easily recognisable by users. While straightforward in design, LB-SMS alerts are effective for delivering concise emergency information, though they do not include distinctive sounds or visual cues like those associated with Cell Broadcast systems.

LB-SMS systems may also integrate additional functionalities to enhance their effectiveness. For example, information derived from location databases can be used beyond alert delivery to support situational awareness, such as mapping population density in affected areas or monitoring evacuation movements. In some systems, it is also possible to determine whether users use domestic SIM-cards or are visiting roamers, allowing to send different messages to them.
The ability to monitor the status of message delivery provides another layer of operational oversight, ensuring authorities can evaluate the reach and performance of the system. Additionally, LB-SMS systems often support sending follow-up messages, such as "all-clear" alerts, which inform recipients from previous alerts when the danger has passed, even if they have left the alert area.

## Mobile apps

Mobile apps are a flexible tool for public warning, allowing alerts to be delivered directly to users' devices. Their effectiveness depends on widespread adoption, as higher download rates indicate broader reach. Some apps require user registration for personalised alerts, such as for other areas, while others deliver notifications automatically to maximise accessibility.

These apps can operate as standalone public warning platforms or integrate with other services, complementing traditional methods like SMS or Cell Broadcast by offering features such as location-based targeting and multimedia content.

### Sirens

Sirens are one of the oldest and most recognisable tools for public warning, providing audible alerts over large areas. Modern systems often integrate sirens with other public warning channels to enhance coordination. Some are connected to IP networks, allowing for remote activation and monitoring. Sirens can use different sounds to indicate specific types of emergencies, and loudspeakers are sometimes incorporated to broadcast voice messages, offering more detailed instructions. While they lack the precision of digital methods, sirens remain crucial for reaching outdoor populations or areas with limited access to mobile technology.

## SECTION 3: SENDING AN ALERT

This section explores the operational framework for issuing public warnings, focusing on who can access and utilise the system, the steps involved in broadcasting an alert, and the practical considerations for ensuring effective communication.

The ability to send alerts may be restricted to specific authorities at various levels, such as national, regional, or municipal agencies, depending on the country's governance structure. Clearly defining these roles ensures efficient coordination and prevents misuse. The process for sending an alert typically involves creating the message, determining the geographical target area, and broadcasting it through the designated public warning channels.

Language is another critical factor. Messages must be accessible to the affected population, which may require providing alerts in multiple languages to accommodate linguistic diversity. Sending an alert in different messages can be done either within the same alert message or through different alerts.

Pre-defined templates can standardise and streamline the alert creation process, ensuring consistency and reducing delays during emergencies. Finally, the ability to send an "all-clear" message after an emergency reassures affected populations and provides closure.

## SECTION 4: TEST AND TRAINING

Regular testing and training are essential for ensuring the reliability and effectiveness of public warning systems. Tests help identify potential technical issues, measure system performance, and build public trust by demonstrating the system's functionality. These can include public tests, where the population is notified and experiences a real alert scenario, or blind tests, conducted without public knowledge to evaluate the system's backend operations.

Training for authorised users is equally important to ensure they can efficiently create and broadcast alerts during emergencies. Training programmes often include simulations, standard operating procedures, and system updates to keep users proficient.

## SECTION 5: FIGURES ON THE USAGE

This section provides insights into the practical application of public warning systems by examining their usage patterns. Identifying the most common types of emergencies prompting alerts helps contextualise the system's purpose and effectiveness, revealing whether it is primarily used for natural disasters, technological incidents, or other crises.

## SECTION 6: DEPLOYMENT AND MAINTENANCE

Deploying and maintaining public warning systems requires significant investment and ongoing resources. The timeline for implementation, including the first operational use in emergencies, reflects a country's readiness and experience. Maintenance costs, encompassing software updates and network optimisation, highlight the system's financial sustainability over time.

Mobile Network Operators play a central role, not only in broadcasting alerts but also through active participation in governance, such as working groups and testing. Their collaboration ensures the system remains aligned with technological advancements and operational needs. Key industry partners, including broadcasters and software providers, supply the platforms and tools enabling alert creation and dissemination. Transparency in these partnerships and the frequency of tender renewals reflects a balance between innovation and stability. This section offers insights into the resources and partnerships essential for sustaining public warning systems effectively.

## SECTION 7: ELEMENTS RELATED TO THE PUBLIC WARNING DEPLOYMENT

The deployment of public warning systems involves navigating various legal, technical, and collaborative challenges. In addition to complying with the European Electronic Communications Code, countries may face specific legal requirements that influence the design and operation of their systems, such as national data protection laws or sector-specific regulations. These frameworks ensure that systems operate within clearly defined boundaries while safeguarding citizens' rights.

Privacy and cybersecurity are central to public warning deployment. The reception of an alert may sometimes be perceived as privacy-intrusive by the population. Decisions from supervisors or courts may shape how these concerns are addressed, while, ensuring compliance with regulations like the GDPR. Cybersecurity is equally vital, as public warning systems are potential targets for attacks that could disrupt emergency communications or spread false information. Measures such as encryption, robust authentication, and network monitoring are essential for maintaining system integrity.

Cross-border emergencies highlight the need for cooperation between neighbouring countries. Discussion platforms or joint mechanisms allow nations to share best practices, coordinate responses, and align technical standards, particularly in regions where emergencies, such as natural disasters, often span national borders. Such collaboration strengthens the overall resilience of public warning systems.

## SECTION 8: INVOLVEMENT OF COMMUNITIES

Community involvement is essential to ensuring public warning systems are inclusive, effective, and responsive to the needs of all populations. Collecting input from diverse stakeholders, including local networks, high-risk communities, and individuals with specific needs, allows systems to be tailored to regional and societal requirements. A structured framework for gathering these requirements fosters ongoing dialogue and adaptation, ensuring the system remains relevant as community needs evolve.

Special consideration must be given to people with disabilities. Alerts should be accessible across all formats, including visual, auditory, and tactile modalities, to ensure that no one is excluded. For example, systems can integrate features like text-to-speech, vibration notifications, or compatibility with assistive devices.

Finally, understanding whether alert messages reach the entire population is crucial for evaluating a system's equity and coverage. This includes identifying and addressing gaps in coverage, such as regions with poor network access, populations without compatible devices, or communities with language barriers. Ensuring universal reach builds trust and strengthens the overall resilience of the public warning system.

## SECTION 9: OTHERS

This section provides a broader perspective on the public warning system, focusing on additional information, ongoing challenges, and future developments. Publicly available resources, such as official websites or reports, offer valuable insights into the system's functionality, governance, and operational details, making them accessible to stakeholders and the general public.

Scientific studies assessing the system's technical performance, public perception, and trust levels are essential for evidence-based improvements. Such research highlights the system's strengths, identifies areas for refinement, and ensures alignment with public expectations.

Understanding current challenges helps pinpoint barriers to effective implementation, whether they involve technical issues, user adoption, or regulatory constraints. Similarly, planned upgrades reflect the system's adaptability and commitment to innovation, ensuring it remains relevant as technology and societal needs evolve.

# Bulgaria

## GENERAL INFORMATION

**Name of the public warning system:**

BG-ALERT

**Which part of the country is covered by BG-Alert? Are the overseas territories (if applicable) included?**

The whole country of Bulgaria is covered by BG-ALERT.

**From a policy and governance perspective, who has overall responsibility for the public warning system at national level?**

Directorate General "Fire Safety and Civil Protection" (DG FSCP) as part of the Ministry of Interior is responsible for the management of BG-ALERT system.

## PUBLIC WARNING CHANNELS

**Which channels are used for Public Warning?**

Mobile-based channels:

- [x] Cell Broadcast
- [ ] Location-based SMS
- [ ] Registration-based SMS
- [ ] National SMS
- [ ] Mobile app
- [ ] Apps designed for other use

Other channels:

- [x] Sirens (about 50% coverage of the population)
- [ ] Fixed-line alert system
- [ ] Emails
- [ ] Social media
- [x] TV & radio
- [ ] Billboards & public signs

**Are the messages sent in compliance with the Common Alerting Protocol (CAP)?**

- [x] Yes
- [ ] No

**Is your CAP feed (if any) public?**

CAP is not publicly available. However, every cell broadcast message is published to the BG-ALERT website www.bg-alert.bg

## Cell Broadcast

**Is there only one Cell Broadcast Entity for the whole country or are there several entities?**

One Cell Broadcast Entity is used.

**Is there only one centralised Cell Broadcast Centre for the whole country or are there several centres (one per operator or one per region for instance) ?**

One centralised Cell Broadcast Centre is used.

**Does BG-Alert work on all network generations (2G, 3G, 4G, 5G)?**

Yes, BG-ALERT works on all network generations 2G, 3G, 4G and 5G

**Approximately what percentage of mobile devices used in the country are compatible to receive alerts from Cell Broadcast?**

No official data is available.

**Is it possible to send "presidential alerts" (overriding the opt outs)?**

Yes, EU-Alert level 1 is not visible in the devices menu and has no option to opt-out by the users.

**Is there a possibility to opt out of certain levels of alerts?**

Yes, using the devices menu users have the possibility to opt-out for:

- EU-Alert level 2 (Extreme and severe threats)
- EU-Alert level 3 (Information)
- EU-Amber (Missing Person Alerts)

Users have the possibility to opt-in for EU-Monthly test (Test Alerts).

**Can silent alerts be sent (alert sent on the phones triggering no noise, this is a new feature described in the last ETSI technical specifications)?**

No, all the levels of alerts, except Test Alerts, have device override for maximum levels of sound. Test alerts follow the user device settings.

**Is Device-Based Geofencing available?**

Not yet.

## Sirens

**Are sirens integrated within BG-Alert?**

No

**Are sirens integrated with IP networks?**

No information / not applicable

### Do the sirens use different sounds?

Yes

### Are loud speakers used?

Some as part of the sirens

## SENDING AN ALERT

### Who can use the system? Who sends the alert? At what level (e.g. national, regional, municipal...)?

The BG-ALERT system is available for using at municipal, regional and national level.

### What is the process for sending the alert?

Every authority having jurisdiction (AHJ) has two options to create alerts and submit them for approval. The first option is by using the Cell Broadcast Entity (CBE) user interface, whenever the AHJ has available connection to an isolated network, dedicated to BG-ALERT system. In this case a user from the AHJ creates the alert message and submits it for approval. The staff from the Directorate General "Fire Safety and Civil Protection" (DGFSCP) checks for the mandatory message content elements and, if everything is correct, sends it to the public.

The second option, always available to all of the AHJ, is by filling in a template and sending it to DGFSCP via e-mail. In this case the message parameters and content are used to create the alert message. If approved, the message is created and submitted for approval by DGFSCP employee using the CBE. Afterwards, another DGFSCP employee sends it to the public.

### In which languages are messages sent?

Bulgarian and English content inside one message.

### Are there pre-defined templates for the alerts?

Not yet, but we are currently working on it

**Do you generally send an "all-clear" message to users who had received the alert/who are in the alert area after the emergency?**

Not at the moment.

## TEST AND TRAINING

**How often are public tests performed?**

The first public test is scheduled for 1 October 2024.

**How often are "Blind tests" performed?**

No "Blind tests" done so far.

**How are the BG-Alert users trained for sending the alerts?**

Every user passes an initial educational course (1 day) before receiving user rights for sending alerts. All the users will pass periodical educational courses in the future.

**How is the population notified so that they are prepared to receiving the test alerts?**

All the information regarding BG-ALERT system is available at the BG-ALERT web-site www.bg-alert.bg. Before the upcoming tests there will be press releases.

## FIGURES ON THE USAGE OF BG-ALERT

**How many times was BG-Alert used last year (outside of tests)?**

Deployed only in 2024.

**Do you distinguish the figures between alerts and vigilance messages sent?**

Yes, we do. Our concept is to use different types of messages for Information, Threats to life and property and Imminent danger to life or health.

**For which type of emergency are public warning messages the most often sent?**

The BG-ALERT system has been used 3 times for real events since September 2024.

**Any additional relevant statistics?**

Not yet.

## DEPLOYMENT AND MAINTENANCE

**When did Cell Broadcast become operational (first message sent for an emergency)?**

The first message was sent on 25.07.2024.

**What were the costs of deployment of Cell Broadcast/Location-Based SMS?**

There was a public procurement in 2022 and the signed contract price was about € 1,074 million (excluding 20% VAT) for the hardware, the software and 5 years of maintenance.

**What is the yearly cost of maintenance of the system?**

5 years of maintenance are included in the price of the contract.

**How are Mobile Network Operators involved in the governance and operation of the Public Warning system (e.g. existence of a working group, regular meetings…)?**

We have signed a formal agreement for cooperation with all the Mobile Network Operators in Bulgaria.

**List the companies involved in BG-Alert (broadcasters & software providers).**

Broadcasters – A1, Vivacom and Yettel
Software providers - Opencode Systems (CBE, CBC) and InfoSystems International (system integrator)

**How often are tenders renewed?**

There are about 4 years maintenance left, included in the signed contract.

## ELEMENTS RELATED TO THE PUBLIC WARNING DEPLOYMENT

**Are there specific legal requirements to comply with (other than the European Electronic Communications Code)?**

DIRECTIVE (EU) 2018/1972 was implemented in Bulgarian Electronic messages Law in 2021. In 2023 the requirements were modified and an additional ordinance had to regulate the order for deployment, maintenance, development and use of the BG-ALERT system. Ordinance № 81213-413 from 29 March 2024 for deployment, maintenance, development and use of the BG-ALERT system for distribution of public warning messages is in force since 9 April 2024.

**How were privacy concerns addressed? Has there been any decision from data protection supervisors/courts?**

Cell Broadcast is compliant with the General Data Protection Regulation as mobile phone numbers are not required by the Cell Broadcast technology.

**How are cybersecurity concerns addressed?**

The BG-ALERT system is available only from an isolated government network. This network has no connection to internet. Every person who has user profile must pass an educational course and provide e-mail and phone contacts. Every message submitted for approval has to be confirmed by the person who created it by a phone call from the phone number provided.

**Is there any cooperation mechanism/discussion platform with neighboring countries regarding public warning?**

Not yet.

## INVOLVEMENT OF COMMUNITIES

**Do you have a specific framework in place to collect requirements from different stakeholders, such as local networks, people with specific needs, high-risk communities...**

Not yet.

**Are there specific considerations for people with disabilities?**

As far as Cell Broadcast messages are concerned, we rely on the user devices and their capabilities to serve their owners.

**Are you aware whether the alert messages reaches the entire population?**

We certainly know that there are people using older devices which are not compatible with the Cell Broadcast technology.

## OTHERS

**Where can we find additional information about BG-Alert?**

BG-ALERT website (available only from Bulgaria):
https://bg-alert.bg

Ordinance № 81213-413 from 29 March 2024 (in Bulgarian):
https://lex.bg/bg/laws/ldoc/2137241924

**Were any scientific studies done on BG-Alert?**

No scientific studies so far.

**Are you facing any specific challenge now related to the use of Public Warning?**

We have not much experience in using the BG-ALERT system, so no specific challenges so far.

**Is there any upgrade planned for the next years?**

We are planning to make Device-Based Geofencing available.

**Any story to share? (person saved thanks to the warning, case of misuse...)**

We have not much experience in using the BG-ALERT system, so nothing to share so far.