# Protection of Underground Electronic Communications Infrastructure

*The use of automated information system for damage prevention against civil work*

December 2014

European Union Agency for Network and Information Security www.enisa.europa.eu

## About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

## Author

Dr. Cédric Lévy-Bencheton

## Contact

For contacting the author please use resilience@enisa.europa.eu.

For media enquires about this paper, please use press@enisa.europa.eu.

## Acknowledgements

For the completion of this document, ENISA would like to acknowledge all participants to the study (by alphabetical order):

**Carolin Groot** (KLIC/Kadaster), **Rita Hammarstedt** (Ledningskollen/PTS), **Pieter Noens** (KLIP/AGIV), **Jörgen Nordman** (Ledningskollen/PTS), **Henrik Ravn Lager** (LER/MBBL), **Henrik Suadicani** (LER/MBBL).



Catalogue number: TP-04-14-977-EN-N ISBN: 978-92-9204-104-5 DOI: 10.2824/3762

## Executive summary

Information exchange on the Internet is possible thanks to a physical infrastructure composed of network equipment and cables, such as fibre optics. The majority of these cables are usually laid underground, for esthetic reasons and to improve their security.

In the last years, ENISA has noticed a large amount of Internet outages due to cable cuts. The source cause can be linked either to malicious actions or to accidental (unvoluntary) events. Thus, a fair amount of unvoluntary disruption can be attributed to underground excavation performed during a civil work, due to a lack of information regarding the presence of underground cables at the dig site.

Certain Member States (MS) of the European Union – namely Belgium, Denmark, France, Netherlands, Sweden, and the United Kingdom – have developed specific tools to prevent the disruption of underground electronic communication infrastructure. These tools, whose use can be either mandatory or voluntary, foster the collaboration between infrastructure owners and excavators: infrastructure owners can declare their underground assets and share the information with the excavator before any planned civil work.

This document analyses existing initiatives deployed by selected MS. Information collected through a survey is analysed to understand the choices made for the development and management of such tools, the technical implementation, the operational usage of the tool, its financing, and security aspects linked to the misuse of information. In particular, confidentiality is a key parameter that need to be tackled before launching any new initiative.

The document then explores the advantages of an automated information exchange tool in the protection of underground infrastructure. It summarizes the principle results found during the survey and explores possible improvement and future developments.

This document aims to provide recommendations to Member States (MS) that wish to protect their underground electronic communications infrastructure against disruption due to civil works. This document shall help MS to assess their need to deploy an automated information system for damage prevention, and eventually assist them in the development of such tool through the following recommendations:

- MS should analyse the reasons behind cable cuts
- MS should evaluate the benefits of an automated information exchange tool to protect underground infrastructure
- MS developing an automated information exchange tool should rely on existing tools and experience
- All stakeholders need to collaborate to define the principles of the automated information exchange tool to protect underground assets
- MS should promote the use of their automated information exchange tool to protect their underground infrastructure
- MS should evaluate the security policy for operating and managing their automated information exchange tool
- MS should evaluate the sustainability of their automated information exchange tool

Finally, this document emphasizes how automatic information exchange tools are a valuable tool to protect underground electronic communication infrastructure against outages due to digging.

# Table of Contents

# 1 Introduction

Nowadays, electronic communications (eCom) are expected to be always available (e.g. telephony, Internet access…). Network access can be vital for the proper operation of services of high importance. For example, access to emergency services, energy, utility SCADA network…

Damages caused to the network infrastructure (such as cables, ducts, manholes, masts, towers, in-building installations) is a cause of unwanted disruption of electronic communications services. In its previous Annual Incident Reports[1] (from 2011 to 2013), ENISA has identified cable cuts as one of the most frequent causes of outage in public electronic communications networks or services in the EU.

Cable cuts can occur due to intentional human activities such as stealing of cables for metals, sabotage act, terrorist attacks, etc. However, it should be pointed out that the majority of such incidents happens unintentionally, as a result of human error (in most cases a third party is involved). Cable cuts often occur during civil works due to the fact that excavators usually do not possess sufficient information about the existing underground infrastructure and/or about the exact location of underground assets in the area of civil works.

## 1.1 Scope of the document

Several Member States of the European Union (hereafter – MS) have launched initiatives to protect their underground assets, in order to prevent any disruption due to civil works. These MS have deployed information systems to facilitate timely exchange of information about the existing underground infrastructure between underground infrastructure owners and excavators.

This study investigates a selection of existing initiatives across the European Union (EU). It analyses experience and good practices of the MS that are using such a tool. The scope of this document is to understand how deployment of an automated information system can protect underground electronic communications infrastructure, and provide guidance accordingly.

This guide on *Protection of Underground Electronic Communications Infrastructure* is one of the deliverables (Work Package 3.2 – Deliverable 1) foreseen in the ENISA Work Programme 2014 under the Work Stream 'Support cooperation"[2]. It provides an analysis of annual 2013 incident reports and provides recommendations on addressing significant incidents linked to cable cuts.

## 1.2 Target audience

The main target audience of this document are Member States which would like to deploy an automated information system to prevent damages due to civil work on the underground electronic communication infrastructure.

The document is written for decision makers and public institutions in charge of defining functionalities of such information systems and/or developing technical specifications (ex: NRAs, ministries responsible for electronic communications…).

Moreover, this document may be of interest for the owners of underground electronic communications assets, not limited to telecom providers (governmental, public and private organizations may also possess underground cables). Civil work enterprises can also get an overview on their role, as they should actively contribute to the protection of the underground infrastructure.

[1] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports

[2] ENISA Work Programme 2014, http://www.enisa.europa.eu/publications/programmes-reports/work-programme-2014, in particular, pp. 43-44

## 1.3 Methodology

The primary sources of information for this document are desktop research activities and interviews with experts from MS that already have, or are planning to have in the near future, an information system for underground infrastructure damage prevention (Belgium, Denmark, Estonia, Netherlands, Sweden). For that purpose, the study uses the questionnaire presented in Annex A.

In order to consolidate findings, additional interviews have been carried out with experts from MS organizations operating electronic broadband infrastructure mapping projects and with experts in infrastructure mapping and cable protection from four MS institutions (Belgium, Denmark, Netherlands, Sweden) operating such systems and from relevant legal acts of Member States (cf. References).

The methodology aims at understanding how such an automated information system can help in protecting underground infrastructure. For that purpose, the answers from the interviews have been compiled under different topics in order to understand the choices made in existing tools. For each topic, the reasons behind these choices are analysed. The characteristics shared by existing tools and their differences are also highlighted. The interviews also provide an overview on current challenges and future evolutions, from the perspective of the entity managing the tool.

## 1.4 EU Policy

Article 13a, from Directive 2002/21/EC of the European Parliament and of the Council[3] on a common regulatory framework for electronic communications networks and services as amended by Directive 2009/140/EC of the European Parliament and of the Council[4], requires that "Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services […] and […] take all appropriate steps to guarantee the integrity of their networks, and thus ensure the continuity of supply of services provided over those networks". Thus, the provisions of Article 13a of Framework Directive are fully applicable to protect the underground infrastructure of electronic communications networks. For that purpose, the use of an automated information system to protect underground infrastructure can be considered as a measure to fulfil the requirements of Article 13a of Framework Directive.

The second EU legislative act in relation with the subject investigated in this document is Directive 2007/2/EC of the European Parliament and of the Council[5] establishing an Infrastructure for Spatial Information in the European Community (INSPIRE[6]). The aim of the INSPIRE Directive is to create a spatial data infrastructure to support EU environmental policies and policies or activities which may have an impact on the environment. The goal is to help make spatial or geographical information more accessible and interoperable for a wide range of purposes supporting sustainable development.

The INSPIRE Directive establishes rules and conditions related to the creation of infrastructures for spatial information operated by the Member States for collecting, storing, accessing and sharing spatial information in a digitalized format. Spatial data of utility facilities are under the scope of the INSPIRE Directive; sewage, waste management, energy supply and water supply are clearly listed in Annex III of the INSPIRE Directive. Though it was proposed to include electronic communications

[3] http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/140framework_5.pdf
[4] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF
[5] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2007:108:FULL&from=EN
[6] http://inspire.ec.europa.eu

infrastructures into the INSPIRE Directive, at this moment, it is out of this legislation: the majority of Member States do not apply the INSPIRE provisions to map electronic communication infrastructure.

However, the INSPIRE Directive includes useful aspects concerning data collection and publication. A few MS are thinking about integrating these aspects into their projects for underground electronic communication infrastructure protection. For instance, the Belgium Flemish Region's information system for underground infrastructure protection will utilize INSPIRE provisions regarding underground infrastructure spatial data presentation.

## 1.5 Outline of the document

The structure of the document is as follows:

Chapter 2 details the existing initiatives in the EU and analyses them from several point of view: development and management, technical implementation, operational usage of the tool, financing, and security aspects linked to the misuse of information about underground infrastructure.

Chapter 3 analyses the survey. It focuses on the advantages of the tools, the main results withdrawn from the survey and explores possible improvements and future developments.

Chapter 4 proposes a list of recommendations toward Member States who are considering the deployment of an automated information exchange to protect their underground electronic communication infrastructure, and for stakeholders interested in such tool (infrastructure owners, civil workers…).

Chapter 5 concludes.

## 2 Overview of existing initiatives

All MSs regulate civil works by relevant rules/legal acts in order to protect public interests and individual rights, such as environment and ground resource protection, existing property protection, etc. Any entity intending to perform the civil works on/under the soil should follow these rules.

In most cases these rules require obtaining relevant permissions which are usually granted by public authorities and/or private entities possessing the land and/ or infrastructure on/under/above the land where civil works will take place. These rules are often laid down in several legal acts and in order to be authorized to perform civil works in a certain land area, the entity should apply to several public authorities and private entities for the relevant permissions. For example, owners of underwater cables are required to declare the location of their cable if they pose a risk to shipping.

This process is often time-consuming, since it is required to collect all the relevant information from land/infrastructure owners, as well as the information about all applicable terms, conditions and restrictions, which delays civil works. Any measure facilitating the receipt of timely and reliable information about underground infrastructures should reduce the delays of civil works and administrative burden.

Thus, for these purposes some MS have established "one-stop" application procedures to issue all the permissions and provide all the related information (e.g. terms, conditions and restrictions) for civil works. Desktop research revealed that several MSs implement automated information systems whose primary purpose is underground infrastructure protection. Table 1 presents the name of the tool and the entity managing the tool for the following MS: Belgium, Denmark, France, Netherlands, Sweden, and the United Kingdom.

| | Name of the tool | Entity managing the tool |
|---|---|---|
| **Belgium (Flanders)** | KLIP[7] | AGIV (*Flanders Geographical Information Agency*) |
| **Denmark** | LER[8] | MBBL (*Ministry of Housing, Urban and Rural Affairs*) |
| **France** | Construire sans détruire[9] | INERIS (*National competence centre for Industrial Safety and Environmental Protection*) |
| **Netherlands** | KLIC[10] | Kadaster (*Cadastre, Land Registry and Mapping Agency*) |
| **Sweden** | Ledningskollen[11] | PTS (*Swedish Post and Telecom Authority*) |
| **United Kingdom** | Dial Before You Dig[12] | Openreach (for eCom) and National Joint Utility Group (multi-sector coordination) |

**Table 1 – Some Member States with automated information systems to protect underground infrastructure**

[7] http://klip.agiv.be
[8] http://ler.dk
[9] https://www.reseaux-et-canalisations.ineris.fr
[10] http://www.kadaster.nl/klic
[11] https://www.ledningskollen.se
[12] http://openreach.co.uk/orpg/home/contactus/avoidingnetworkdamage/protectingnetwork/networkprotection.do

Such automated information exchange tools may share similarities with infrastructure mapping projects[13]. Yet, they can act as an enabler toward the development of a tool for the protection of underground eCom infrastructure.

Table 1 may not be exhaustive, due to a lack of publicly available information on the subject. Moreover, several initiatives may currently be under development in Member States not referenced in this document. Thus, the reader is encouraged to communicate to ENISA information about systems and initiatives not covered in this document.

## 2.1 Development and management

Interviews revealed that currently operating automated information systems in MS for underground infrastructures protection (hereafter – information systems) are managed by public institutions, though a few respondents indicated that, before launching these information systems, there existed private sector initiatives (systems) for sharing information held by infrastructures owners about underground infrastructures. Respondents also mentioned that those private sector initiatives based on information systems operated quite well, but, as a second step to improve underground infrastructures protection, MS established new systems operated by public institutions.

These systems were launched at about the same time in all interviewed MS – in the second half of the first decade of the 21st century (ranging from 2005 to 2009). This is probably due to the fact that by that time MS already had finished digitalisation of their maps and the availability of digital maps were the prerequisite for the development of information systems intended for excavators and underground infrastructures owners. Indeed, all respondents highlighted that a Land Registry digital map is a core element of their systems (national cadastre offices possess national digital maps, that can be obtained for a fee).

Information systems have been operated by various types of public institutions:

- By the national cadastre offices for one respondent (Netherlands),
- By an agency responsible for the development of the Geographical Data Infrastructure, that realizes solutions for other government agencies, businesses and citizens, for one respondant (Belgium),
- By the electronic communications NRA for one respondent (Sweden),
- By a ministry not responsible for electronic communications for one respondent (Denmark).

Three of the four interviewees responded that their systems had been established and operated following dedicated legislative acts, which also defined their institutional tasks and responsibilities concerning the management of those systems (DK, BE, NL). One of the four respondents pointed out that the information system had been launched and operated not subject to any legal act (SE). That project initially was driven by the general objective to strengthen critical infrastructure protection; for that purpose, the interviewee highlights their very important decision to launch an early and broad call for all stakeholders to get involved.

Table 2 compares the advantages of the structure and the challenges to overcome depending on the type of organization managing the system.

[13] http://www.broadbandmapping.eu/wp-content/uploads/2014-03-24_Broadband-mapping-study-draft-final_report_v01.pdf

| | Done in... | Advantages | Challenges to overcome |
|---|---|---|---|
| **National cadastre office** | 2 MS | • Direct access to the maps and characteristics of the land<br>• Cross-sector approach | • Requires a good knowledge of specific sectorial needs |
| **Electronic Communication National Regulatory Agency** | 1 MS | • Knowledge of incidents related to cable cuts<br>• Aware of the needs of the electronic communication sector | • May need to buy maps if no other option available<br>• Communication with other sectors may be difficult/out of mandate |
| **Ministry not responsible for electronic communications** | 1 MS | • Cross-sector approach<br>• Possibility to create adapted laws | • May need to buy maps<br>• Requires a good knowledge of specific sectorial needs |
| **Independent supervising entity, not regulating electronic communications** | Not investigated in the interviews | • Coordinator between specific sectors<br>• Possibility to enforce similar functionalities across different sectors | • Particular sectorial needs may not be prioritary |

**Table 2 – Advantages and challenges to overcome depending on the type of organization managing the system**

## 2.2 Technical aspects

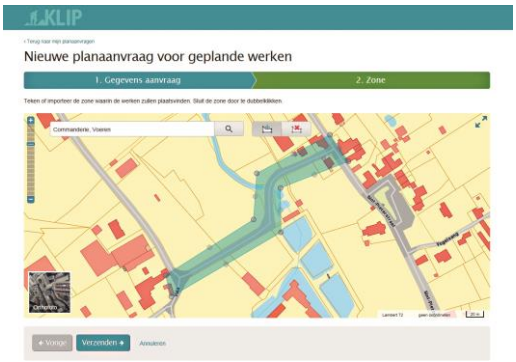
### 2.2.1 General aspects and functionalities

All interviewed MSs use a common approach for underground infrastructure protection and their information system architectures are very similar, the implementation details of these systems are different.

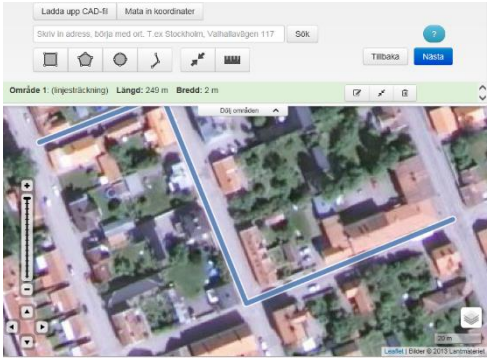
All MSs investigated have launched web-based portals which provide a single application for the receipt of all the relevant information and permissions for civil works. These different applications share common functionalities:

- Infrastructure owners can declare their underground assets and contact information through the Internet. They can be informed of planned civil work in areas where they declared underground assets.
- Excavator accesses system via Internet, registers with it providing contact information, and, using graphical interface tools, draws on a digital map the area where he intends to perform excavation or other kind of ground works.

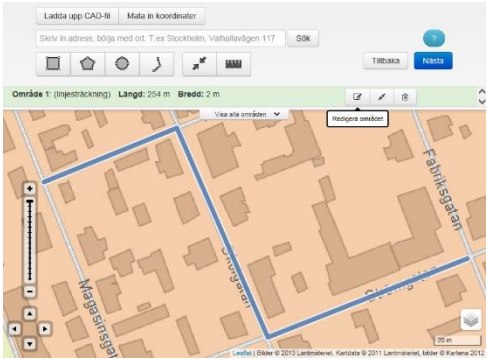
Figure 1 presents the web interface used by a) KLIP (BE) and b), c) Ledningskollen (SE) . Such an interface is usually very intuitive in order to facilitate the usage of the tool by non-expert users. In Ledningskollen, users can choose between two views: orthophoto or cadastral map. During the interview, it was explained that users prefer the orthophoto view, which makes it easier to distinguish landmarks.




**a) Map view in KLIP (BE)**




**b) Orthophoto view in Ledningskollen (SE)**




**c) Cadastral map view in Ledningskollen (SE)**

**Figure 1 – Web-based interface of a) KLIP (BE) and b), c) Ledningskollen (SE) with two different views,**

### 2.2.2 Development of the tool

Interviews revealed that MS information systems were developed utilizing a large variety of software. Due to the complexities of such systems, every tool investigated runs several different software programmes. Indeed, such a system consists of a web-based portal containing graphic data (digital map), a database of underground infrastructure owners, user access interfaces, user authentication…

Respondents pointed out that they utilized several kinds of software: commercial, open source, home made. Graphical data formats vary as well. Some information systems utilize raster graphical presentation method, whereas others employ vector methods.

The survey highlights several constraints to consider before and during the deployment of the tool:

- Respondents indicate that it is important to agree among all stakeholders on information system functionalities and data formats to provide to and retrieve from the information system.
- All respondents pointed out the importance of the system to be user-friendly. To achieve this, all owners continuously upgrade their systems, implement new functionalities which save end user's time, provide a more clear information, enable access for devices with all kinds of operational systems, including mobile devices.
- All respondents highlighted that final decisions on data formats and other terms and conditions of provision of information about underground infrastructures to information system was done after intensive consultations with all stakeholders (programmers, system owners, underground infrastructure owners, excavators, public organizations and institutions).
- In order to minimize manual work required to upload/download to/from information systems, institutions operating these systems have been developing/upgrading application programming interfaces (APIs). For example, underground infrastructure owners, utilizing

APIs, connect their Geographical Information System (GIS) to information system for underground infrastructure protection which allows to automatically update information system database with the updated data from the GIS of infrastructure owner or enables to generate fully automatically responses to excavators requests to provide information.

## 2.3 Operational usage of the tool

### 2.3.1 Purpose of the tool

Considering that automated information systems are currently the most advanced systems which significantly contribute to underground infrastructure damage protection, this chapter overviews the examples of such systems already operating in a few MSs. In the investigated cases, the demand for such systems were put forward by various stakeholders including underground infrastructure owners, excavators, governmental institutions, and municipalities.

It should be noted that interviewed respondents confirmed that their owned automated information systems had been developed for the primary purpose of reduction of the number of underground infrastructures damages. Their systems cover all kinds of underground assets: utility facilities such as sewage, waste management, energy supply, water supply and electronic communications infrastructures such as cables, pipes, ducts, and manholes.

Hence, such tools provide an automatic way to identifiy owners of underground infrastructure in areas of planned civil work and protect underground infrastructure by providing:

- To the excavator: the list of infrastructure owners with underground assets in areas of planned civil works.
- To underground infrastructure owners: notifications of planned civil work in areas where they possess underground infrastructure.

### 2.3.2 For underground infrastructure owners

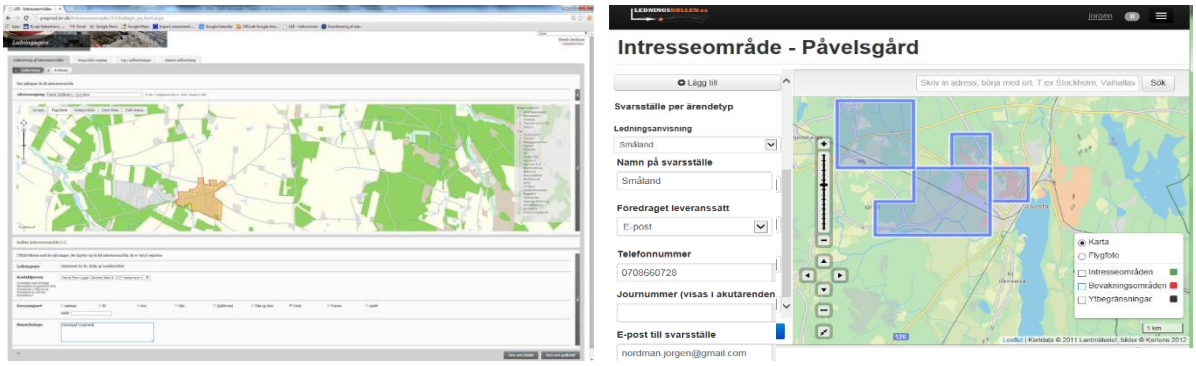
As mentioned above, digital maps with databases, which contain information about underground infrastructure and their owners (including contact information) are key elements in the currently operating information systems dedicated for underground infrastructure damage prevention.

In most cases, legislative acts oblige infrastructure owners to provide data about their underground assets to information systems. Legal acts describe who, what, when and how this should be provided:

- According to some MS legislations, every private or public organization that possesses underground cables and pipes has to provide the information about areas with cables and pipes (BE, NL).
- A respondent from one MS indicated that the provision of information about underground infrastructure to information system is obligatory only for legal entities.
- In certain cases, privately-owned last mile lines placed in a private land are excluded from the scope of legislation (DK).
- Legal acts also provide other exclusions, for example, military and police underground assets are out of scope of legal acts (DK, BE).

On the other hand, one interviewed MS uses a voluntary approach for infrastructure owners to join the information system and finds this approach successful (at this moment more than 600 underground infrastructure owners have joined the system. It was also noticed that more than 100 new owners join the system each year)(SE). However, the respondent pointed out that there are a lot of small infrastructure owners that still have not joined Ledningskollen due to several possible reasons. One reason could be that such infrastructure owner only possess a small amount of underground fibre

optic in rural areas, and therefore think that they can notice and have control of everyone trying to dig in the area.




**a) LER (DK)** **b) Ledningskollen (SE)**

**Figure 2 – Declaration of underground assets by the infrastructure owner**

Figure 2 presents the interface of a) LER (DK) and b) Ledningskollen (SE), used by infrastructure owners to declare their underground assets in a pre-defined geographical area. Information stored by the system include the geographical area and the details of the contact person for this area.

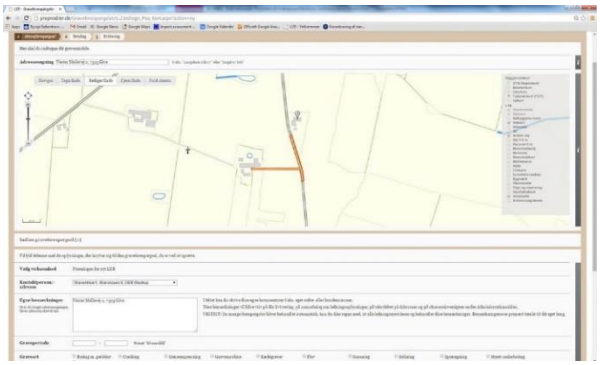
### 2.3.3 For civil workers

Employing these systems, excavators have the possibility to send requests via the Internet to obtain information about the existing underground infrastructure in the area of the planned civil works, including information about its owners. Excavators define the area of planned civil works on a map and the system performs the following actions:

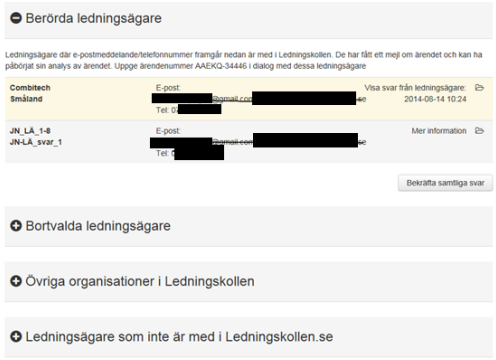
- The systems automatically identify underground infrastructure and its owners within the area demarcated for planned civil work
- Excavators receive the information about underground infrastructure locations.
    - In some cases, this information is directly available in digital maps via the same information systems.
    - In other cases, excavator and infrastructure owners establish a direct contact to protect underground assets, either by exchanging maps or via other mean (for example, by requesting infrastructure owners to participate in excavation works in order to show or mark their underground infrastructure on site).
- Excavators also receive (via the Internet) a permission to perform civil works together with all relevant information and restrictions, including information and restrictions regarding the protection of existing underground infrastructure. Such permission can be transmitted either directly by the system or by the land owner after evaluation of the requirements.

In three of the four MS studied, excavators are obliged by legal acts to submit requests to information systems before starting excavation. In one MS, excavators voluntary use the information system. Civil work projects request for a permission to dig by attaching the required information and documents within a period defined by law (when applicable).

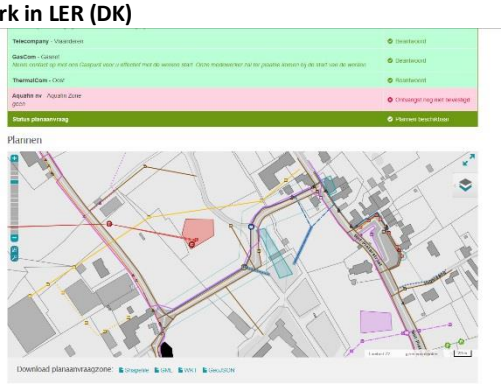
When voluntary, excavators have an incentive to use the system to demonstrate insurances that they have taken all precautions to avoid cable cuts. For example in Sweden, insurance companies are aware of Ledningskollen. The respondent incitates insurance companies to ask if excavators have used the tool before digging, when handling a claim. The interview showed that some insurance companies already do it.



**a) Declaration of civil work in LER (DK)**




**b) Information on asset owners in Ledningskollen (SE)**




**c) Information on asset owners in KLIP (BE)**

**Figure 3 – Declaration of civil work by excavator in a) and the resulting information retrieved in b) and c)**

Also in Sweden, the largest telecom operator of the country has decided to use Ledningskollen as the only way to get information about their cables. Since this operator possess cables in the whole country, it amplifies the need to use Ledningskollen.

In both cases, excavators enjoy benefits of having a single point to contact underground infrastructure owners and intensively use these information systems. For example, in 2013 there were more than 200 000 requests in BE Flemish Region, 115 000 excavators requests in DK, 520 000 request in NL, 135 000 requests in SE.

Figure 3 presents the interface of a) LER (DK), b) Ledningskollen (SE) and c) KLIP (BE) used by excavators to declare their civil works in a pre-defined geographical area. For that purpose, excavators can draw the geographical area of their planned digging directly in the tool, as presented in Figure 3 a). The system returns a list of infrastructure owners with declared underground assets in the area, as depicted in Figure 3 b) and c).

### 2.3.4 Process of data exchange

The entire process of data exchange is not always fully automated. In some MS, the excavator needs to contact the infrastructure owners identified by the tool in order to request information.

Indeed, three of four interviewed respondents pointed out that underground infrastructure owners provided detailed information about existing underground infrastructures directly to the excavator, without using the information system, as presented in Figure 4.

One respondent indicated that, for every single excavator's inquiry, their system (NL) automatically collects digital data about underground infrastructures in the requested area, draws the exact underground infrastructure locations on a digital (topographic) map, and stores this file in its memory until excavator retrieves it. This process is presented in Figure 5.

As a result, in most cases the file with information about underground infrastructure in the area of interest of the excavator can be promptly retrieved (in average, within 1 hour). Future developments aim at optimizing this process by allowing infrastructure owners to automatically provide detailed information about their assets directly from their GIS system.

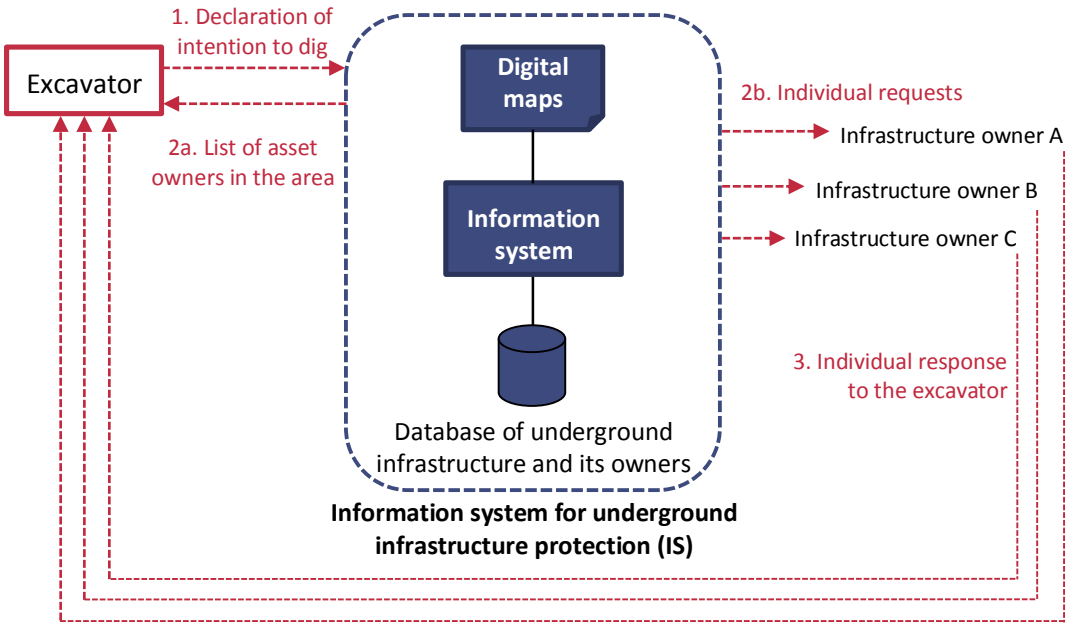



**Figure 4 – Process of information exchange: case when infrastructure owners provide information directly to excavator**

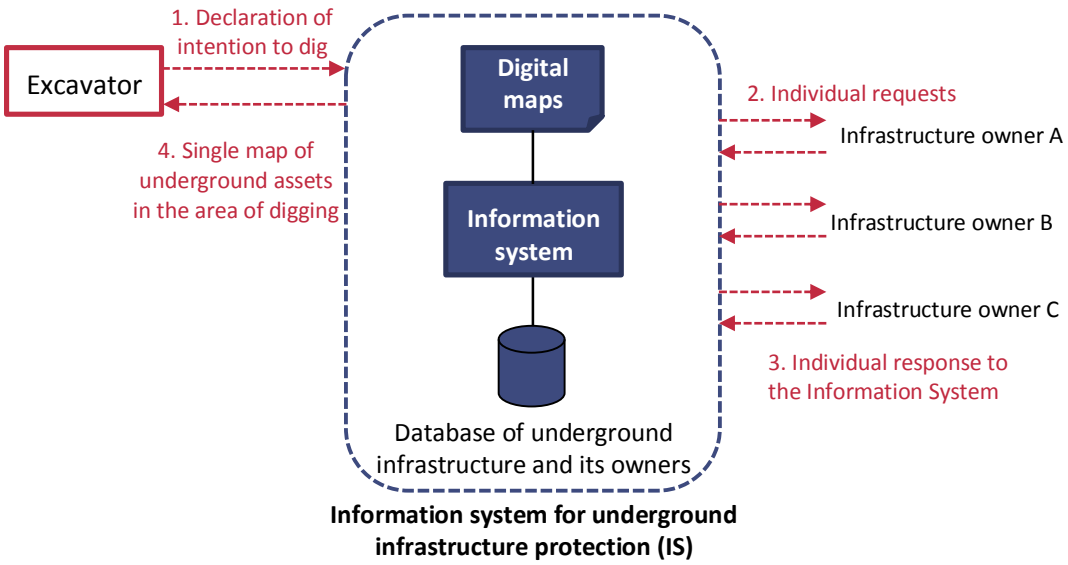



**Figure 5 – Process of information exchange: case when information system provides digital maps to excavator**

### 2.3.5 Timeline of declaration

The maximum period of time within which infrastructure owners should provide detailed information on their underground assets is defined by legislative acts or, in the case of a voluntary system, set by the infrastructure owners individually. This maximum period is determined so that infrastructure owner can provide accurate data without impeding the planning of a civil work project. In existing approaches, it varies between a few days (5 to 10) to a few weeks. For example, this limit is set to 15

working days in BE. Nevertheless, all respondents indicated that in the majority of cases, infrastructure owners respond to the excavator within a significantly shorter period of time (mainly within one day).

All respondents indicated that they used measures to ensure that their systems background digital maps and databases with information about existing underground infrastructures were timely updated. They indicated that an annual update of background digital maps was sufficient, but information about a newly built underground infrastructure or a change of infrastructure owner, or changes in the owner's contact details should reach systems databases without delay in order to ensure that excavators obtain correct information. Infrastructure owners which have their own GIS systems manage to perform these updates automatically. One MS legal act obliges to provide such updated information within 14 days (DK).

Figure 6 details the timeline of this declaration process. Particular attention must be given to any change operated by the infrastructure owner in the period between the information exchange and the actual civil work (new assets, new declaration…). Indeed, only accurate and reliable data can protect underground infrastructure.

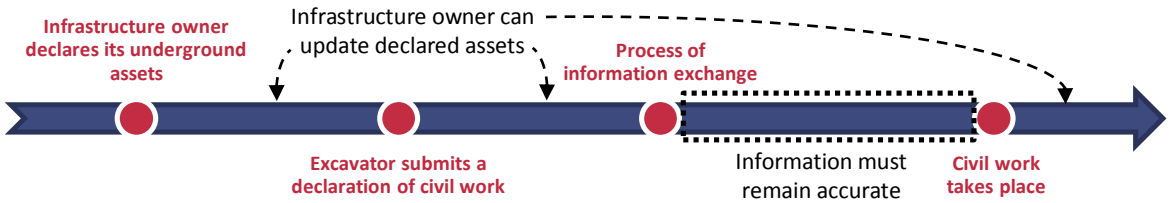



**Figure 6 – Timeline of the declaration process**

### 2.3.6 User support

All respondents mentioned that user support means had been implemented in their information systems:

- All institutions interviewed handle user support via e-mail.
- Some provide on-line available manuals, wizards, tutorials on how to use their systems(including films hosted on public video sharing platforms).
- Some institutions have telephone inquiry services with dedicated personnel in order to provide information to excavators and infrastructures owners how to use of their information systems. Moreover, some institutions may limit their support via telephone by calling back users who contacted their support via e-mail or another mean (SE).

## 2.4 Financing

Development of three information systems were financed by governments (in the case when those information systems were defined by legal acts). One information system was financed by public institutions (electronic communication NRA, Transport Administration, and the National grid).

All respondents of institutions which already had operational information system indicated that they did not apply for EU funding for their system development, but one MS institution intending to develop such a system pointed out that it had recently applied for the support from EU structural funds (EE).

Interviews revealed that models of defrayment of operational expenses of information system could be divided into two types. In one case operational expenses of the information system are covered by excavators by charging them for utilizing this system. In the second case these expenses are covered by governments.

Moreover, institutions, which operate information systems and which charge fees to excavators, use different fee calculation approaches. One approach is to impose a fixed fee for every single inquiry to the information system. The other approach is to charge a fee depending on the area requested for information about underground infrastructure. In this case excavator pays fixed tariff for every square meter of the area which he requests information about.

Table 3 compares the advantages and challenges to overcome for the financing schemes covering operational expenses in Member States with existing tools.

| | Usage | Advantages | Challenges to overcome |
|---|---|---|---|
| **Free** | 2 MS | • Good incentive to use the system | • Requires funding from one or several entities to guarantee the operation (ex: government…) |
| **Price depending on the surface area of the digging** | 1 MS | • Possibility to propose a fair price adapted to the type of digging<br>• Possibility of a self-financed system | • Possible loss of revenue when "gaming the system": excavators request only maps for the start and the end of their digging<br>• Potential risk for security if excavators interpolate cable path when "gaming"<br>• Requires additional security for payment processing |
| **Fixed price per request** | 1 MS | • Possibility of a self-financed system<br>• Price not linked to the size of digging: "gaming" is difficult | • Requires a certain amount of users<br>• Requires additional security for payment processing |
| **Mix of different financing schemes** | Not investigated in the interviews | • Possibility to mix several types of financing schemes or to adapt the price depending on the request (size of the enterprise, area of digging, number of requests per year…) | • Potential possibility to exploit the system to use the cheapest scheme<br>• Some information may not be available in certain schemes |

**Table 3 – Comparison of the different financing schemes used to support operation of the system**

## 2.5 Security measures to minimize risks of misuse of information about underground infrastructure

All respondents pointed out that information about underground infrastructure is sensitive in terms of confidentiality (public security or business secrets). Particularly, access to precise data with its exact location and information about its infrastructure owners, need to remain private for infrastructure owners. Thus special measures were implemented in their information systems in order to avoid their use for malicious purposes (such as business espionage, sabotage acts, terror attacks).

### 2.5.1 Authentication and access control

All respondents indicated that one of such measures utilized in their systems was admission control:

- Any system user has to be authenticated to declare their assets. The request for information may also require authentication (this is the case in all cases investigated).

- Access to the information system is organized in different ways. Some systems require user's registration and provides user's account with password, others use a public security system with certificates.
- Users register themselves for a specific user profile (asset owner, civil worker…). Access to functionalities is granted according to the rules defined in system.
- Through access control rules, the system adapts its interface and functionalities to the role of the user (underground infrastructure owner or requester…).

### 2.5.2 Granularity of information

All respondents also highlighted a second security measure to limit the granularity of information stored. Namely, their information systems contain only approximate locations of underground infrastructure and contact details of underground infrastructure owners to ensure confidentiality:

- The requesters obtain only limited information about the underground infrastructure and its owner in the area of digging. Infrastructure owners have the information about the exact locations of their underground assets in their GIS or, for example, paper maps.
- Infrastructure owners receive a request from the information system to provide information about their assets in a particular territory to an identified requester. They may disclose information only under agreed terms and conditions. Thus, even in case of a leak of information from information system, the exact locations of underground infrastructure shall remain private.

In the case of the fully automated system investigated, the information system stores files with the exact locations of underground infrastructure until the excavator retrieves it. The maximum storage period of this file is limited (here, 20 working days). When this period expires, the files are automatically deleted from the system's memory.

### 2.5.3 Other security measures

Finally, respondents pointed out that special attention was paid to IT security during their information system development (programing), use and maintenance phases in order to minimize security breaches.

## 2.6 Summary of usage for four existing tools

Table 4 summarizes the responses at the interviews related to the usage of four tools: KLIC (NL), KLIP (BE), Ledningskollen (SE) and LER (DK). This table does not compare the solutions from a qualitative point of view, since every approach is adapted to the particularities of a Member States and the needs of stakeholders.

Members States that wish to deploy such tool may rely on this table to investigate these existing tools. The goal is to help them understand and validate functionalities and usages of a possible future system.

| | KLIC (NL) | KLIP (BE) | Ledningskollen (SE) | LER (DK) |
|---|---|---|---|---|
| **Project launch date** | 2008 | 2007 | 2010 | 2005 |
| **Infrastructure owners in the system** | 1 000 | 300 | 600 | 3 700 |
| **Number of requests in 2013** | 520 000 | 195 000 | 135 000 | 115 000 |
| **Number of excavator declared** | 15 000 companies (can represent multiple users) | 2 000 companies (can represent multiple users) | 24 500 companies (can represent multiple users) | 2 200 companies (can represent multiple users) |
| **Legal aspect** | Mandatory declaration:<br>• Infrastructure owners<br>• Excavators | Mandatory declaration:<br>• Infrastructure owners<br>Excavators | Voluntary usage:<br>• Infrastructure owners<br>• Excavators | Mandatory usage:<br>• Infrastructure owners<br>• Professional excavators |
| **Private individual use possible?** | Yes | Yes | Yes | Yes |
| **Average delay of answer** | 1 hour to 2 days | A few days | 1 to 5 days | 1 to 5 days |
| **Fine for infrastructure owners not declaring** | ~50 000 € to 280 000 € | 50 € to 100 000 € | - | - |
| **Financing of the development stage** | Excavator requests | State funding | Public institutions | State funding |
| **Financing of the operational stage** | Excavator requests | 2014: State funding<br>1/1/2016: Excavator requests | Public institutions | Excavator requests |
| **User fee per request** | ~21,50 € | 2014: Free<br>1/1/2016: 10 € | Free | ~12 € average |
| **Support offered** | • E-mail (contact form)<br>• Online help<br>• Customer service online contact | • Helpdesk by telephone and e-mail<br>• Online help<br>• Information sessions | • E-mail<br>• Telephone (after e-mail)<br>• Online help | • E-mail<br>• Telephone<br>• Online help |

**Table 4 – Summary of usage for four existing tools: KLIC (NL), KLIP (BE), Ledningskollen (SE) and LER (DK)**

# 3 Analysis of the survey

## 3.1 Benefits of the tool

All interviewed experts confirmed that the frequency of underground infrastructure damages after implementation of their information systems decreased. However, they did not collect quantitative data to support their statements, since baseline situations had not been recorded and methodologies to make a quantitative evaluation of the project success had not been developed.

Nevertheless, the respondents indicated that their information systems for underground infrastructure protection were recognized by stakeholders as successful initiatives. The following advantages of such national initiatives were identified:

- Those projects consolidated efforts of all stakeholders: public institutions, underground infrastructure owners, and excavators to achieve common objectives to reduce unintentional damages of underground infrastructures during civil works.
- A properly functioning, single, state-wide information system provides excavators with an easy and quick access to information required to prevent underground infrastructure damages during civil works.
- Common rules and procedures (whether defined by legal acts or based on agreements among stakeholders) ensure certainty for all subjects playing different roles in these initiatives. Infrastructure owners are aware of whom, what, and when they need to provide information about their assets. Excavators know when, how, and to whom they have to apply for information about underground infrastructures and from whom, how, when they can obtain it.
- Graphical representation of underground infrastructures on digital maps in a user-friendly, easy-to-understand form ensures that even non-professional excavators realise where exactly this infrastructure is located in its civil works polygon.
- APIs for connection of underground infrastructure owners and GIS with information systems enabled automated provision of information about underground assets to the system which minimized infrastructure owners' efforts and also decreased the time period to obtain this information for excavators.

## 3.2 Main findings of the survey

**Finding 1: Importance of civil work in cable cuts**

Unintentional damages of underground electronic infrastructures during excavation works is one of the most frequent causes of disruptions in public electronic communications networks or services within EU MS. Such events can cause negative impact on several vital sectors of the society.

**Finding 2: Cable cuts are often linked to the lack of information**

The main reason for unintentional damages of underground infrastructure is that excavators do not have any information about underground infrastructure in its excavation polygon, or this information is not sufficient enough.

**Finding 3: Automated information exchange can be benefical to all stakeholders**

A common platform for exchange of information about the existing underground infrastructure between its owners and excavators decreases civil work delays and also helps to prevent underground infrastructure from damages during civil works.

**Finding 4: Existing automated information exchange systems help in preventing cable cuts**

Information systems already implemented in several EU MS for automated exchange of information about the existing underground infrastructure between its owners and excavators currently is the most advanced means which significantly contribute to the underground infrastructure damage protection.

**Finding 5: Existing automated information exchange systems share similarities**

Despite the fact that MS which had information systems applied different approaches for their system development and operation (different financing models, obligatory or voluntary use, legal basis or voluntary initiative,…), general architectures and operation principles of their developed information systems were very similar.

**Finding 6: Automated information exchange systems rely on digital maps**

Digital maps with database which contain information about underground infrastructure and their owners are key elements in the currently operating information systems.

**Finding 7: Direct integration into the stakeholders' own information system has benefits**

APIs for automated information exchange between infrastructure owners GIS and information system for underground infrastructures protection decrease the owners burden and reduce information retrieval times for excavators. APIs can lead to advanced functionalities, such as automatic answers.

**Finding 8: Confidentiality is important to consider before sharing information**

Information about underground infrastructure is sensitive in terms of public security or business secrets. Security measures should be implemented in information systems containing such sensitive information in order to avoid their use for malicious purposes.

**Finding 9: International collaboration is needed to protect cross-border cables**

Protection of underground/underwater cross-border cables is still an open issue. Stronger international collaboration is needed to investigate and to define common measures to protect these assets.

## 3.3 Possible improvements and future developments

Answering the questions about what could be improved in their systems, respondents highlighted the following issues.

### 3.3.1 Reduce the time for information exchange

The time for the excavator to collect information from all infrastructure owners in their area of digging is still too long. This could be improved by further automating the system, implementing new functionalities which facilitate information exchange between underground infrastructure owners and excavators.

### 3.3.2 Expand the usage of the tool

Small infrastructure owners are reluctant to join information systems. Their major arguments are that information systems are sophisticated, they do not have digitalized geo-referenced information of their assets, and too much effort is needed to provide information.

A few solutions have been discussed and are already implemented by some respondents:

- The simplification of the tool for non-technical users.
- Awareness raising and training for small cable owners and excavators.
- Live support, preferably through telephone, for users who remain unfamiliar with computer systems and/or with the declaration process.

### 3.3.3 Improve information exchange

Current systems operate employing raster geodata (representation) format in digital maps. Two information system owners wish to upgrade them into vector geodata format maps considering that this geodata format are best suited for direct data processing or aggregation.

Moreover, the majority of respondents have expressed the necessity to define common data models to guarantee the quality of information.

### 3.3.4 Facilitate international collaboration

Regarding underground/underwater cross-border cables, all respondents pointed out that only part of these assets which were within their states territories had been registered in their information systems. They also indicated that, for the time being, there was no strong collaboration and exchange of information between neighbouring countries about such infrastructures. Every state takes responsibility of the protection of underground/underwater cross-border cables which are laid down in its territory.

Finally all respondents expressed their good will to share their knowledge regarding development and managing of information systems for underground infrastructure protection. They also indicated their willingness to participate to an EU-wide initiative for underground infrastructure protection.

# 4 Recommendations

Taking into account the findings of this study, several recommendations are proposed for MS which are considering the implementation of measures to protect underground electronic communications infrastructure from damages.

**Recommendation 1: MS should analyse the reasons behind cable cuts**

Before implementing measures to protect underground electronic communications infrastructure from damages, MS should perform a baseline situation analysis identifying major reasons of underground infrastructure damages.

In this assessment, MS should identify stakeholders affected by damages and evaluate their interest to tackle this problem. This first analysis can be followed through time by performing quantitative calculations of all involved stakeholders loses due to underground infrastructure damages.

**Recommendation 2: MS should evaluate the benefits of an automated information exchange tool to protect underground infrastructure**

MS should perform a cost/benefit analysis for the projects for underground infrastructure protection.

This analysis can be backed up by the inputs from the involved stakeholders: underground infrastructure owners, civil workers, and their electronic communication national regulatory agency, which collects major incident due to cable cuts.

**Recommendation 3: MS developing an automated information exchange tool should rely on existing tools and experience**

MS developing such information system are encouraged to contact entities responsible for the development and management of such tool in other MS, in order to exchange and share experience.

MS should consider the principles, outcomes and results of tools already implemented in other MS. This should facilitate the development of a solution adapted to their needs, according to their particular structure and conditions applicable inside their territory.

Moreover, MS can also mitigate their effort by integrating this automated information exchange tool directly in their effort to deploy INSPIRE Directive.

**Recommendation 4: MS shall encourage collaboration between all stakeholders to define the principles of the automated information exchange tool to protect underground assets**

MS should encourage all stakeholders, i.e. relevant public institutions, underground infrastructure owners, and excavators, to collaborate in order to define the principles of the automated information exchange tool in order to protect underground assets.

Technical and organizational details of information systems should be defined during public discussions with all relevant stakeholders, taking into account their needs as well as the national specificity regarding underground infrastructures and civil work in the MS. It is recommended that information system architectures and functionalities are similar to the described above information systems, which are already implemented in a few MS.

Referring to the experience of MSs already managing such projects, we recommend not to limit the project scope by underground electronic communications infrastructure protection. Other utilities of infrastructure should be included since these underground infrastructures are equally affected by unintentional damages during excavation works and it is obvious that all parties are interested to have a single system.

**Recommendation 5: MS should promote the use of their automated information exchange tool to protect their underground infrastructure**

The project of information system development for the automated exchange of information between underground infrastructure owners and excavators should be recommended as an effective measure for underground infrastructure protection since such projects implemented in a few MS are considered as successful.

**Recommendation 6: MS and the involved stakeholders should evaluate the security policy for operating and managing their automated information exchange tool**

It is recommended that MS developing such tools integrate security aspects covering the operation of the tool (for the declaration of assets and the map requests by excavators) and its management (for the data storage and processing).

MS should define and adapt the security policy of the tool with respect to:

- The operational requirements set by the stakeholders, such as infrastructure owners (example: ensure the confidentiality of assets) and excavators (example: reliability of data).
- The management of the tool such (for example: security of stored information).

Stakeholders can also develop their own internal security policies. For example, infrastructure owners can validate the legitimacy of a request before disclosing information.

**Recommendation 7: MS should evaluate the sustainability of their automated information exchange tool**

MS are recommended to evaluate the sustainability of their automated exchange tool in order to understand its usages, its adoption by stakeholders and the results on the protection of underground electronic communication assets. For that purpose, MS have several possibilities, such as deploying an information exchange platform performing surveys, analysing incident reports on cable cuts…

Respondents emphasize the need to perform an evaluation at the beginning of the project and after its deployment.

The evaluation of the sustainability shall permit MS to adapt the tool to fit the (evolving) needs of their stakeholders. For example, it can include the development of new functionalities such as APIs to facilitate external integration.

# 5 Conclusions

This document investigates several MS initiatives for underground infrastructure (including electronic communications infrastructures) protection. The results show that the operation of a single automated information system for the exchange of information can prevent underground assets from unintentional damages during civil works.

One main finding is that confidentiality is a main concern for infrastructure owners. For this reason, the automated information exchange tool takes the form of a directory which provides excavators with the contact information of underground asset owners in their area of digging.

Hence, these tools are likely to differ from existing infrastructure mapping tools, which may store precise information regarding underground assets (position, type…). Yet, such infrastructure mapping projects can still represent an enabler to protect underground electronic communication cables from outages due to civil work.

The investigations revealed that, despite the fact that the initiatives investigated in this document include different technical and organizational details, they share the following similarities:

1. Infrastructure owners declare their contact information for the geographical areas where the possess underground assets.
2. Excavators declare their intention of digging in a defined geographical area.
3. The automated information exchange system acts as a liaison between the infrastructure owners and the requester.
4. Excavators receive the maps showing the underground assets present in the area where they intend to dig.

Finally, the usage of automatic information exchange tools proves to be a valuable tool to protect underground electronic communication infrastructure against outages due to civil works.

# References

## Legislation

**European Union**

- Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services.
- Directive 2009/140/EC of The European Parliament And of the Council amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services.
- Directive 2007/2/EC of the European Parliament and of the Council establishing an Infrastructure for Spatial Information in the European Community.

**Belgium**

- "Legal framework of the KLIP". Available online: https://www.agiv.be/producten/klip/meer-over/visie-en-wettelijk-kader/wettelijk-kader

**Denmark**

- "LER Act". Available online: https://www.retsinformation.dk/Forms/r0710.aspx?id=137551
- Administrative order for the LER act. Available online: https://www.retsinformation.dk/Forms/R0710.aspx?id=143431

**The Netherlands**

- Act of 7 February 2008 containing rules relating to the exchange of information on underground networks (Underground Networks (Information Exchange) Act) or "WION act". Available online: https://zoek.officielebekendmakingen.nl/stb-2008-232.html

# Annex A: Questionnaire to obtain information about systems for underground infrastructure protection

## Project management issues

1. Does your institution manage this system alone or in collaboration with other public institutions? If yes, please, name these entities describing your duties and the duties/assistance of other institutions.

2. Since when has your system been operating?
   2.1. When was your system launched?
   2.2. Is it still under development?

3. What where the major obstacles and problems in the development phase of this project? (Legal, financial, organizational)

4. How did you fund the project (participation from operators, state funding…)?

5. Did you apply to/receive any funding from European Projects?

6. Have you ever been contacted by other Member States to help them implement a mapping tool for infrastructure protection?

## Gathering of information about underground infrastructure issues

7. How do you obtain information about the existing infrastructure and/or owners? From whom do you collect this information? (e. g. operators, governmental/public institutions, cross border networks owners, any entity possessing el. com. infrastructure)

8. Is the information provided on a voluntary or obligatory basis?

9. What does this information include? (e. g. Geo referenced data of existing infrastructure, names of the owners of infrastructure, their contact information, etc., information about planned civil works, other)

10. Please, describe how detailed information is required.

11. How is this information updated? How often?

12. What are the major obstacles to obtain correct, exhaustive information? What prevents from receiving it on time?

13. Do you use or plan to use data/outputs of infrastructure or other type of mapping projects as a source of information for your damage prevention system? If yes, please, describe how.

14. Do you take into account cross-border cables?

## Technical details about your system

15. How does your system operate, i.e. is it web-based, fully automated, or manual operations are required? What software and what type of software (in-house, open-source, commercial, other…) does it run?

16. How is the information stored? (Database, file repository…) Do you use a standardized/open data format? For data acquisition / storage / exchange?

17. Do you plan to integrate your software as part of an Open Data policy?

18. How is access your system by user (public access, access with authentication, access restricted to dedicated users only…)?

## General questions about your system

19. Is the use of your system for entities planning to execute civil works obligatory or voluntary?

20. Do you propose guidelines, tutorial or training to user your software? (For submitters? For users/requesters?)

21. Do you collect data about how frequently the system was used (for example, how many times per year)?

22. Did the damage to the existing infrastructure decrease after launching your system? If yes, do you have any quantitative data supporting this?

23. Do you map previous incidents (infrastructure damages) on your software?

24. What are advantages and/or disadvantages of using mapping for infrastructure protection?

25. What do you think could/should be upgraded/improved in your system?
    25.1. Are you upgrading/improving it or are you planning to do this soon?

26. Would you participate in an EU-wide initiative to use mapping systems as the tool for underground infrastructure protection?

TP-04-14-977-EN-N

**ENISA**
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

**Athens Office**
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

ISBN number: 978-92-9204-104-5
DOI: 10.2824/3762

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu