D2.6 – CSG Guidelines for cybersecurity and personal data protection

Andrea Capaccioli (DBL), Sabina Giorgi (DBL), Rebecca Hueting (DBL), Luca Urcioli (ZLC), Gianni Rondinella (CambiaMO), Floridea Di Ciommo (CambiaMO)

Document Number	D2.6
Document Title	Guidelines for cybersecurity and personal data protection
Version	1.1
Status	Final
Work Package	WP 2
Deliverable Type	Report
Contractual Date of Delivery	30.06.2021
Actual Date of Delivery	30.07.2021
Authors	Andrea Capaccioli (DBL), Sabina Giorgi (DBL), Rebecca Hueting (DBL), Luca Urcioli (ZLC), Gianni Rondinella (cambiaMO), Floridea Di Ciommo (cambiaMO), Andrés Kilstein (cambiaMO) Juanita Devis (imec- SMIT -VUB)
Reviewer	Imre Keseru (VUB), Thais Lamoza (door2door)
Keyword List	Cybersecurity, privacy, data protection, guidelines, recommendations
Dissemination level	PU[1]

[1] This is the public version of this deliverable which does not includes the Annex 2 – Berlin pilot risk assessment and recommendations.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

INDIMO Consortium

The project INDIMO - Inclusive Digital Mobility Solutions has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533. The consortium members are:

No	Participant Legal Name	Country
1	VRIJE UNIVERSITEIT BRUSSEL	BE
2	VDI/VDE INNOVATION + TECHNIK GMBH	DE
3	INTERUNIVERSITAIR MICRO-ELECTRONICA CENTRUM	BE
4	CAMBIAMO S.C.M.	ES
5	DEEP BLUE SRL	IT
6	TECHNION - ISRAEL INSTITUTE OF TECHNOLOGY	IL
7	MOZGASSERULTEK BUDAPESTI EGYESULETE	HU
8	FUNDACION ZARAGOZA LOGISTICS CENTER	ES
9	POLIS - PROMOTION OF OPERATIONAL LINKS WITH INTEGRATED SERVICES, ASSOCIATION INTERNATIONALE	BE
10	EUROPEAN PASSENGERS' FEDERATION IVZW	BE
11	DOOR2DOOR GMBH	DE
12	VIVERO DE INICIATIVAS CIUDADANAS	ES
13	COOPCYCLE	FR
14	FONDAZIONE ISTITUTO SUI TRASPORTI E LA LOGISTICA	IT
15	POSTE ITALIANE - SOCIETA PER AZIONI	IT

Copyright Statement

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

Executive summary

The deliverable D2.6 Guidelines for cybersecurity and personal data protection discuss the work done in Task 2.4 (T2.4) regarding the definition of guidelines and recommendations for improving and considering cybersecurity in the development of digital mobility services and digital delivery services. The deliverable aims to help to integrate and improve cybersecurity and data protection during the design or re-design phase of a digital service. D2.6 is part of the INDIMO Toolkit together with D2.1 Universal Design Manual and D2.3 Universal Interface Language. Together they provide guidance to professionals and practitioners in different phases of the development and operation of digital mobility and delivery services.

An analysis of possible cyber risks for digital mobility services has been done, highlighting the main concerns over possible risks related to Internet of Things (IoT), phishing, mobile applications and human factors. Also, ethical issues related to data privacy and security have been discussed introducing the privacy by design principles and strategies. The data coming from other project deliverables (D1.2, D1.3, and D1.4), which discussed cybersecurity and data protection topics from different perspectives, formed a first base for designing the guidelines and recommendations.

The Cybersecurity and privacy assessment guidelines are based 1) on the risk assessment performed in each of the INDIMO pilots, 2) the data from baseline questionnaires collected in T4.5, and 3) on literature review and analysis of secondary data. The risk assessment has been done by performing semi-structured interviews and questionnaire surveys with developers and those responsible for the pilots. It must be noted that data and results related to the Berlin pilot have not been included in this public deliverable, but they are reported in a confidential document [2].

The results presented in this document are both general guidelines for the design of digital mobility applications and specific recommendations for the next pilots' phase, which are related to the redesign of the services. The idea is to approach cybersecurity and personal data privacy by design and consider them as part of the design of the digital mobility services.

The main guidelines presented here are:

- **Establish processes and procedures to enhance organisational preparedeness to to cyberthreats and attacks**
- **Consider human factors as the first line of defence**
- **Consider the third-party services used and evaluate their security and how they could impact the service**
- **Design for maintenance, it must be easy to continuously improve and maintain the system and the service, without an impact for users**
- **Actively monitor the system to identify intrusions, and possible threats**
- **Avoid collecting unnecessary data from users**

[2] The pilot responsible organisation requested to keep the response confidential and not to publish it in any of the public INDIMO reports. The data collected for this pilot is provided as a separate annex that will be accessible only by 1) selected partners in the consortium and 2) the CINEA project officer.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

- **Clearly present personal data usage to users**
- **In case of use of IoT devices check and improve physical security**
- **Work to prevent phishing and make it easy to users to report phishing activities**
- **Design for inclusivity means design for security**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

Table of Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

List of figures

List of tables

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

Acronyms

ACRONYM	
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CM	Crisis Management
DLP	Data Loss Prevention
DoS	Denial of Service
GDPR	General Data Protection Regulation
IoT	Internet of things
IR	Incident Response
MaaS	Mobility as a Service
PDCA	Plan, Do Control and Act model
PUF	Physically Unclonable Functions
SMS	Service management system
UBM	User Behaviour Monitoring
UDM	Universal Design Manual
UIL	Universal Interface Language
WP	Work Package

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

1. Introduction

1.1. About INDIMO

The INDIMO project aims to enable researchers, operators of digital mobility services and platforms, developers of digital mobility solutions and policy makers to include the user perspective and co-creation approaches in the entire development process of digital mobility solutions. This way, products and services delivered would be tailored to the actual needs of transport users. The project will identify the main characteristics of demands that digitally based mobility solutions place on users, focusing on all types of transport users and, in particular, on vulnerable-to-exclusion citizens (such as older people, children, people with disabilities, low income, low education level). The project will develop the INDIMO Inclusive Digital Mobility Toolbox consisting of the Universal Design Manual, Universal Interface Language for transport services, Guidelines for cybersecurity and personal data protection and a Policy Evaluation Tool. These tools will support policy makers, developers and service operators to develop digital mobility solutions universally accessible to citizens focusing on accessibility and social and spatial inclusivity. The toolbox will be applied and tested on five pilot projects in Madrid (Spain), Antwerp (Belgium), Emilia-Romagna (Italy), Berlin (Germany) and Galilee (Israel). INDIMO has five project objectives, as follows:

- **Objective 1:** To improve the understanding of the needs of users towards the digital transport system.
- **Objective 2:** To improve the knowledge about the requirements of a personalised digital transport system towards users.
- **Objective 3:** To co-create tools that can help engineers, developers, operators and policy makers to develop an inclusive, universally accessible personalised digital transport system.
- **Objective 4:** To facilitate the concept of universal design throughout the planning design process of digital applications and services both for accessibility and inclusion.
- **Objective 5:** To navigate future policy by channelling project results into European, regional and local policy making.

1.2. Vision for D2.6 – Cybersecurity and privacy assessment guidelines

1.2.1. The INDIMO Toolbox

INDIMO's main goal is to expand the use of existing and emerging digital mobility services to target users-groups that are currently excluded due to physical, cognitive, cultural or socio-economic barriers. Fulfilling this goal requires a holistic approach that takes into consideration a variety of digital services and an extensive data collection from end-users, developers, operators, and policy makers in order to establish policies and guidelines towards more inclusive digital information systems and mobile

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

applications related to transport and goods delivery services. The outcome of the project will be a comprehensive digital mobility deployment Toolbox, which will be comprised of:

- The Universal Design Manual (UDM) for digital transport services (D2.1);
- The Universal Interface Language (UIL) for digital transport services (D2.3);
- The Cybersecurity and privacy assessment guidelines (D2.6);
- The policy evaluation tool and recommendations for policy makers (D2.7).

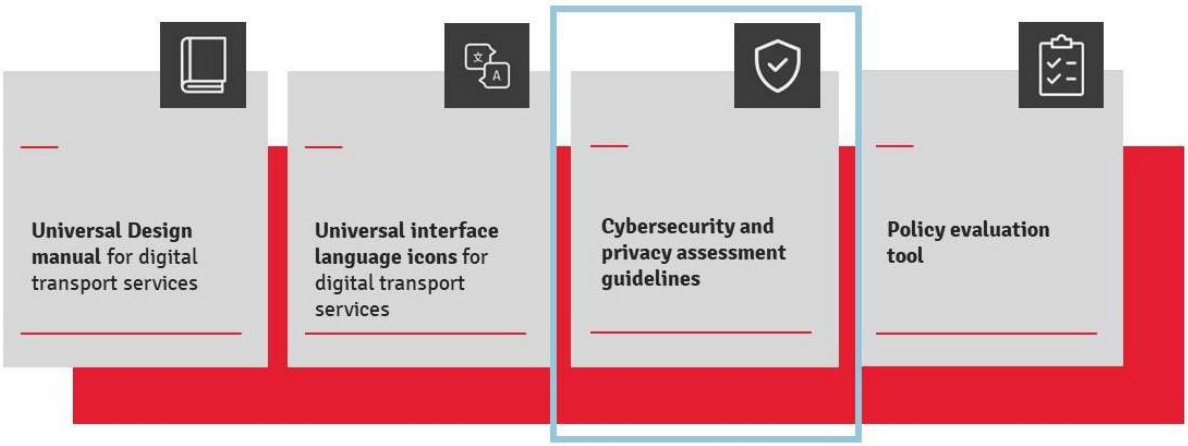


Figure 1 The Cybersecurity and privacy assessment guidelines and the other INDIMO Digital Mobility Toolbox

The INDIMO Toolbox supports a user-centric design approach, and is based on the principles of universal design, extending them also to cybersecurity and privacy.

The aims of cybersecurity and data protection guidelines are to:

1. Investigate the ethics, data protection and cybersecurity issues in inclusive digital mobility solutions;
2. Create guidelines about data protection and cybersecurity for designing user friendly digital applications and services;
3. Define a cybersecurity risk assessment framework based on ISO27001 for the digital mobility and logistics services, and apply it in the pilots to define cybersecurity requirements and security evaluation criteria;
4. Provide recommendations to improve data protection and cybersecurity through the INDIMO Policy Evaluation Tool.

The guidelines created and presented in this document are meant to be used for design and re-design of services with a security by design approach, and for increasing awareness among users about digital data security and possible security risks for them.

1.2.2. How was this document made?

The guidelines for cybersecurity and personal data protection are compiled for developing digital mobility services that consider cybersecurity and personal data protection from the early stage of the service design. They are part of the INDIMO Toolbox, and as for the other tools created in the INDIMO project they have been

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

supported by the work of the INDIMO pilots, and the recommendations have been validated by them, before the starting of the pilots' phase 2. The idea is to approach cybersecurity and personal data privacy by design and consider them as part of the design of the digital mobility services.

The document is based on the data collected, adapting the methodology defined during T4.1 and presented in D4.1 (2020), in two main stages: 1) cybersecurity risks assessment performed in each pilot, using a questionnaire and semi-structured interviews as part of T4.5, 2) personal data protection questions that have been added to the baseline questionnaire administered in T4.2. In addition to this, a literature review and a collection of secondary data from each pilot has been carried out. For more detailed information about the methodology used readers can refer to section 4 of this document.

1.2.3. Structure of the deliverable

This first version of the D2.6 – Guidelines for cybersecurity and personal data protection is the sixth deliverable of Work Package 2 (WP2) and it is complementary to the other deliverables submitted in M18: D2.1 – Universal Design manual (D2.1, 2021); D2.3 – Universal Interface Language (D2.4, 2021); D2.5 Enhancing appropriation of digital mobility solutions (D2.5, 2021). More advanced versions of these tools, revised based on the pilot testing will be delivered by the end of the project (D2.2, D2.4, D2.7).

In section 2, cyber risks of digital mobility services regarding four main selected topics (IoT, phishing, mobile applications and human factors) are described. In section 3 ethics and data are discussed, introducing privacy by design principles and strategies. Section 4 summarizes the methodology used for the risks assessment and the baseline questionnaires. Section 5 describes the insights from other deliverables, namely D1.2, D1.3, and D1.4, concerning cybersecurity and personal data protection. Section 6 includes the main results from the risk assessments performed in each pilot, which made possible then to create specific recommendations, and the analysis of the data from the baseline questionnaires. Section 7 contains the recommendations for each pilot to be considered in the next phases of the projects. General guidelines for digital mobility services are presented in Section 8.

2. Cyber Risks of Digital Mobility Services

Digital mobility services have a great potential in supporting vulnerable people in their daily activities. They can play a key role in increasing autonomy and improving safety while moving or independently executing routine tasks (e.g. collecting packages or paying the bills). However, digital technology poses new challenges for cyber-security and privacy that need to be addressed for its successful deployment. These challenges are even more critical when the end-users are vulnerable people. Due to the lack of technical skills, physical impairments or language limitations, vulnerable users are even more at risk of cyber attacks (G. Sonowal, 2017) and are less aware about disclosing private information than average users. Recent research has demonstrated that smart-city security is a multi-faceted problem, where the overall security of the system is

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

determined by the weakest link (Hadi Habibzadeh, 2019). New digital services are nowadays pervasive, and shape our lives daily, that is why human and societal dimensions are central as much as the technical ones for a successful cybersecurity strategy (Nai et al., 2020).

In this section, we review the state of the art of cybersecurity vulnerabilities and privacy challenges for digital mobility services. We describe how these challenges relate to the target end-users and adopted technologies. In the literature review, we identified four main topics of cybersecurity risks related to the INDIMO pilots: IoT, phishing, mobile applications and human factors.

2.1. Internet of Things (IoT)

IoT are a component of smart-cities and are part of new innovative services deployed in cities. They are enablers for new features and services, such in the case of the INDIMO pilot in Antwerp where smart-traffic lights are considered. Their security can be considered a challenge for having a safe and secure functioning service. Securing IoT poses a series of challenges starting from the limited computational power of wireless sensor networks to the dynamic and heterogeneous nature of such systems. Such heterogeneity leads to incompatible and diverse architectures and protocols that do not grant interoperability between systems. This has an impact on security and privacy, considering that a single countermeasure cannot satisfy the requirements of all the applications.

IoT security is critical in the smart city context since the devices are integrated in the urban environment and their vulnerabilities can impact the safety of citizens. For example, when sensors and actuators are used to control traffic lights, a possible attack can cause accidents and physical damage.

IoT security needs to be addressed at multiple levels: device level, network level, system level. At device level cryptography needs to be applied, considering the limited computational power of the device. Protection needs to be guaranteed both at firmware level, as well as the hardware level. This is important as IoT devices deployed in cities can be physically accessed by an attacker, who can read, reverse engineer, and modify the device to access the entire system (Habibzadeh et. al., 2019).

To address this challenge, PUFs (Physically Unclonable Functions) have been proposed as a possible solution against tampering. Security of device level can also be implemented at circuit level through randomized computation and memory access (Ammar et. al., 2018).

At network and system level, secure communication needs to be ensured between the different IoT devices, and higher-level servers and cloud computing infrastructure. Common attacks at this level include DoS (Denial of Service), data injection, spoofing, and data leakage (Zhang & Li, 2011). Encryption, anonymity, and access control needs to be implemented to reduce the risk of these attacks. An emerging solution to reduce the risks is the adoption of edge computing, which reduces the amount of the data that needs to be processed remotely by introducing an intermediate level of computation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

units that process the data locally. In this way, data sharing is confined to a local scope and less prone to global attacks.

Beyond the technical challenges, security and privacy need to be addressed at system level. The risk is that cyber threats can undermine citizens' trust in digital services. Those services are more and more interlaced with daily activities of people, and any successful strategy for cybersecurity must consider the human and societal aspects as well the technical ones (Nai et al., 2020).

From the analysis of several studies, Habibzadeh et al. (2019) discussed the idea that to have a secure smart city there is the need to use a holistic approach that tackles technological, organizational, and social challenges. Looking at the user perspective, a first risk is the possible lack of familiarity about security issues, leading to them becoming easy targets for attackers while interacting with smart-cities services. Also, as noted by Habibzadeh et al. (2019), there is a security disparity among various stakeholders: data is shared and circulated through different organizations both public, and private, with possible different security guidelines. Increasing the transparency of data and security features is an important factor to get "real" informed consent from the users.

2.2. Phishing

Phishing is a type of social engineering attack that aims to acquire user sensitive information such as username, password, or bank information. It is a type of risks which can be relevant also for digital mobility services, and for digital delivery services: attackers could target users to steal credentials or credit cards numbers. Vulnerable people such as older people, people with disabilities and people with cognitive issues tend to be the easier target for phishing attacks (Sonowal et. al., 2017). In most of the cases, the attacker using deception techniques tricks the user into visiting a seemingly authentic website from a legitimate and trusted organization. The unsuspected user enters private information that then is used by the attackers for malicious purposes. Misspelled URLs and sub domains are the most common type of tricks used by the phishers (Jang-Jaccard & Nepal, 2014; Sonowal et. al., 2017).

Phonetic similarities between authentic and non-authentic URLs together with the lack of graphic indications are a major vulnerability for users with reduced vision impairments. Blind people typically use readers to navigate the applications and for this reason they face extra challenges in detecting malicious requests (Sonowal et. al., 2017). These difficulties were also confirmed by the participants during the appropriation of digital technologies workshop we conducted in Antwerp.

Due to the lack of digital skills and consequently lack of knowledge about digital frauds, older people users are among the most popular targets for phishing attacks. Moreover, senior citizens tend to have higher credit card limits making them the perfect target for a financial attack. Senior citizens are also less likely to report a phishing attack due to the lack of knowledge on where to report it. (Alwanain, 2020). Segments of population with low digital skills, and lack of knowledge about digital frauds face similar challenges.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

Possible approaches to limit the risks of phishing include the integration of inclusive design principles to allow users to better recognize which requests are coming from authentic sources and which are not. Especially, for the case of reduced vision people it is recommended to include phonetic features (Sonowal et. al., 2017). Once a phishing attack has been identified, the best approach to reduce its spread is by actively tagging and reporting it (Jakobsson, 2007). However, users do not typically report attacks because they do not know how it can be reported. Companies should therefore design and implement features to ease the reporting of phishing attacks on their interfaces. Companies can also take a proactive measure to defend against attacks by registering domain names that are suitable for phishing (Jakobsson, 2007), e.g. typosquatting or URL hijacking.

Educating final users to recognize the threats raises their level of concern about phishing. Some recent non-traditional methods based on computer games or phishing awareness training have demonstrated significant improvements in the capacity of users of identifying phishing and avoiding attacks (Alwanain, 2020; Jakobsson, 2007).

2.3. Mobile applications

Today there are 3.88 billion smartphone users which represent 48.33% of the world population (Turner, 2021). Their increasing computational power, personalization and mobility makes them the perfect device to support everyday needs. Recent studies have shown that vulnerable populations such as immigrant communities or ethnic minorities use more mobile devices than computers. This is because smartphones are more affordable, require fewer digital skills and do not require infrastructure cost (Correa et. al., 2018). In the last decade smartphones together with tablets had taken a key role in supporting blind people in their daily tasks. In a recent study with reduced vision people, 87.4% of participants reported mainstream devices are replacing traditional visual aids. This was particularly true for object detection, navigation, help apps, audiobooks, readers, and character recognition applications (Martiniello et. al., 2019). At the same time, these new functionalities require an increased level of sensitive or private information that also leads to an increased risk of cybersecurity attacks.

The majority of cyberattacks today occurs because of software vulnerabilities caused by software bugs. The last are typically related to memory, user input validation, race conditions, and user access privileges. Memory safety violations are attacks performed to modify the content of a memory location. The most popular memory attack is buffer overflow where the program tries to store more information that the buffers are intended to contain leading to the overflow to adjacent buffers and eventually to the corruption or overwriting of the data (Jang-Jaccard & Nepal, 2014). User input validation occurs when the input data do not follow certain rules and the incorrect data validation can lead to data corruption. One example of this is SQL injection where the attacker injects SQL commands from the webform to change the database or to dump database information such as credit card information or passwords. Attackers can also exploit race condition errors occurring when parallel processing is not programmed correctly and where the timing of parallel events affect the behaviour of the system. Finally, privilege confusion can be defined as the act of exploiting software

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

vulnerabilities to gain access to resources that are not normally accessible to the user. With these privileges attackers can perform actions such as changing passwords or accessing protected secret keys (Jang-Jaccard & Nepal, 2014).

Today, the increasing number of smart city services and the need to monitor the city in real time have generated a growing need of collecting and processing data. Corporate systems process large amounts of data in the smart city networks. The use of GPS tracking data, personal information on shopping habits, location and personal interest poses significant privacy concerns. When applied in the context of smart cities, new risks can also emerge leading to an increase of social inequalities and biases, especially on people with low income and education (Habibzadeh et. al., 2019).

Recent studies have demonstrated that vulnerable populations such as older people and undocumented immigrants are concerned about sharing personal data and would like to have better control over the data flows. However, this concern is not supported by an understanding of how data flows and how they can customize the permissions over data collection and purpose (Pakianathan & Perrault, 2020; Guberek, 2018). Older people have also reported being willing to compromise their privacy in exchange of convenience (Pakianathan & Perrault, 2020). Immigrants, in a similar way, are constantly facing the tension between self-expression, group privacy and self-censorship related to their immigration status (Guberek et. al., 2018).

To address these challenges service providers could take different actions: providing transparency about the use of personal data and entities that participate in information flows, limiting the amount of data that is shared with other users and investigate how to guard the specific privacy needs of their vulnerable users. It is also recommended to develop training and educational resources where vulnerable users could learn more about privacy risks and how to mitigate them.

2.4. Human factor risks

ENISA (2020) analysed the threat landscape, and the associated incidents, and it identified that 84% of attacks relied on some sort of social engineering and that 71% of organisations experienced malware activities spreading from one employee to another. A report from IBM showed that 60% of the attacks against organizations are performed by insiders.[3] This shows how much is important to consider the human factor for a better security, also considering that a successful attack is the result of a combination of different factors, not only technological, but also connected with the culture, the policies and the practices of an organisation (Besnard and Arief, 2004).

At the same time, the human factor has been defined as “the first line of defence” (Parsons et al. 2017) against security threats, highlighting how a consistent approach considering the role of people in the cybersecurity scenario can improve the response and preparedness to attacks. Within this vision Pollini et al. (2021) defined a clear framework that take into consideration human factors as the strategic link for security in an organisation, considering three main factors: the individual, the organizational and the technological in a “holistic” approach.

[3] https://www-05.ibm.com/services/europe/digital-whitepaper/security/index.html

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 875533.

Hence, specific non-technical countermeasures can be taken, together with the technological protective measures usually recommended. Among the first ones Pollini et al. (2021) identified: i) adopting user-centred design approach to promote and implement usable rules and practices, ii) improve the usability of tools supporting work specific needs ensuring that their compliance with security restrictions does not jeopardize the user experience, iii) defining security policies and training campaigns that use a customised approach commensurate to the knowledge and skills of the employees and targeted to specific information security areas (example dividing among IT people and non-IT people).

Instead looking at the technological measures, the Israelian National Cyber Directorate (2021) identified the use of software for User Behaviour Monitoring (UBM), that can detect insider threats, targeted attacks, financial fraud etc. as a protective measure. These software include access privileges (including monitoring and controlling access, e.g. a user is flagged in case he/she access a folder containing a company's strategic material), and usage of biometric identification to authorize access. Other important measures can be identified such as:

- **Data loss Prevention (DLP).** These systems are used to prevent leaking of sensitive information;
- **Restricted Use of Removable Media.** Viruses or information leakage can happen when transferring information using USB sticks. Using logical means, USB access can be blocked. Likewise, physical means can be used to prevent USB usage;
- **Restricting Access to Cloud Storage Services.** Cloud storage services like google drive, Box or Dropbox can be a source of infection for organizations. Likewise, information can leak outside an organization. Also in this case, organizations can block access to these services using a firewall or a proxy through a browser.
- **Managing User Access Privileges Permissions.** Privilege permissions can be issued ad-hoc and limited to work-related tasks only. Permissions can be reviewed and updated periodically;
- **Implementing and internal firewall and an Intrusion Prevention System.** Internal firewalls can be used to monitor and minimize attacks from insider threats. The firewall can monitor all traffic in the network, blocking unauthorized access and communication;
- **Blocking communication devices.** Devices that are not authorized to join a network can be blocked, preventing information leakage;
- **Proactive cyber-defence.** Proactively review cyberthreats and update defence accordingly;
- **Honey pot.** A honey pot consists in creating attractive but false information, in order to capture insiders.

3. Data and ethics

Data protection is a central matter, a fundamental right and an ethical principle that should guide the action of organisations, even more nowadays that the emergence of big

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

data and AI show us the danger of misusing data collected from users, and the danger of data breaches. Professionals and researchers are exploring the ethical issue in cybersecurity from some years now (Christen et al. 2020; Macnish et al. 2020), providing theoretical and practical experiences on how to approach the ethical dilemmas that are rising from the implementation of pervasive ICTs technologies, big data and automated processing.

The European Union considers data protection as a fundamental right, and the GDPR legislation made clear the importance of defending data protection and how to proper manage data collection and retention. GDPR Compliance and the process of implementation and review of the adopted policies can become opportunities for the organisations to reflect on their practices and understand if, from an ethical point of view, they are respecting their values, together with the laws. In the Article 4(1), the GDPR provides a certain definition of "personal data": it "means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". The article 9(1) also defines what to consider "special categories of personal data" as "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data regarding a natural person's sex life or sexual orientation". The two definitions already identified a well-defined concept of what to consider personal data, opening for the necessary boundaries to its collection, and use which are defined in the GDPR.

A carefully designed and implemented data protection and cybersecurity strategy become even more important when there is the involvement of vulnerable categories of users, where a breach and an attack could expose them to repercussion higher than for other users (e.g., like in some extreme cases where this could be an issue of physical security or discrimination for minorities). For this reason, the analysis of pilots' activities, and the drafting of guidelines and recommendations that will follow in this document took into consideration also two main approaches to address ethical issues: privacy by design principles (Cavoukian, 2011), and the privacy design strategies Hoepman (2014).

3.1. Privacy by design principles

Cavoukian (2011) defined the "privacy by design" as a concept in the 90's, to address the systemic effect of the emerging pervasive ICTs technologies, making visible how privacy should become a default mode of operation for organisations. She defined seven main foundational principles, which are the following:

1. **Proactive Not Reactive; Preventative Not Remedial**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

Privacy by design is proactive, it anticipates and prevents privacy invasive events before they happen. This means that it aims to prevent privacy risks and infractions. Privacy by Design comes before-the-fact, not after.

2. **Privacy as the Default Setting**

   Privacy by design ensures that personal data are automatically protected in any given IT system or business practice. No action is required from the user side to protect their privacy, it is built into the system by default.

3. **Privacy Embedded into Design**

   Privacy becomes an essential element of the core functionality delivered, and an integral part of the system, without diminishing its functionality. Privacy is embedded into the design and architecture of IT systems.

4. **Full Functionality—Positive-Sum, Not Zero-Sum**

   Privacy by design avoids putting in contrast privacy vs security, and wants to demonstrate that it is possible to have both, seeking to accommodate all legitimate interests.

5. **End-to-End Security—Full Lifecycle Protection**

   Privacy by design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved. All data are securely retained, and then securely destroyed at the end of the process, in a timely fashion.

6. **Visibility and Transparency—Keep It Open**

   Privacy by design means that data processing is transparent and visible to users, that can verify its compliance to the given information. Information about personal data processing policies and procedures are available to users.

7. **Respect for User Privacy — Keep it User-Centric**

   Architects, designers and operators need to offer empowering user-friendly options, appropriate notice and strong privacy defaults that would keep the interests of users uppermost.

3.2. Privacy design strategies

Starting from the privacy by design principles and by considering data protection legislation, Hoepman (2014) defined eight privacy design strategies. They provide a more practical approach and a classification of privacy design patterns and technologies that can enhance privacy. The strategies are useful for designing privacy by design system. They are the following:

1. **Minimise.** The amount of processed personal data should be restricted to the minimal amount possible. This strategy helps to limit the possible privacy impact by ensuring that no unnecessary data is collected. The processing of personal data should be proportional in respect to the scope, and it should be checked for possible less invasive alternatives.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

2. **Hide.** Any personal data, and their interrelationships, should be hidden from plain view. The hidden data are less probable to be abused. Data can be maintained hidden by encryption, anonymisation or pseudonymising both in transit or in storage.
3. **Separate.** Personal data should be processed in a distributed fashion, in separate compartments whenever possible. Data is separated, for example, by splitting databases and processing data locally.
4. **Aggregate.** Personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful. When possible, data should be aggregated for processing, making them less sensitive, since referred to large groups instead of individuals.
5. **Inform.** Data subjects should be adequately informed whenever personal data is processed. Users should be informed about which information is processed, for what goal, and by which means. Also, they should receive information about third parties' involvement. Data access rights and how to exercise them are also important information to give to users.
6. **Control.** Agency should be provided to users over the processing of their personal data. After being informed, users should be able to act, by consulting, modifying and deleting information collected about them. Users should have the tools for exerting their data protection rights.
7. **Enforce.** A privacy policy compatible with legal requirements should be in place and enforced. The proper technical protection mechanisms should be in place in order to enforce the identified privacy policies, with the appropriate governance structures (e.g., in the case of access control, or privacy rights management).
8. **Demonstrate.** Be able to demonstrate compliance with the privacy policy and any applicable legal requirements. The data controller should prove to be in control and demonstrate how the privacy policy is implemented in the IT system.

4. Methodology

In this section we present the methodological approach used for collecting and analysing the data for the creation of guidelines and recommendations. The work done in T2.4 went in two main directions: 1) the risk assessment of each pilot to map cybersecurity threats and protective measures as faced by organizations involved in mobility services (carried out in task T4.5); 2) the analysis of baseline questionnaires (carried out in task T4.2) regarding cybersecurity and personal data protection from a user perspective (see also Deliverable D4.2 Baseline data report for pilots).

Another important data source, together with the literature analysis, that informed the compilation of the guidelines is the work done in other project tasks, especially the ones related to WP 1. The results of this work that has a focus on cybersecurity and personal data protection are presented in three deliverables: D1.2, D1.3 and D1.4, which are summarised in Section 5 of this deliverable. The deliverables already presented key

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

points regarding the topics addressed in this document, looking at cybersecurity from different perspectives: in D1.2 from a user perspective looking at requirements and needs, in D1.3 looking at users' capabilities, and in D1.4 analysing the barriers to the deployment of inclusive digital mobility services. What is important is that some of the insights coming from those deliverables match with the data analysis from the risk assessment and the questionnaires, reinforcing the content of recommendations and guidelines presented here.

4.1. Risk Assessment Methodology

To determine cybersecurity guidelines for the pilots, the approach consisted of reviewing the data collection methodology defined in D4.1 and adapt it in T4.5 to collect data from the pilots and perform the risk assessment. To develop the methodology the team reviewed the standards proposed by ISO27001 and those from the National Institute of Standards and Technology, NIST 800-55. These two standards are similar in practice, but some slight differences can be found in terms of layout and content. Experts believe that the ISO27001 guidelines are more feasible for mature organizations that have in place well-established processes or products (Auditboard, 2021). In addition, ISO27001 offers more technical details than NIST on security controls. This was not the case for the majority of the pilots in INDIMO, where solutions were on a prototype stage and companies involved were of small-size and not operationally mature. Hence, following internal meetings with INDIMO risk management team, it was decided to adopt part of the ISO27001 but put major focus on the NIST framework (Chew et al., 2008). Yet, this had to be further simplified given the early stage of the solutions developed by the pilots. The final methodology developed is believed to facilitate the decision concerning the identification of main processes / products, vulnerabilities and necessary investments in additional security policies, controls, and procedures. Finally, these guidelines are based on a stepwise approach were both secondary and primary data needs to be collected. Therefore, enabling its replicability in additional pilots / cases.

The data collection can be summarized in two steps: a desk research to collect secondary data and a questionnaire for primary data.

- **Secondary data collection.** Pilots were requested to collect and share with the team any relevant material in which any of the following information was available and possible to share e.g., IT architecture of the system, data management plans, risk management plans, enforced regulatory frameworks, overall cybersecurity strategies and policies applied and other relevant documentation that could be used to contextually describe the cybersecurity state-of-play in the organizations involved in the pilots. The information was requested via e-mail, and, when necessary, online meetings were organized to discuss any doubts raised after an initial review of the material. At the end of this process, the team summarized the material collected and triangulated it with other data collected from the interviews/questionnaire used in the second stage of the data collection (see below).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

- **Semi-structured interviews/questionnaire.** A questionnaire was used to interview developers involved in the pilots. The questionnaire was a combination of open-ended and closed questions to evaluate main cyberthreats. A first draft of the questionnaire was developed by Deep Blue and ZLC based on the material reviewed in the desk research step. Thereafter, 2 external cybersecurity experts were requested to review the draft of the questionnaire and give comments and feedback. At the end of the review process, the questionnaire was updated, consolidated, and sent to the pilots' main contact point. A copy of the questionnaire is available in the Annex of this report. It is split into the following thematic areas/topics:
  - **Managerial processes** to plan and improve cybersecurity. Open ended question.
  - **3rd parties involved** and main data exchange. Open ended question.
  - **Risk assessment** measured as impact and likelihood. Closed question, where impacts and likelihood were measured using a Likert scale from 1 very low to 5 very high.
  - **Threats involving users with special needs**. Open ended.
  - **Protective measures**. Open ended.
  - **Efficiency / effectiveness KPIs**. Open ended.

4 pilots responded to the questionnaire above: in Antwerp, Galilee, Madrid and Berlin pilots a developer was interviewed (both directly from the team or, for language reasons, by a person from the pilot). In 1 case (Emilia Romagna) data were collected with two meetings with Poste Italiane team participating in the INDIMO project. In one of the two meetings, a semi-structured interview was performed with one of the Poste Italiane cybersecurity expert. The interview covered exclusively the protective measures adopted for parcel lockers. This was a mitigation strategy that was adopted since, for confidentiality reasons, Poste Italiane could not release information about likelihood and consequences of cybersecurity risks that are currently faced. Additional secondary material was provided to outline the managerial processes that are enacted by Poste Italiane to plan and improve cybersecurity.

Additional confidentiality issues had to be handled for Berlin and Galilee. In the Berlin pilot, the main developer requested to keep the response confidential and not to publish it in any of the public INDIMO reports. The data collected for this pilot is provided as a separate annex that will be accessible only by 1) selected partners in the consortium and 2) the CINEA project officer. In the Galilee pilot, our main contact could answer only questions related to the assessment of risks. While the remaining parts were answered by means of the secondary data provided.

4.2. Baseline questionnaire

The design of the questions in the baseline survey specifically addressing the assessment of cybersecurity and personal data protection from the user perspective was carried out by Task 2.4 and Task 4.5 contributors (cambiaMO, DBL, Imec, and ZLC) and pilots' partners (i.e ITL and Poste Italiane, IMEC, Technion, cambiaMO, VIC, CoopCycle, Door-to-Door). The survey was set up as part of Tasks 4.2, 4.3 and 4.5 to collect data

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

about the baseline situation in the pilots based on the INDIMO Evaluation Framework (Deliverable D4.1).

Evaluation of cybersecurity and personal data protection was mainly based on **5 statements** proposed to the respondents (out of a total of 25 statements for the whole Baseline survey). The 5 statements for the assessment of cybersecurity and personal data and their correspondent variables include:

- **Q20** - I consider that the app has informed me sufficiently about the use that will be given to my data (***Information about use of data***)
- **Q21inv** - I'm not sure the app will take care of my privacy (e.g. spamming) (***Care about privacy***)
- **Q22** - I trust that the app will keep my information safe and not to disclose it to third parties (***No disclosure to third parties***)
- **Q23inv** - I doubt that the people responsible for the app will contact me immediately if they experience data privacy risks (***Information about risks***)
- **Q24** - I trust that if, I agree to share my data with third parties, it will be done ethically and responsibly (***Ethically data sharing***)

Variable ---------- Indicator of Trustfulness	Information about use of data	Care about privacy	No disclosure to third parties	Information about risks	Ethically data sharing
Trust	✓		✓	✓	✓
Privacy	✓		✓	✓	
Perceived security		✓	✓	✓	

Table 1. Variables and indicators covered by Baseline survey questions

Respondents had to state their **level of agreement or disagreement** with the statements indicating a value on a 6-grade Likert scale. Figure 2 provides a description of the scale used, from 1 (strongly disagree) to 6 (strongly agree).

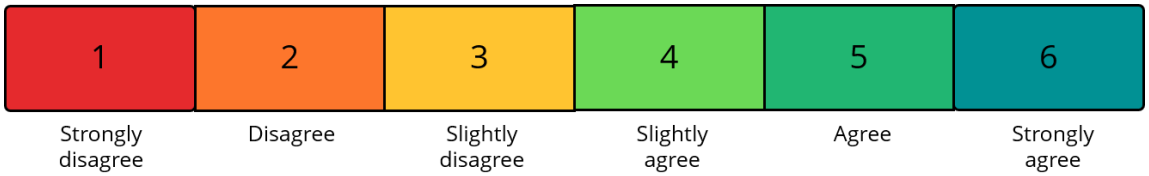


Figure 2. The Likert scale used in the Baseline survey to assess each statement proposed.

Following usual best practices in survey design (Weijters & Baumgartner, 2012), for two of the five statements survey items were reverted in order to (1) keep respondents from answering carelessly, and (2) help correct the agreement bias[4]. Consequently, in the

[4] A category of response bias common to survey research in which respondents have a tendency to select a positive response option or indicate a positive connotation disproportionately more frequently.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

analysis the answers given to those two statements were re-reversed to assume the same sense as the rest of questions with positive wordings.

5. Insights from project deliverables

The cybersecurity and personal data protection dimension have been already addressed and discussed transversally in the INDIMO project. Important output and insights related to the security and privacy of users and stakeholders have been presented in other deliverables of the project. Here there will be a summary of the main output from deliverables D1.2, D1.3 and D1.4, used also to generate the guidelines.

5.1. D1.2 User needs and requirements on a digital transport system

In D1.2, the user needs and requirements were discussed as part of the co-creation of personas and user journeys related to the INDIMO pilots, but also through the discussion of five specific case studies, one of which is directly addressing cybersecurity and privacy for older people, people with reduced vision, and refugees.

The main outcome relates to the need of respecting privacy and data security, following the current legislation, but also laying attention on possible risks, like eavesdropping with impaired persons, or protecting data of refugees to prevent giving away locations to authorities or human traffickers. Older people are concerned with risks connected with the protection of bank details and financial data. Especially for reduced vision people and people with reduced mobility, there is the necessity to give away personal information to have a good service, which points to the need of collecting only the needed data, trying to minimise data collection. Furthermore, the understanding of regulations poses a challenge for users, with unclear, or too complicated language and visualisation. Users need more clarity about the usage of data.

The case study on privacy and security presented in D1.2 focused on three main categories: older people, people with reduced vision, and refugees. It draws specific recommendations for each of the categories, and general ones. Here we report the general recommendations expressed in the use case, they are relevant also considering the results from the data collection and the risks assessment analysis performed in this deliverable:

- While engaging with vulnerable groups, consider developing clear and transparent documentation toward personal data usage, go further than the GDPR-rules;
- When considering cybersecurity requirements, take into account a holistic view; involving not only technical requirements, but also human factors and communication issues;
- During the meetings and the interactions with users in the Communities of Practice context, consider giving also specific training on cybersecurity and privacy;

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

- Usability is important also for cybersecurity, for the designing of a usable and inclusive service and product taking into account literature best practices for cybersecurity.

5.2. D1.3 Users capabilities and requirements

In D1.3 Users capabilities and requirements, the usage capabilities, requirements and limitations related to the users' profiles were analysed. Based on this analysis a list of inputs for the Digital Mobility Toolbox have been elaborated. The input to the Guidelines for cybersecurity and personal data protection provided by D1.3 are summarised in the table below.

The inputs mostly regard solutions and suggestions for creating a safely user interaction, preventing for possible security and privacy risks both from human errors and for possible attacks. Confirming also other results discussed later in the deliverable, it is relevant to note the need for increasing the awareness of users toward the data usage, and the terms of the services, with more understandable presentation. Also, the involvement of target groups throughout the process is important for the security by design approach.

Input
Accessibility
Involve target groups throughout the process.
Confirmation of purchase by parents-tutors/ warning message (for cognitively impaired people)
Privacy and data security
Certifications of privacy and good practices for handling credit card info.
Checklist of what data is stored and for how long.
Terms and conditions summarized in checkboxes
Use a code to deliver instead of the real identity of the user (pick up a person, for DMS)
Allow payment alternatives, especially cash but also digital wallets payments (such as PayPal).
Feedback, such as notifications and warnings, to reassure online payments.

Table 2 Inputs from D1.3 for Guidelines for cybersecurity and personal data protection

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

5.3. D1.4 Barriers to the design, planning, deployment and operation of accessible and inclusive digital personalised mobility and logistics services

In D1.4 the drivers and barriers related to the development and deployment of accessible and inclusive digital mobility services was analysed. While the results of this deliverable are relevant for the Policy evaluation tool, there are insights useful also for what concerns the data privacy protection. The results come from 10 deployment case studies and a workshop with relevant stakeholders.

What is important to highlight from the results, which are presented in Table 3, is the central role of data collection, sharing, and analysis for the different digital mobility services and the stakeholders. The table highlights what kind of data is collected in the different types oof services and for what purpose.

Type of service	Service name	Data collection/ protection and privacy
Car- & ridesharing	Cambio Brussels	Only mobility related data, with limited use, especially about vulnerable to exclusion users
	Mobitwin	Older people have trouble understanding privacy related issues and do not understand the importance of GDPR.
Bike sharing and micro mobility	HIVE Lisbon	Data collection is very limited and is not really used for analysis. Contradicting vision on use of data: in detail or rather a general approach. Data is needed to address impact on public space
	Brussels Mobility	
Smart Logistics services	La Pajara Madrid	Only information relevant to delivery is stored, but not used for any other purpose.
	Mobile Locker	Information about efficiency/use of the lockers is collected and used to find most profitable location.
	Citypack Valencia Lockers	
Multimodal routeplanners & MaaS	HSL	Fear that sharing data will lead to advantage for competitors Lack of trust in public services handling data.
	HVV Switch	
	BKK FUTAR	
	Jeasy	

Table 3 Insights from D1.4 related to data collection/protection and privacy

The case studies have concluded that there is a need for creating a framework for secure mobility data collection and exchange to ensure both better services and the security of

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

the users, especially in shared mobility and Mobility as a Service applications where there is a continuous interaction between the digital application/service and the users. So, it will become important for new digital mobility services to prepare and also evaluate the policy implications of such possible new framework, which will reflect also on the design of more safe experience for the users.

6. Insights from the INDIMO pilots

In this section, the results from the pilot risk assessment and desk research, and the results from the baseline questionnaires administered in the context of the pilots for T4.5 are presented. These are two different perspectives, from one side the risks assessment from the organisational point of view, which makes the risks connected to cybersecurity and data protection visible for the different companies and organisations running the pilots. From the other side the baseline questionnaires of the pilot evaluation reflect on the vision from the user perspective, to see how the topic of privacy and data security are considered by users within each pilot.

The five pilots of INDIMO are the following (a more extensive description of each pilot can be found in the INDIMO website[5]):

- Pilot 1 - Emilia Romagna: Digital Lockers. Organisations involved: Poste Italiane, ITL.
- Pilot 2 – Antwerp: Inclusive traffic lights. Organisations involved: IMEC.
- Pilot 3 – Galilee: Informal ride-sharing in ethnic towns. Organisations involved: Technion.
- Pilot 4 – Madrid: Cycle logistics platform for delivery healthy food. Organisations involved: cambiaMO, Coopcycle, VIC.
- Pilot 5 – Berlin: On-demand ride-sharing integrated into multimodal route planning. Organisations involved: door2door.

6.1. Pilot risk assessment and desk research

The results of the risk assessment and the desk research for each pilot are presented below. The risk assessments have been carried out following the methodology already presented in Section 4 of this deliverable. The risk assessment and the recommendations for the Berlin pilot are provided as a separate annex accessible only by 1) selected partners in the consortium and 2) the CINEA project officer. The main developer requested to keep the response confidential and not to publish it in any of the public INDIMO reports. The risk assessment of Emilia Romagna pilot does not have the risks matrix analysis since it was not possible to collect that data, as explained in Section 4.

[5] https://www.indimoproject.eu/pilot_projects/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

6.1.1. PILOT 1 – Emilia Romagna

FORMAL / INFORMAL MANAGERIAL PROCESSES[6,7]

To ensure security the company follows diverse standards and guidelines. Certifications connected to cyber security that were mentioned, include the following:

- **ISO 9001.** Criteria for quality management system. The standard has a strong customer focus expecting involvement of top management and continuous improvement.
- **ISO 27001:2013.** This standard refers directly to requirements for creating, implementing and maintaining information security management systems. An important model, part of this standard is the well-known Plan, Do Control and Act model (PDCA) that aims to ensure the correct design, deployment and update of the Information Security Management System.
- **ISO 20 000.** This standard refers to requirements to implement, maintain and continually improve a service management system (SMS).
- **NIST.** NIST 800-55 proposes a robust methodology to identify and measure the impacts of security controls. The NIST is a document providing information for measuring the impacts of security controls through three categories: *implementation*, *efficiency and effectiveness* and organizational *impact measures*.
- **GDPR.** The company has measures in place to ensure that all orders are processed according to clients' instructions and existing GDPR requirements for Data Protection Agreements regulating the usage of personal data.

Some examples are mentioned as part of the implementation of measures to ensure an enhanced protection against security threats:

Security by design: during the design of a product/service, the organization includes cybersecurity as one of the requisites to be considered. Hence, security is applied to both hardware and software. In software a dynamic analysis, rather than a static one is applied. Tests are applied and software is certified. Thereafter it is sent to production with the right standards. This also addresses part of possible ethical issues, in combination with the GDPR compliance.

Physical security: apart software, physical security is evaluated and monitored. Some of the checks that are performed include: signal coverage in the location where the parcel box is placed, installation in security conditions. The box is also built/designed to withstand sabotage and thefts of parcels.

Vulnerability Assessment: vulnerability assessment is performed periodically and in determined situations. In this aspect control points are established to perform the assessment and monitor risks associated to cybersecurity.

Poste Italiane Cybersecurity Framework

[6] https://www.posteitaliane.it/it/cyber-security-sostenibilita.html

[7] https://www.posteitaliane.it/it/cyber-security.html

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

A Chief Information Security Officer (CISO) has been entrusted to ensure the management and responsibility of company's information security.

There are three important initiatives to mention:

The Security Innovation Lab, dealing withs with applied research and has launched numerous project initiatives within the FP7 and H2020 European programs.

The Computer Emergency Response Team (CERT). The CERT deals with prevention, analysis and protection from cyber threats and has a Cyber Security Competence Center, located in Rome. The group is dedicated to the study of new techniques to counteract the sabotage of computer software. CERT's security experts, with different tasks: coordinating all the activities of response to computer emergencies, to ensure customers and consumers correct use of the internet, coordinating all IT emergency response activities and exchange of knowledge from individuals in the context of cyber security.

The Cyber Security Technological District of Cosenza. The group works with the creation of solutions for the protection of electronic payments.

A framework has been developed. This is composed of the following pillars:

- **IT Security Policy** and supporting document system. Objectives and strategic directives aimed at guiding the management of the security of resources and IT processes in support of business services. The Policy aims to contain, within predefined acceptable limits, the risk of compromising confidentiality, integrity, and availability of information.
- **IT risk assessment.** Poste Italiane uses an IT risk assessment and management methodology aimed at limiting the risks of loss of confidentiality, integrity, ensuring a correct distribution of the investments of safety.
- **Permanent Security Plan (PPS).** The Plan consists of all the interventions and technological projects necessary to ensure the presence, updating and proper functioning of the security platforms.
- **Security by Design Activities.** Security analysis performed during design, implementation and production phases of new services or modification of existing services.
- **Security incidents data collection and analysis**. This activity is performed to fulfil the obligations established by current legislation on data security, prevention and combating of IT crimes - in line with Legislative Decree 196/2003. The IT security incident management methodology adopted by Poste Italiane and formalized in a specific Operating Procedure is in accordance with the Good Practice Guide for Incident Management of ENISA - European Union Agency for Network and Information Security (European Security Agency networks and information).
- **Certifications.** Poste Italiane follows and maintain necessary quality and security standards by adopting a Management System Integrated IT Quality and Security that incorporates the aspects highlighted by international standards and industry benchmarks.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

- **Projects for security innovation.** Diverse projects / studies are being realized by Poste Italiane in the cybersecurity field. Focus is on the issues of identity management, mobile security, and distributed ledger (blockchain technology).

To guarantee security for mobile applications, Poste Italiane performs the following activities (this applies to all apps that display Poste Italiane's logotype):

- Analyse the types of data collected and possibly transmitted by the Apps used;
- Prevent complaints from customers for offenses attributable to the use of the App directly, indirectly or allegedly connected to the brands of Poste Italiane and Group companies;
- Prevent direct damage (for example fraud, etc.) due to improper use of the App or indirect damage (for example damage to image, etc.) due to improper use of brands;
- Protect intellectual property (source code, logos, trademarks, etc.).

Poste Italiane is part of the following international organizations that are working in the field of Cyber Security:

- **European Electronic Crime Task Force (EECTF).** It was founded in agreement with the United States Secret Service (an American government agency set up to prevent and combat financial fraud). The main objective consists of fighting and prosecuting international computer crime.
- **Global Cyber Security Center (GCSEC). A**n international non-profit foundation that studies, research and disseminates IT security solutions.

SECURITY THREATS AND PROTECTIVE MEASURES

According to information reported by public sites, a group of hackers managed to open 2,732 PickPoint package lockers in the city of Moscow on December 4th. PickPoint is a local company with a network of 8,000 lockers located in the cities of Moscow and St. Petersburg. This attack has uncovered important vulnerabilities of parcel lockers and highlight the need to setup proper countermeasures.

The PickPoint parcel lockers, in Russia, were located in open and freely accessible spaces. Furthermore, these lockers communicate with PickPoint's system via the internet. This implies that hackers could access the system and thereby communicate with the lockers, ordering them to open. Unlike PickPoint, Poste Italiane's lockers are positioned in private spaces. The reason is that Poste Italiane uses the lockers as a home delivery backup service for shipments on the Italian territory. Hence, when the postman tries to deliver a parcel and cannot find the receiver, then he can leave the parcel in a close parcel locker. These lockers cannot be placed outdoors. They are placed within areas that have a minimum of protection or controlled access. For example, condominium spaces with doors or porters that control access. In the case of the Emilia Romagna pilot, the lockers are within the municipal administration space. During the installation, the technicians carried out an inspection to verify the conditions to host the lockers and thereby the security conditions to use the service. In addition, Poste Italiane's lockers are produced and developed entirely by Poste, which has control over the entire locker design and implementation process, which integrate payment services in addition to logistical processes.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

Apart from the "physical" measures to secure access to the lockers, Poste Italiane has set up processes and conditions for using the service, which ultimately improve security or protection from attacks by hackers. First of all, there is the issue related to the private use of the box. The box can only be used by users registered in the Poste Italiane platform. Registration requires users to be authenticated by email and telephone number to poste.it before being able to take advantage of the services that the device offers. In addition, an initial authentication is provided by means of a one-time password (OTP) generated by the locker administrator and delivered to the user, which allows registration for the use of the specific locker. Each user can only use the lockers on which he has previously registered, with control of the locker administrator.

To access the box and make shipping and payment, users need to log in to the device. This is done by taking advantage of the free post office app that users can download to their smartphone via the Google Playstore or Apple App Store. If users are authorised for the service, a service card (Punto Poste Da Te card) appears in the app. Hence, there are three levels of access to guarantee security: users must have the Italian post office app, they have authenticated themselves by creating a user of the service and finally log in with the app with the access credentials to poste.it.

For the pilot case of the INDIMO project, in Monghidoro, project partner ITL (Institute of Transport and Logistics) will register the users to enable them to use the lockers. ITL will create forms with one-time password (OTP) codes to distribute to users requesting access to the service. The users will complete the registration procedure for the service online and subsequently access the Poste Italiane app by entering any other additional information. These impersonal codes are delivered on paper. The administrator generates them and then distributes them. Following the user registration procedure for the service, Poste Italiane connect users to the locker, and therefore provide access to the contents of the lockers.

The security system set up by Poste Italiane also provides for the delivery of the package by the postman. When the package is delivered, the handheld device available to the postman informs him that the package can be delivered to a parcel locker. The 13-digit consignment note of the package is assigned exclusively to a specific box. When the postman approaches and scans the code of the package to be delivered, the box opens and the postman can deliver the package. When the locker is closed, the user receives a push notification on their device containing information on the package delivered (there are sensors that recognize / validate the presence of the package). When the user accesses the app, the Punto Poste service card informs him that there is a package waiting in the locker and the QRCODE is shown which can be used to collect the delivered package.

In the case of Pick Point in Russia, remote communications between the central server and the parcel lockers take place over the public Internet. This exposes lockers to various vulnerabilities. Poste Italiane lockers communicate with the Poste Mobile SIM and on a private APN (Access Point Name). Therefore, internal services are not exposed on the Internet. Additionally, as specified above, users must authenticate to the app, providing an additional layer of security.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

The SIM CARDs used are profiled to work with mail services with applets registered on the assigned device. Therefore, communication is only passed if used on that specific device. In the event of a hacker opens the box, takes out the SIM and uses it on a different device, this would not work. At the time of installation, the SIMs are registered only on the assigned device and pass communication only to and from the assigned device. So, if you swap the SIMs, the lockers would not work.

SIM cards are passive. It is not possible to open the boxes remotely. Also, not all cells can be opened at the same time. The boxes are assigned to single shipments or to single codes. You should authenticate and activate the codes manually.

A successful attack involving unauthorized access to steal information and money should overcome further obstacles posed by payment systems. Physically there is no information on SIM cards, they are completely stateless.

In Russia it is possible to open the boxes remotely because the software allows it. For Punto Poste it is not possible to make calls from individual mailboxes, which open only on request. The user arrives at the box, he does not authenticate because he authenticates with the app, on which the notification containing the QR code to be used to collect the package is generated. The user approaches and shows the QR. If correct, the code is recognized by Poste Italiane, the cell is searched, receives the communication and is opened.

When collecting the package, Poste Italiane uses the authentication carried out on the app. To make a shipment, users first authenticate themselves on the box and then select the desired functionality, choose the suitable cell available and deposit the shipment inside it.

Delivery is a prerogative of the Poste Italiane group. Only Poste Italiane Group personnel can access the box. In case of deliveries by other couriers, the user can transmit the code (generated by the app) to that courier to open the cell booked in advance or to pre-authorize the consignment waybill (always through the appropriate functionality of the app). The cell reservation can also be used to exchange objects, for example keys, with other family members or trusted people, by communicating the code for opening the cell to the other person. This service is also active in the Monghidoro pilot.

Also, for using the payment services, the users must log in to the locker using an access QR Code generated by the app. Then they can select the desired operation (between payment of postal bills and top-ups), choosing the physical or digital payment method enabled.

Service Accessibility

Concerning the accessibility to the service, the height of the screen has been lowered to facilitate access. This make easier to access the service for people with reduced mobility and can help older people, while for foreign people there are not specific inclusivity actions promoted.

Data about the age of users are not stored in the app or mobile phone, but are exchanged with the locker on a private network. So, data are not disclosed, nor are easily accessible by hackers. The postman only receives a message indicating the locker

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

to place the package. Therefore, no type of information about users is stored or communicated.

It can be confirmed that these services comply with GPDR requirements.

Monitoring: the boxes have internal sensors that monitor their status. A vibration sensor that measures if it is shaken, or if someone tries to force the locks. If the motion sensors detect a break-in, the security room receive a warning to intervene. The state of use of the individual boxes is also monitored, to check whether they are occupied or not, i.e., a volumetric sensor is used. An opening sensor is present in the tailgate, and if it is opened it sends signals to the control room. There is a process in case of maintenance to signal in advance that the door of the specific locker will be opened. The locker signal and the power supply are periodically monitored. In the event of anomalies relating to the status of the power supply or the locker signal, a warning is triggered for the control room indicating a possible infringement.

EFFICIENCY / EFFECTIVENESS IMPACTS

Performance impacts are computed by using a Business Impact Analysis (BIA). This is a systematic process to determine and evaluate the effects of the interruption of critical business operations, after a relevant disruptive event, e.g. accident, natural disaster, emergency etc.

Budget to allocate on security depends on the BIA classification and it is a cost that is dynamically updated depending on threats, likelihood, and impacts.

The implementation of the GDPR has followed a specific investment budget.

6.1.2. PILOT 2 - Antwerp

FORMAL / INFORMAL MANAGERIAL PROCESSES

A formal managerial process has been established by the organisation managing the service (IMEC) and can be summarized with the following steps:

- **Governance.** Governance is ensured through the definition of roles and responsibilities related to privacy concerns.
- **Training and awareness.** Examples of activities performed are (but not limited to) person training sessions, eLearning's, regular information sharing on best practices and awareness sessions.
- **Privacy Incident management.** Existing incident management procedures have been updated to include privacy related incidents.
- **Data subject requests.** Subjects can request their data, and eventually can contact the appointed Data Protection Officer to receive a more accurate reply.
- **Third Party Management.** This includes handling of data processing agreements, audits of existing suppliers, assessment of new suppliers.
- **Privacy by design / default.** IMEC has established processes and milestones in the project management processes to ensure that privacy is include from the start. Activities related to the processing of personal information are subject to a risk evaluation. Data Privacy Impact Assessments are also performed

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

accordingly, answering to possible ethical concerns also considering the sensitivity of the managed data.

- **Policies and guidelines.** Necessary policies are implemented and communicated to the organization. Personal information is performed in line with GDPR and IMEC policies
- **Information security and physical security.** This is managed by the Information Security Officer and include requirements derived from the GDPR, advices from protection authorities and market information. Protection and processing of personal information is also controlled and monitored.
- **Regular audits and monitoring.**

Apart from the above company guidelines to manage cybersecurity, some additional measures had to be established for the Proof-of-Concept development and demonstrator. These measures aim to prevent cybersecurity risks and eventually mitigate those in case an attack is performed during the demonstrations or tests. The following measures are planned / being implemented:

- Limit physical access to hardware and software.
  - Beacons are placed and guarded before tests and removed afterwards. IMEC employees are present during the whole duration of the test and the risk of tampering with beacons is minimal.
  - Smartphones used in the test are owned and configured by IMEC. The application will be installed on these devices by an IMEC developer. No distribution of the application is envisioned. Users will have access to these smartphones only during the test.
- Ensure correct feedback to users.
  - Software mechanisms will be in place in the application to ensure that when any malfunctioning is detected (e.g., network connection lost), the user will be informed appropriately.
  - In person assistance is provided during the test, so that when an error that could not be programmatically detected happens (e.g., received traffic light status does not match actual traffic light status), an IMEC employee can intervene appropriately, e.g., by warning that a defect has occurred. An IMEC employee will always be present during the test to ensure the safety of the user.

3rd PARTIES INVOLVED

The application developed needs to interact with the beacons and eventually later with traffic light providers (Siemens). As of today, there is no connection between beacons and traffic lights, therefore, despite some vulnerabilities may exist, this will not cause any harm or malfunctioning of the traffic lights.

From a data privacy viewpoint, no sensitive data is exchanged between the pilot solution and the traffic lights. Traffic light status, because of its nature, is public knowledge.

In a later phase, a connection with the traffic lights will be established. For instance, the solution could request for green phase or request an extension of the green time at the crossing. Also, in this case data privacy concerns are not expected, since no sensitive

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

data is exchanged. Nevertheless, the data exchange may open for a cyberattack that could manage to command/alter traffic lights status. Therefore, mechanisms to avoid unauthorized control of the traffic lights need to be ensured.

RISK ASSESSMENT

The results of the risk assessment are summarized in the matrix in Figure 3, where probability is on the horizontal axis and impact on the vertical. The analysis of the matrix shows that no major risks have been identified in the pilot, where all the risks are clustered in the bottom-left section of the diagram (green area). The risks that scored relatively highest are the following:

- Unauthorised use of credentials allowing access to information systems.
- Unauthorized physical access to premises (to steal or destroy devices or data).

The experts interviewed perceive these risks as very low, yet in case these take place, the potential impacts can be important.

The respondents highlighted two additional risks that could be relevant for users with special needs:

- **Transmission of incorrect traffic light information** (software malfunctioning). In case of a software malfunctioning, perhaps provoked by an intruder, reduced vision persons may receive green light signal when actual phase is red, resulting in crossing during red phase The likelihood is very low, 1, but the impact very high, 5.
- **Spoofing**. This event may be similar to the previous, but slightly wider in terms of potential cascading events that could happen when data is transmitted between beacons and receivers. Also in this event, likelihood is scored 1, but impacts are very high, 5.

During the interviews it was mentioned that likelihood is low considering the demonstrator context. There will be limited access and users with special needs will be accompanied and assisted during the demo, in order to maintain the necessary safety level. Likewise, the possibility of an external intruder is remote. However, in the event of a large-scale implementation these risks will need to be taken into consideration with slightly higher levels of likelihood and impacts.

PROTECTIVE MEASURES

The following measures are indicated by the pilot (apart the processes indicated as "tacit" previously):

- Participants are guided by an IMEC employee or mobility guide so when the system fails to deliver correct traffic light information, this person can ensure the participant's safety.
- Any authorization keys or mechanisms are kept safely by IMEC employees on IMEC owned devices. Test devices to be used by participants during the test are owned and maintained by IMEC, no access given to 3rd parties until day of test.
- Tests are set up and performed in presence of IMEC employees to prevent physical tampering with setup. Limited time window in which infrastructure is

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

setup in public environment makes it unlikely that a cyber-attack (e.g., spoofing Bluetooth beacons) can be prepared to take place.

- Protection of API access codes. The access codes to communicate with external systems that expose the TLC will be hardcoded in the application during installation on a device. This would not be a secure solution for distributed applications on devices owned by 3rd parties. Since we control all devices on which the application is to be installed, there cannot be unauthorized access (see above) if the device itself is safe and protected.
- Secure connection. The application will be communicating with the Traffic Light Controller via wireless communication technology (e.g., 4G) over the cloud. The team is unsure which protocol is to be used, but they can safely assume that the configuration of the smart light operator will be secured (e.g., via end-to-end encryption, via https, etc.). There is a risk for eavesdropping during this communication, so special attention will be given to secure this connection. The impact of eavesdropping remains small, however, since the application in the current scope only reads traffic light information and does not request alterations to the functioning of traffic lights.

EFFICIENCY / EFFECTIVENESS IMPACTS

The three KPIs used to measure the potential impacts of a potential failure are all expected to be affected. In case of failure during the pilot/demonstration, costs are expected to be low. According to the experts, redeployment and postponement of the demonstrator is a minimal cost. Brand/image and sales/profits are expected to be affected only in case of a large-scale implementation. Yet, these are difficult to assess due to the lack of a business model.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

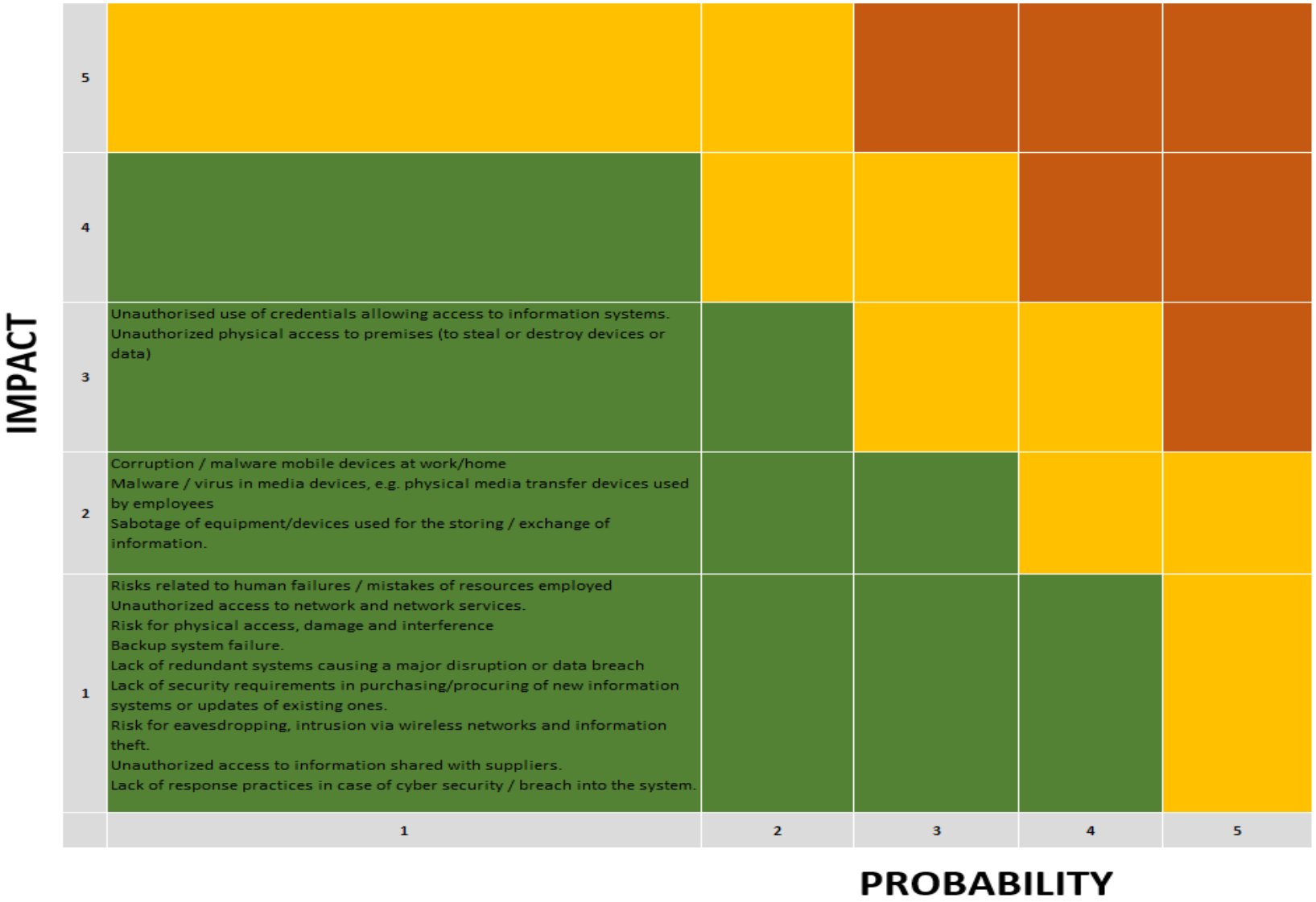


Figure 3. Risk matrix pilot 2 Antwerp.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

6.1.3. PILOT 3 – Galilee

FORMAL / INFORMAL MANAGERIAL PROCESSES

Existing guidelines issued by the Israel National Cyber Directorate recommend the creation of teams for Crisis Management (CM) and Incident Response (IR)[8]. The National Cyber Concept for crisis adds that every organization must be prepared to face cyber threats through structured processes. The scope of the IR team is to prepare the organization overcoming important cyber incidents. Organizations should provide the necessary resources to the team, in order to allow its establishment and operations. Eventually, organizations can hire external cybersecurity services. The CM team need to be an inherent part of the organization and establish communication channels with several functions, i.e. HR, operations, risk management, legal advisers, public relations etc. Yet, they need to liaise with external organizations, like regulators and other cybersecurity experts to receive assistance (Figure 4).

Reporting incidents is a fundamental part of the processes to be established in the organization. For this it is recommended to involve the Cyber Information Security Officer (CISO), or public relations, the CM team, and even the national CERT (Computer Emergency Response Team) to determine whether the incident is part of a larger scale attack. To enhance the resilience of the organization in case of an attack, it is recommended that plans are developed in advance, to facilitate and speed up rapid decision-making during a crisis.

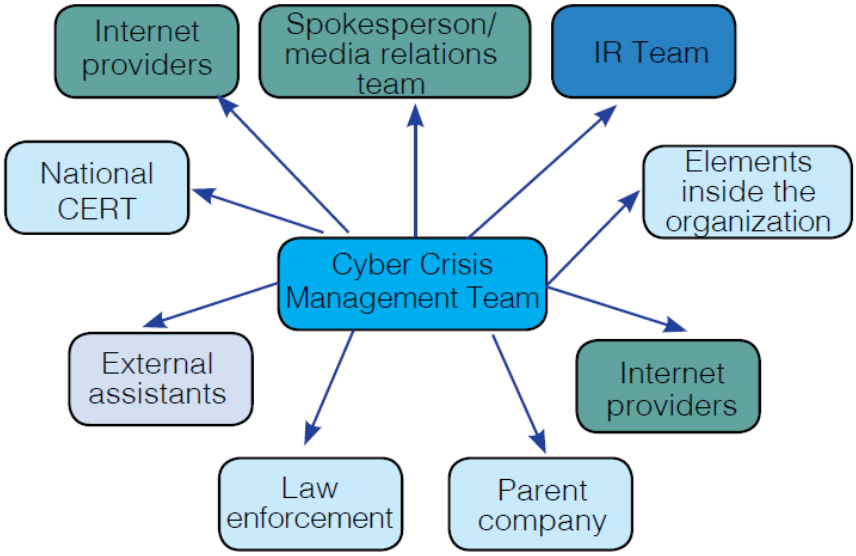


Figure 4. Interface Chart of Cyber Crisis Management teams (The Prime Minister's Office – Israel National Cyber Directorate, 2021)

Regarding the IR team, the following technical capabilities are recommended to be secured:

[8] The Prime Minister's Office – Israel National Cyber Directorate (2021), Organizational Preparedness for a Cyber Crisis Characterization & Requirements from Crisis Management Team and IR Team.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

- Collect data like network traffic.
- Analyse and filter data to determine whether a cyberattack is on-going.
- Make changes to the systems to block or remove suspect activities.
- 24/7 real time monitoring.

RISK ASSESSMENT

Several risks are in the midzone of the risk matrix, hence they can all be considered medium risks, for which some actions need to be undertaken. The following threats are considered as having a very low frequency of occurrence (1), while a very high impact (5).

- Risks related to human failures / mistakes of resources employed.
- Unauthorized access to network and network services.
- Risk for eavesdropping, intrusion via wireless networks and information theft.
- Lack of security requirements in purchasing/procuring of new information systems or updates of existing ones.

Next, the following risks have a slightly higher probability of occurrence (2), but the impact decrease by 1 point of the Likert scale used (4).

- Corruption / malware mobile devices at work/home.
- Risk for physical access.
- Sabotage of equipment/devices used for the storing / exchange of information.
- Lack of redundant systems causing a major disruption or data breach
- Unauthorized access to information shared with suppliers.
- Lack of response practices in case of cyber security / breach into the system.

Other risks classified with equal probability (3) and impact (3) are:

- Malware / virus in media devices, e.g. physical media transfer devices used by employees.
- Unauthorized physical access to premises (to steal or destroy devices or data).

Finally, two risks are seen as highly probable (4), but low impacts (2).

- Backup system failure
- Unauthorised use of credentials allowing access to information systems.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

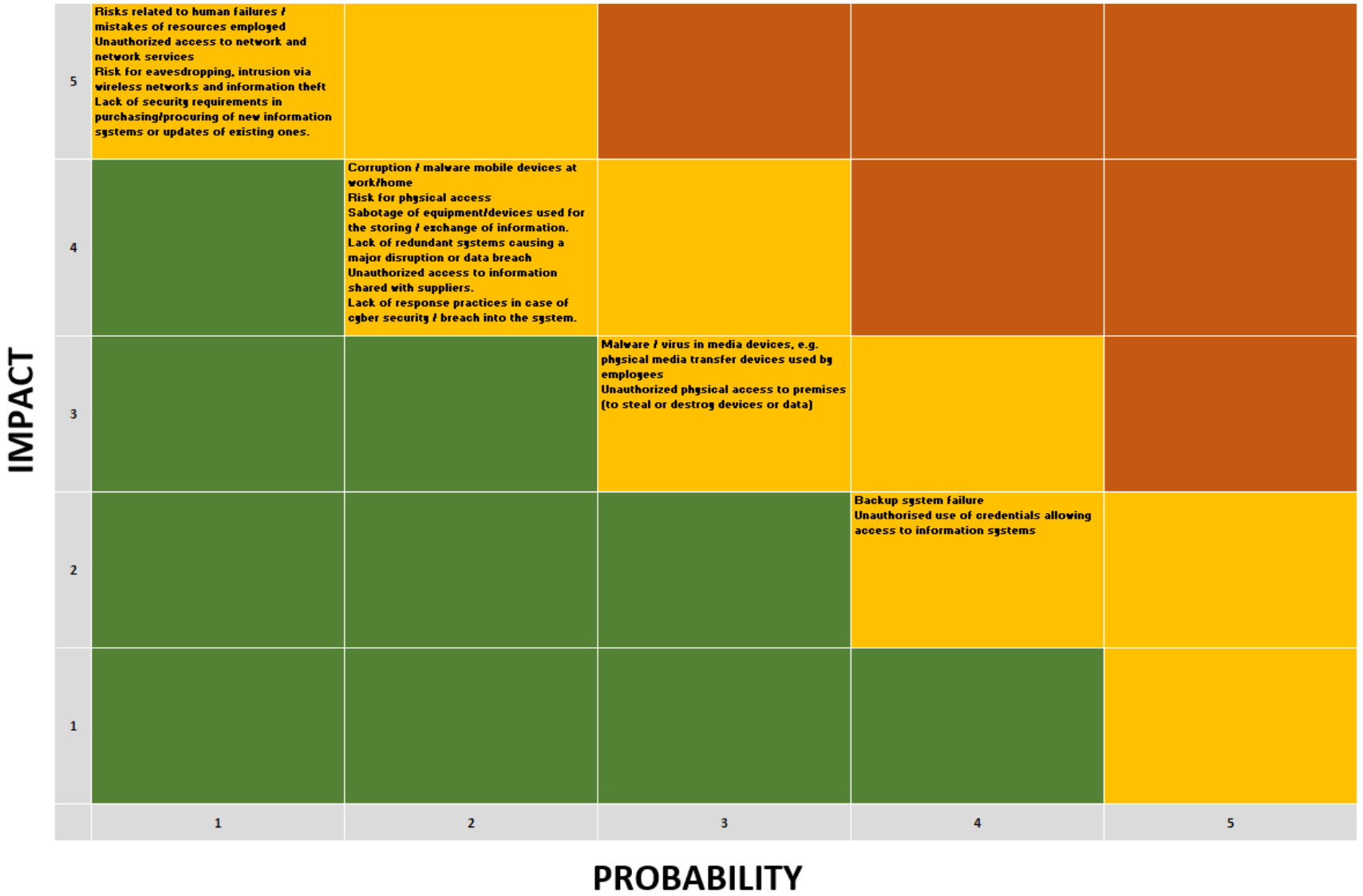


Figure 5. Risk Matrix Pilot 3, Galilee

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

PROTECTIVE MEASURES

Israel National Cyber Directorate recommends the establishment of clear and structured processes to report incidents and thereby setup for rapid response and intervention:

- Identify stakeholders and link them. Especially official national bodies in the field.
- Notify the incident to them as soon as possible. In case the organization is part of wider supply chain, the communication should identify the relevant tier 1 stakeholders.
- Carry out drills / training / exercise to detect and recover from incidents.
- Develop recovery plans a priori.
- After the incident, involve the legal stakeholders to proceed with legal actions against the attackers.

From a technical viewpoint, a toolbox is recommended in the same guidelines. This consists of the following technical capabilities:[8]

- Network traffic sniffer.
- Hard drives clones.
- Memory dumps.
- Tools to identify malicious activities.
- Tools for forensic activities.
- Tools to recover deleted data.

Cybersecurity also implies protecting from physical access to computer infrastructure. Hence, physical security measures need to be considered and implemented, e.g. doors and physical gates activated with magnetic cards (or other identification technologies), CCTV systems and alarm systems. Finally, vetting of employees' background has to be performed by the security personnel in the company. Likewise, employees need to be trained, in order to raise their awareness about being involuntarily targeted and exploited to perform a cyberattack. **Errore. Il segnalibro non è definito.**

6.1.4. PILOT 4 – Madrid

FORMAL / INFORMAL MANAGERIAL PROCESSES

The platform and the operator operating this pilot are both small non-profit cooperatives, which at the moment have not yet established formal managerial processes to govern cybersecurity threats. Informally, the company developing the service (CoopCycle) follows standard best practices and ensures that relevant software applications are updated regularly. There is one employee that monitors server logs daily in order to detect any possible malicious activity. The company expects that more monitoring features will be activated in the future, e.g. online scanners, and pen-testing software.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

3rd PARTIES INVOLVED

The mainly third parties services used are: cloud servers' providers (ovh), databases, geocoding APIs for geolocation, and Stripe for process payment (credit cards info did not pass through their own server, but they are managed by Stripe[9]). The platform pays particular attention to the privacy of users whose personal data are not shared for marketing analysis. CoopCycle does not activate cookies for data analytics. While the mobile application does not have social login, it is possible to use Facebook to login in the browser version. In that case a minimum of user information is shared through Facebook login at the moment of the registration.

RISK ASSESSMENT

For this pilot it is possible to identify low, medium and high risks. The risks that are considered low, are listed below:

- Risk for physical access (prob = 1, Impact 4).
- Backup system failure (prob = 1, Impact 4).
- Sabotage of equipment/devices used for the storing / exchange of information. (prob = 1, Impact 3).
- Unauthorized physical access to premises (to steal or destroy devices or data) (prob = 2, Impact 3).

The risks that ultimately scored as medium are the following:

- Unauthorized access to network and network services. (prob 2, impact 5).
- Risk for eavesdropping, intrusion via wireless networks and information theft. (prob 2, impact 4).
- Lack of security requirements in purchasing/procuring of new information systems or updates of existing ones. (prob 2, impact 4).
- Unauthorised use of credentials allowing access to information systems. (prob 3, impact 4).
- Unauthorized access to information shared with suppliers (prob 3, impact 3).

The last cluster concerns the high risks, for which immediate actions need to be undertaken by the company (prob 3, impact 5):

- Risks related to human failures / mistakes of resources employed.
- Corruption / malware mobile devices at work/home.
- Malware / virus in media devices.
- Lack of redundant systems causing a major disruption or data breach.
- Lack of response practices in case of cyber security / breach into the system.

Additional risks flagged by the pilot, are Distributed Denial or Service attacks (DDOS). The likelihood and impacts are both scored at level 3, indicating a medium importance of the risks.

[9] https://stripe.com/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

PROTECTIVE MEASURES

The company is using the following protective measures:

- Access control list, different kind of users' access to different kind of data.
- Rules are implemented, for different level of information.
- APIs protected by tokens, renewed hourly.
- Manually monitoring of activities, to detect potential breaches in the system.

The company is also addressing the needs of vulnerable users by implementing additional security measures, responding also to possible ethical issues connected with data security and privacy. These are two factor authentication, encryption of sensitive data in databases and offline data accessibility, to overcome possible outages of external services, i.e. creating redundancy.

EFFICIENCY / EFFECTIVENESS IMPACTS

Overall costs of cybersecurity are expected to be significant. In case of a breach in the system, new databases will need to be created and new servers will need to be setup. This would imply a shift of focus of developers' resources from operations to security (stopping the attack), hence generating costs in terms of losses of operational performance. The brand image of the company could also be affected in case of an attack. The company may expect an overall loss of trust and a potential reduction of customers using the platform. In this case, social network and Press Releases could help re-establishing trust.

Apart the impacts on costs to create databases and reconfigure services, the company expects losses in profits, due to reduced sales. If the platform is not usable, members will not be able to access, generating a loss in sales and profits.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

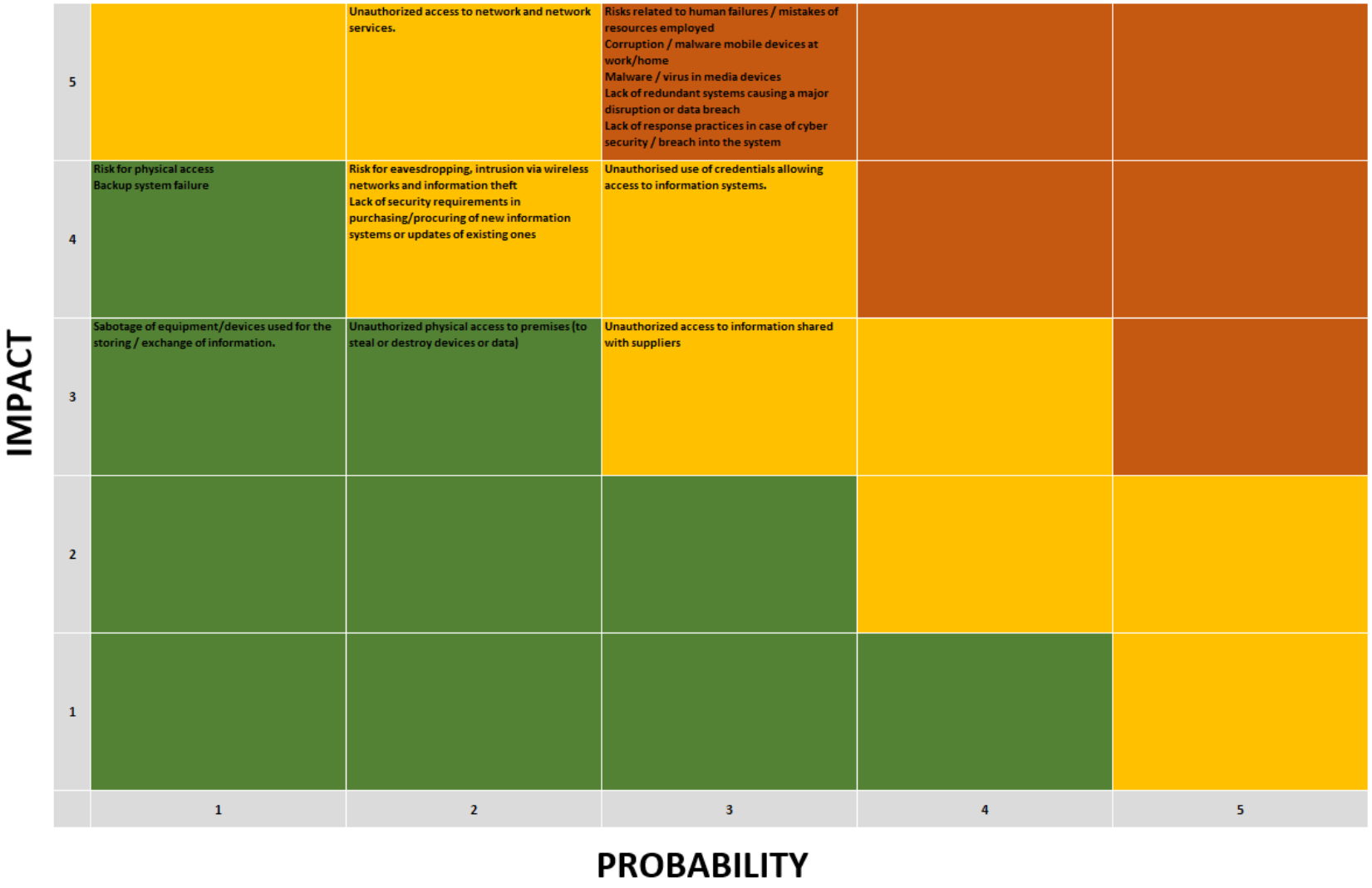


Figure 6. Risk Matrix Pilot 4, Madrid.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

6.2. Baseline questionnaires

To understand to what extent the tools developed in WP2 as part of the INDIMO Digital Mobility Toolbox (and specifically the Guidelines for cybersecurity and personal data protection) have an impact on user acceptance of digital mobility and delivery services in INDIMO pilots, data on Trust, Privacy and Perceived Security were collected by each pilot. This data collection is based on the guidelines for pilots included in the Pilot handbook (D3.1) and on the assessment proposed indicators included in the INDIMO Evaluation framework (D4.1).

The data refer to the five INDIMO pilots and the variables on trust, privacy and perceived security such as *information about use of data, care about privacy, no disclosure to third parties, information about risks and ethical data sharing* have been investigated together with other variables on user acceptance, gender, inclusivity and accessibility and presented in D4.2 Baseline data report for pilots.

6.2.1. Baseline data collection

The Baseline survey was conducted throughout the five (5) pilots between December 2020 and April 2021. A total of **130 answers** were collected among users of the digital mobility and delivery services of the INDIMO pilots. The degree of development of each digital mobility and delivery service and its users are different, therefore, the number of answers by pilot varies: from the 78 answers of the food delivery service in Madrid collected through an online questionnaire linked to the purchase process to the 5 answers of the Galilee pilot where the survey was carried out through a face-to-face interview to the few regular users of the informal service. During the baseline survey (beginning of 2021) the P1-pilot still did not have the service running at the designed location (Monghidoro town-Emilia Romagna). The baseline survey has been designed to be answered by current users of the "Punto Poste Da Te" digital lockers service. Therefore, this baseline survey has been conducted in Rome where digital lockers have been installed in residential and office buildings.

Most respondents were women (56%), belonging to age groups 25-34 (48%) and 35-44 (28%) and holding a master (45%) or a bachelor (36%) certificate. These characteristics of the sample are in line with the key aspect of the mobility in general where the women show higher mobility patterns between 29 and 49 (Di Ciommo et al., 2020). Most of the times this women hypermobility need is not satisfied by the current transport system. Therefore, the introduction of new digital mobility services will be more than welcome by women, especially when they are well educated with a higher level of digital skill. Table 4 provides a synthetic view of the data collected.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

Pilot Age	Gender % answers Female	Male	Not decl.	Not binary	Total No. of answers	Total % answers
Pilot 1						
18-24	8%				1	8%
25-34		8%			1	8%
35-44	31%	23%			7	54%
45-54	8%	15%			3	23%
55-64	8%				1	8%
Total P1	**54%**	**46%**			**13**	**10%**
Pilot 2						
25-34	11%	11%			2	22%
35-44	22%	11%			3	33%
45-54		11%			1	11%
55-64	22%				2	22%
65-74		11%			1	11%
Total P2	**56%**	**44%**			**9**	**7%**
Pilot 3						
18-24	40%				2	40%
25-34	20%				1	20%
35-44	20%				1	20%
65-74	20%				1	20%
Total P3	**100%**				**5**	**4%**
Pilot 4						
18-24	6%	1%			6	8%
25-34	33%	17%	4%	1%	43	55%
35-44	13%	13%	3%		22	28%
45-54	5%	3%			6	8%
55-64	1%				1	1%
Total P4	**59%**	**33%**	**6%**	**1%**	**78**	**60%**
Pilot 5						
18-24	4%				1	4%
25-30		4%			1	4%
25-34	32%	24%		4%	15	60%
35-44		16%			4	16%
36-40		4%			1	4%
45-54		4%			1	4%
51-55	4%				1	4%
66-70		4%			1	4%
Total P5	**40%**	**56%**		**4%**	**25**	**19%**
Total	**56%**	**38%**	**4%**	**2%**	**130**	**100%**

Table 4. Baseline survey descriptive data from D4.2

In the following section, tables (Table 5 to Table 9) and figures (Figure 7 to Figure 11) present the baseline survey results per each pilot. The table includes three descriptive measures: the average of given assessment values; the "Bottom-Two-Box" (BTB), that is the summation of responses Strongly disagree (1) + Disagree (2) and which gives a measure of the intensity of disagreement; the "Top-Two-Box" (TTB), that is the summation of responses Strongly agree (6) + Agree (5) and which gives a measure of the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

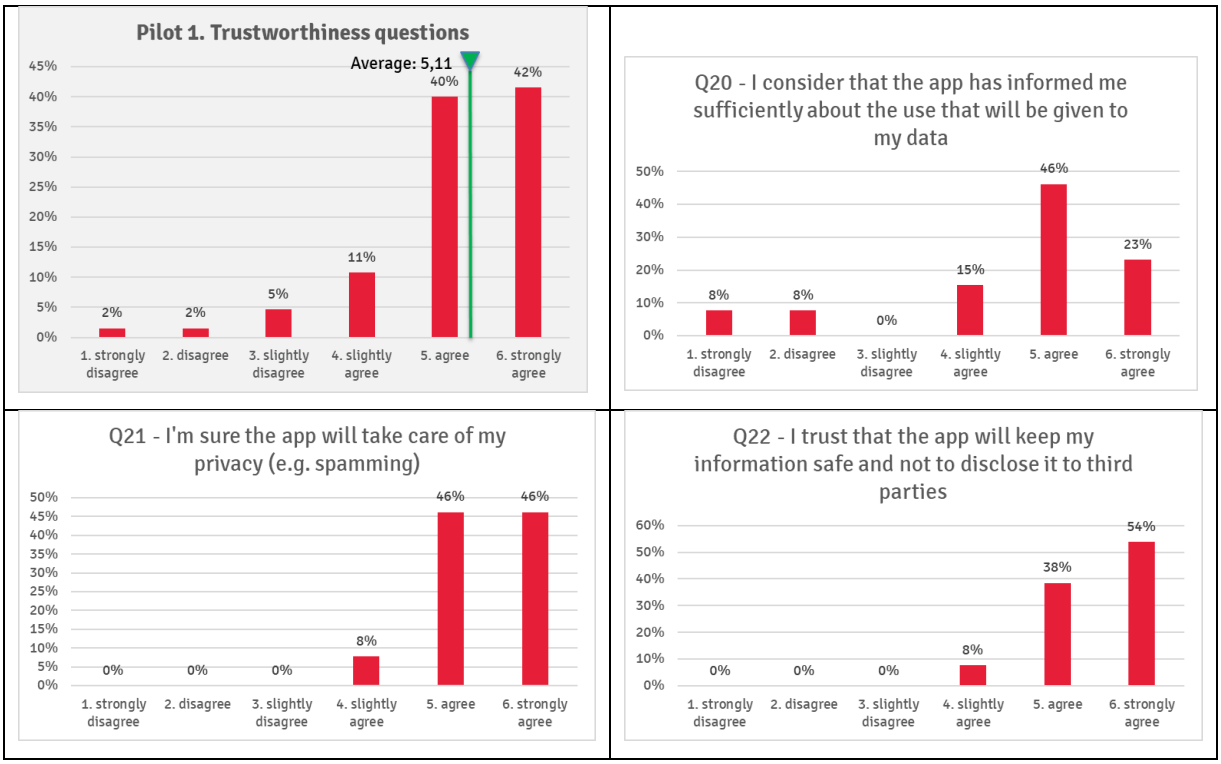
intensity of agreement for the given statement, while the figure shows the graphical distribution of the 5 answers on cybersecurity and personal data protection and a comprehensive diagram of the 5 identified variables. The detail of this figure helps to better understand the nuances in the perceptions and attitudes of each pilot's current users in terms of cybersecurity and personal data protection.

6.2.2. Pilot 1: Digital Lockers – Emilia Romagna

For P1- the Baseline questions analysis reveal a good level of Trust, Privacy and Perceived security with an average for all questions at 5,11. Bottom-Two-Box is at 0% for 4 of the 5 questions, reaching an 15% only for Information about use of data (Q20), then highlighting the concern about the provision of transparent information on data protection and use. The indicators with the lowest Top-Two-Box are Information about use of data (Q20) and Information about risks (Q23).

Variable (Question)	Information about use of data (Q20)	Care about privacy (Q21)	No disclosure to third parties (Q22)	Information about risks (Q23)	Ethically data sharing (Q24)	Trustworthiness variables / questions
Average	4,54	5,38	5,46	4,92	5,23	**5,11**
Bottom Two Box	15%	0%	0%	0%	0%	**3%**
Top Two Box	69%	92%	92%	69%	85%	**82%**

Table 5. Pilot 1: Summary table



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

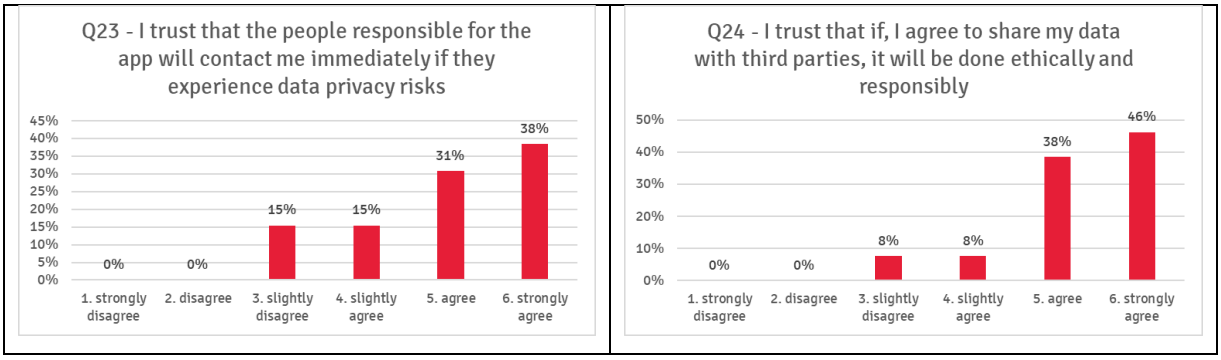


Figure 7. Pilot 1: Distribution of answers on trustworthiness

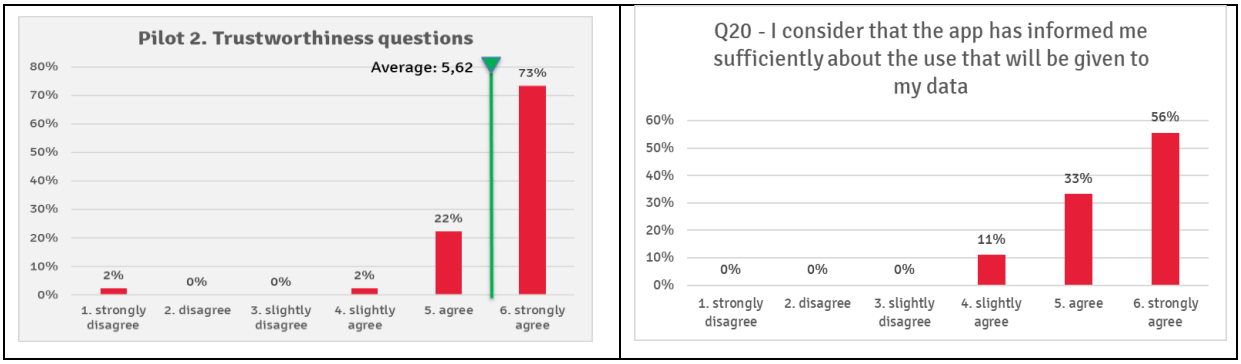
For some variables such as "Information about risks", there is some slight distrust that should be investigated and considered when new solutions will be designed for making the digital lockers services more inclusive. A clear requirement highlighted by end-users in the qualitative fieldwork was related to the training request that could be used for intervening on the trust perception.

6.2.3. Pilot 2: Inclusive traffic lights - Antwerp

In P2, the baseline questions disclose a very good level of trustworthiness with an average for all questions at 5,62. Bottom-Two-Box is at 0% for 4 of the 5 questions, reaching an 11% only for Ethically data sharing (Q24), then highlighting the concern about the provision of clear ethical framework for data protection and use.

Variable (Question)	Information about use of data (Q20)	Care about privacy (Q21)	No disclosure to third parties (Q22)	Information about risks (Q23)	Ethically data sharing (Q24)	Trustworthiness variables / questions
Average	5,44	5,78	6,00	5,44	5,44	**5,62**
Bottom Two Box	0%	0%	0%	0%	11%	**2%**
Top Two Box	89%	100%	100%	100%	89%	**96%**

Table 6. Pilot 2: Summary table



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

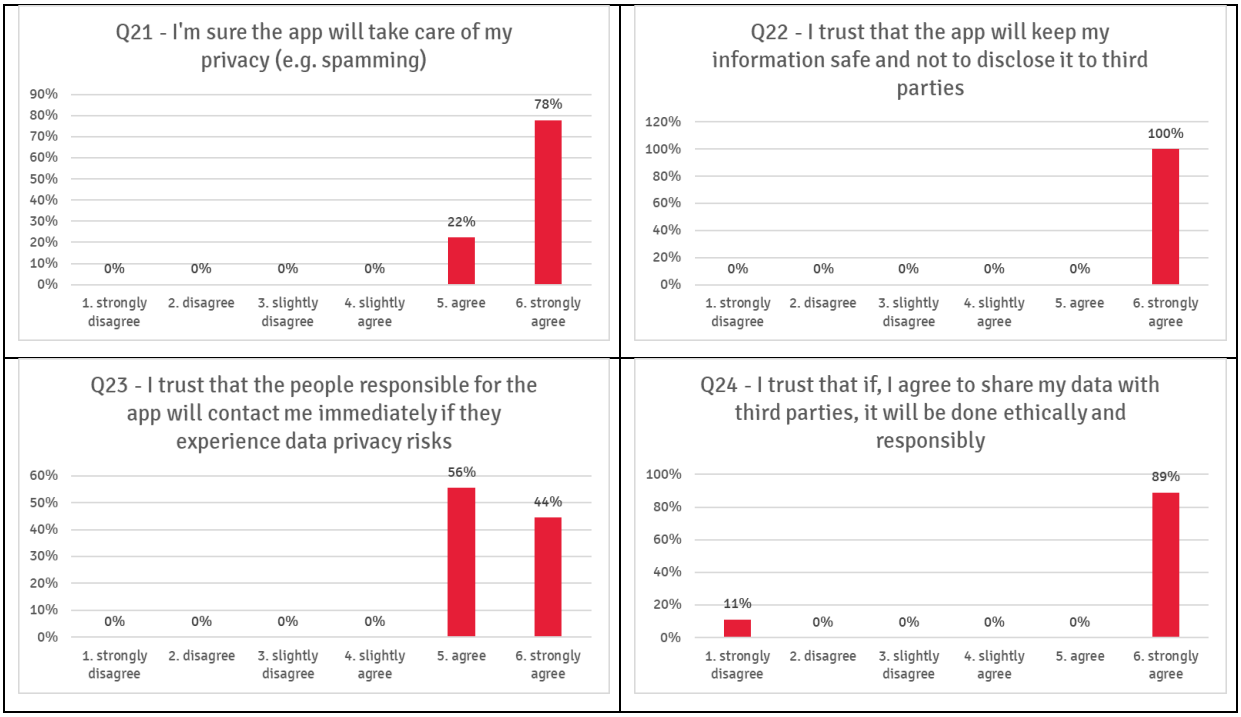


Figure 8. Pilot 2: Distribution of answers on trustworthiness

The dissonant voices for P2 are very few. However, the second phase of the pilot implementation should pay attention to these few discrepant opinions.

6.2.4. Pilot 3: Informal ride-sharing in ethnic towns - Galilee

In P3, the baseline questions disclose a fair level of trustworthiness with an average for all questions at 3,88. Even more than for Antwerp, in this location the small number of answers (5) does not allow for sound quantitative considerations. We can still say that the trustworthiness should be based on the provision of transparent information on data protection and use.

Variable (Question)	Information about use of data (Q20)	Care about privacy (Q21)	No disclosure to third parties (Q22)	Information about risks (Q23)	Ethically data sharing (Q24)	Trustworthiness variables / questions
Average	3,80	3,80	4,40	2,60	4,80	**3,88**
Bottom Two Box	0%	0%	0%	40%	0%	**8%**
Top Two Box	0%	20%	40%	0%	80%	**28%**

Table 7. Pilot 3: Summary table

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

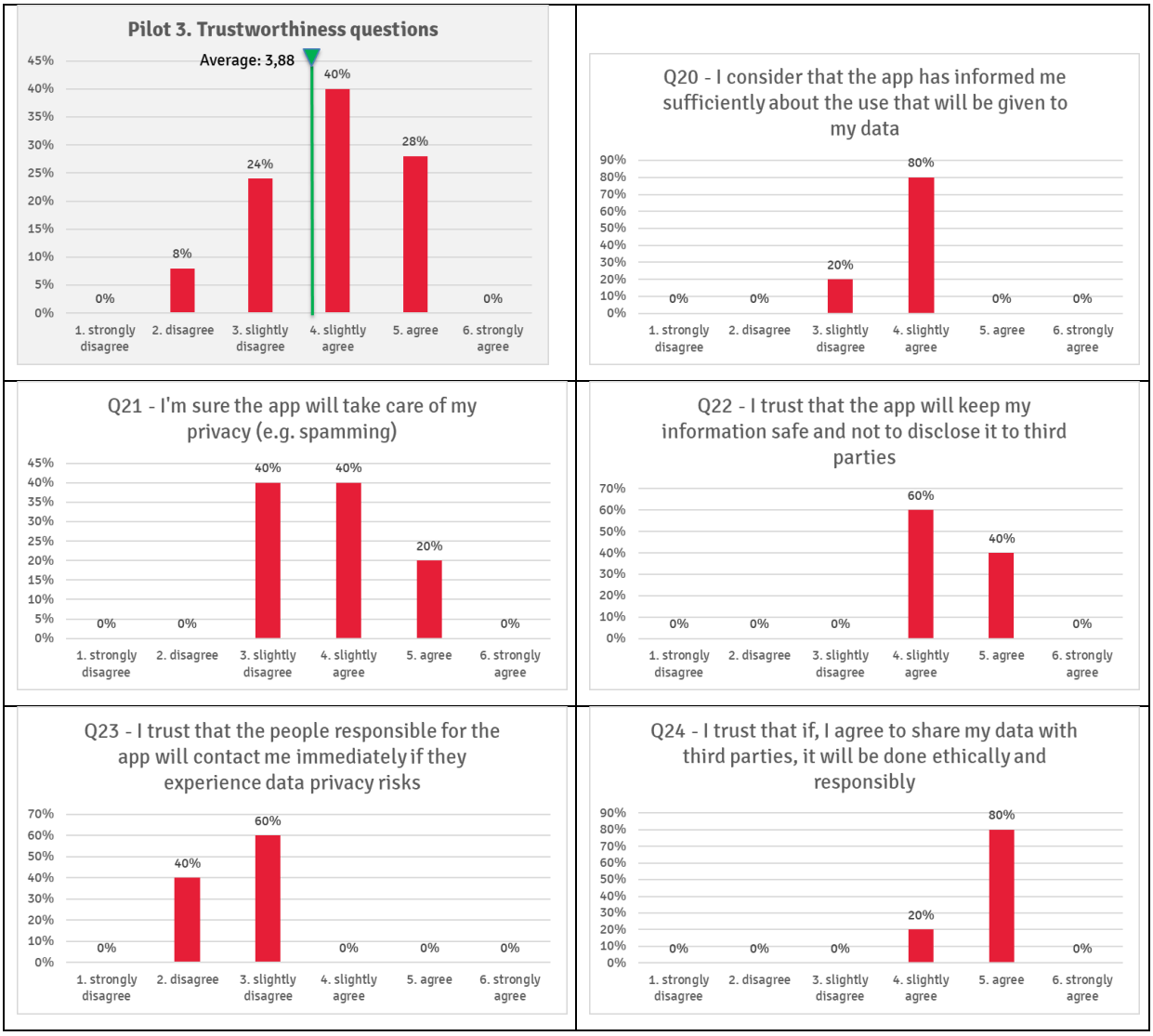


Figure 9. Pilot 3: Distribution of answers on trustworthiness

Currently, few users seem to show some concern about trust and privacy, and less about perceived security.

6.2.5. Pilot 4: Cycle logistics platform for delivery healthy food - Madrid

In P4, the baseline questions on cybersecurity and personal data protection show a middling level of trustworthiness with an average for all questions at 4,61. Bottom-Two-Box is at 6% for 4 of the 5 questions, reaching an 10% only for Information about risks (Q23), then stressing the worry for a prompt and shared reaction in case of data privacy risks. The indicators with the lowest Top-Two-Box are Information about use of data (Q20) and Information about risks (Q23).

Variable (Question)	Information about use	Care about	No disclosure	Information about risks	Ethically data	Trustworthiness variables /

	of data (Q20)	privacy (Q21)	to third parties (Q22)	(Q23)	sharing (Q24)	questions
Average	4,54	4,55	4,76	4,45	4,74	**4,61**
Bottom Two Box	6%	6%	6%	10%	6%	**7%**
Top Two Box	55%	59%	69%	54%	60%	**59%**

Table 8. Pilot 4: Summary table

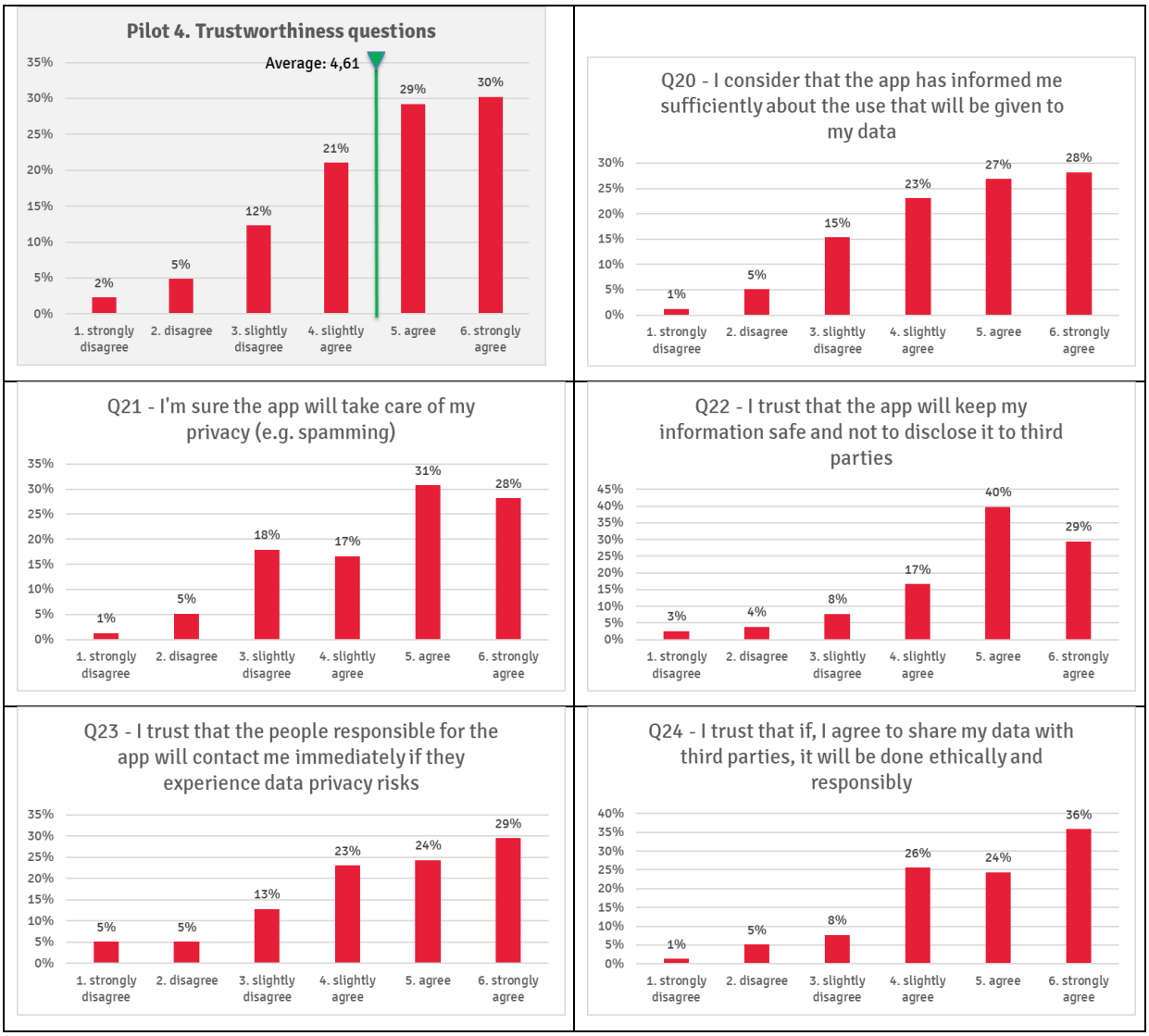


Figure 10. Pilot 4: Distribution of answers on trustworthiness

P4 allows us to consider that current users, even when they use the services, have still some concerns about the trust, privacy, and perceived security.

6.2.6. Pilot 5: On-demand ride-sharing integrated into multimodal route planning - Berlin

Also, in P5, the baseline questions display a middling level of trustworthiness with an average for all questions at 4,77. Bottom-Two-Box is higher than the rest of the pilots,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

ranging from 4% to 20% only for Care about privacy (Q21), then emphasising the concern users have about the provision of transparent information on data protection and use. The indicators with the lowest Top-Two-Box are, like in other pilots, Information about use of data (Q20) and Information about risks (Q23).

Variable (Question)	Information about use of data (Q20)	Care about privacy (Q21)	No disclosure to third parties (Q22)	Information about risks (Q23)	Ethically data sharing (Q24)	Trustworthiness variables / questions
Average	4,28	4,60	5,12	4,68	5,04	**4,77**
Bottom Two Box	12%	20%	4%	8%	4%	**8%**
Top Two Box	52%	80%	84%	64%	76%	**70%**

Table 9. Pilot 5: Summary table

Figure 11. Pilot 5: Distribution of answers on trustworthiness

In P5, the measured variables show a lower indicator of trust and privacy.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

7. Recommendations for pilots

The following section contains recommendations for each pilot to improve privacy and security within the project activities and beyond with attention to gender issues related with cybersecurity.

7.1.1. PILOT 1 – Emilia Romagna

The Italian pilot shows a high degree of knowledge of security and protection from cyberattacks. The company is aligned with most of the security standards and certifications available in the market, namely ISO9001, ISO27001: 2013, ISO 2000, NIST and GDPR. The company has both the know-how and the technical skills to properly anticipate and tackle various vulnerabilities and adopts security approaches by design, then tests and certifies solutions before implementation. Similar importance is given to physical security, therefore to the protection of ICT resources that could ultimately facilitate a cybercrime.

From a user's perspective, the experience of the pilot so far showed the need for taking into account the organisation of training for users about the use of the service and possible risks, with the involvement of local stakeholders.

However, there are some improvements that could benefit seniors and foreigners who need to access the service, but which are not currently in the roadmap for development by Poste Italiane and therefore will not be taken into consideration for the next pilot activities within the project.

These are as follows:

- Adoption of low-screen lockers to facilitate access for wheelchair users to enhance security for the usage of lockers (e.g. people could need to ask for help if the access is not accessible with wheelchairs).
- Implement a solution to place packages in easily accessible lockers if users have reduced mobility to increase the security for the usage of lockers (e.g. people could need to ask for help if lockers are out of their reach).
- Ability to choose preferred language in mobile phone app and parcel locker screen. Changing languages can improve information retrieval and hinder any other fraudulent attempts to exploit language gaps.

7.1.2. PILOT 2 – Antwerp

The pilot in Antwerp is working to develop and demonstrate a Proof-Of Concept. This implies that much of the communications between devices as well as the users' interaction with the system will take place in isolated and controlled environments. Hence, risks can be considered as low, if the following conditions can be controlled during the development and demonstration stages:

- **Limit physical access to hardware and software.**
  - Beacons need to be stored in safe places with controlled / authorized access, in order to avoid manipulation/tampering.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

  - During the tests, they should be properly guarded by IMEC employees.
  - Once removed, the beacons need to be placed back in the safe storage with controlled /authorized access.
  - Similarly, the smartphones need to be stored in safe places, and only authorized developers from IMEC should be able to configure / install the application.
  - Protect codes used for API access, e.g. hardcoding the access codes.
- **Ensure resilience / incident avoidance in case of malfunction or wrong information communicated to users.**
  - The software in the device should include mechanisms in place to ensure detection of malfunctions and thereby warn the user properly.
  - Provide assistance on the field during the tests, in order to react properly in case of a malfunction or any imminent risks that could compromise the safety of the users involved.

Apart the demonstration phase, other risks and necessary recommendations to control cybersecurity concerns must be considered. From a user perspective, as emerged from the baseline questionnaires, there is the need to provide a clear ethical framework for data protection and use, with the strengthen of a privacy by design approach and following specific strategies. The pilot is planning to connect traffic lights to the system developed, which exposes the pilot to risks like corrupting the data exchanged between users, beacons and traffic lights. For instance, an intruder could manipulate the system and thereby transmit improper traffic light information. This event could result into life threatening outcomes or injuries (especially for users with special needs, e.g. reduced vision). Hence, our recommendation is to adopt solutions like 1) allow data exchange only across private networks, 2) cryptography, 3) traffic monitor and anomalies detection. Finally, managerial guidelines like plan-do-check-act approaches will be necessary to continuously monitor the system and be able to capture risks and respond properly.

7.1.3. PILOT 3 – Galilee

The pilot shows good maturity and knowledge about what risks apply and their potential impacts. Some general recommendations can be pointed out based on the national guidelines for cybersecurity developed by the Israel National Cyber Directorate. These include the establishment of 1) a cyber security officer (CISO) and 2) Crisis Management (CM) and Incident Response (IR) teams. Also, it may be worth to consider adopting a privacy by design approach when there will be the re-design of the application during the next project's phases.

Other recommendation for this pilot includes the implementation of the following processes:

- Plan-do-check act management approach
- GDPR compliance
- Payments integrated with external providers, to take advantage of their security solutions.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

- In case third parties' providers are used for geospatial functionalities, developers should ensure that location information is not associated with personal information to prevent data security and ethical issues.
- Traffic monitoring and intrusion detection systems equipped with alerts.
- Provision of clear and transparent information on data protection and use to users.

7.1.4. PILOT 4 – Madrid

In the current stage, the pilot is operated by a non-profit federation of 64 small delivery goods and food cooperatives, including 62 in Europe and 2 in Canada that share a common digital platform. Some recommendations can be put forward for accompanying their current growth and scale up of the solution developed:

- The implementation of standards and guidelines developed in ISO28000 or NIST800 are recommended.
- Usage of technologies for detecting intrusion anomalies, e.g., online scanners, and pen-testing software.
- Integrate payments with external providers, to take advantage of their security solutions.
- Establish processes/routines to control possible mistakes of CoopCycle employees and/or respond to incidents. Perform auditing and drills.
- Establish rules for usage of external devices (e.g. usb devices, personal devices, ecc) at work/home.
- Use backup systems to ensure redundancy.
- Protect APIs using tokens that are renewed hourly.
- Create a process for a prompt and shared reaction in case of data breach and inform users to increase trust.
- To address possible ethical issues connected with the data security aspects it may be worth to work on specific strategies such as Inform.
- Require support from INDIMO cyber security experts for making more secure this growing cooperative platform.

8. General Guidelines

From the analysis of the different data and insights considered in this deliverable, we draw general guidelines for improving cybersecurity and personal data protection in digital mobility services. The guidelines are meant to be used for design and re-design of services with a security by design approach, and for increasing awareness among users about digital data security and possible security risks for them.

8.1.1. Establish processes and procedures

Usually, bigger companies and organisations already have in place plans, processes and procedures for security management and against cyberthreats, while it may be not true for smaller and newer companies and organisations. What is important, especially for

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

new and smaller organisations, is to have in mind that with a scale-up of the service there is the need to include a stronger focus on security. The establishing of a security management system, and the definition of proper processes to manage risks. Having a PLAN-DO-CHECK-ACT style process is a key aspect to consider. ISO27001 is the most common standard for how to manage information security in organisations. Regarding cyberthreats ISO28000 and NIST800 are among the most used standards and guidelines, and they can be applied also to SMEs or small organisations.

8.1.2. Consider the human factors

The increasing complexity of new technologies requires to approach cybersecurity not only from a technical perspective, but to consider and integrate in the cybersecurity strategy also human factors, and organizational perspectives. Human factors can be seen as a "first line of defence" (Pearsons et. al, 2017). Understanding why people make errors or commit violations compromising security is an important step to understand how to create a better security culture, which go beyond the company. Users too must receive proper information and even training to avoid doing errors and reducing risks.

8.1.3. Consider third-party services

Almost every digital service makes use of third-party services for specific features (e.g. geolocalisation, payment, etc). There is the need to understand how the different parties involved are connected and which role they play and prepare for alternatives or contingency plans. Third-party services are useful because they allow to not reinvent the wheel all the time, and also, they could have a high level of security, such as in the case of credit card payment systems. However, if there are major third-party components of your system it is important to consider them, and asses their security for the security of the whole service. An attacker that compromises one of the third-party services used may create a major disruption of the service.

8.1.4. Design for maintenance

Maintenance is a core aspect for security, a system not properly maintained is prone to vulnerabilities and risks. It is important to monitor and quickly apply security updates and patches. Since the majority of cyber-attacks today exploit software vulnerabilities caused by software bugs and design flaws (Jang-Jaccard & Nepal, 2014), paying attention to bugs and vulnerabilities is essential. The vulnerabilities discovered must be fixed or mitigation measures must be taken to reduce the risks. A continuous check and update is better than having larger ones. The system must be designed so that the service is not impacted by security updates.

8.1.5. Monitoring the system

As emerged during the risks assessment, it is important to have in place a monitoring system for checking data traffic and intrusion detection. It will help to prevent and react faster to attack and intrusion to the systems. It must be prevented that communication and data management happen over insecure connections.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

8.1.6. Avoid collecting unnecessary data from users

One of the main ethical issues emerged is the users' concern about data collection and usage. Identify which type of data needs to be collected, stored, processed, transmitted, and limit the data to what is really needed for the service. This can reduce the impact on security and privacy data leakage. Also, vulnerable user groups sometimes need to share more type of sensitive data to fully access a service. Design a way to collect fewer personal data and being able to provide the same service to all groups of people would be an effective way of increasing security and inclusion at the same time. The use of privacy design strategies such as Minimise, Hide, and Separate can help.

8.1.7. Clearly present personal data use to users

Design for security, and design for vulnerable groups, imply to change the way in which the service terms of service and policies are presented. It is important to develop clear and transparent documentation towards personal data usage, terms of service and policies to address data security and ethical concerns. Summaries and checklists can be prepared to clearly present what data is stored and for how long, and what the terms of service are.

8.1.8. Physical security

If physical IoT devices are deployed for managing the service, it is important to pay additional attention to tampering and physical access, to prevent sabotages and attacks coming from a direct access to a device. This can be a relevant issue for smart-city IoT application, which like in the case of the INDIMO Antwerp pilot can have potential issue for people's safety. Also, if third party devices are used, it is essential to prevent the use of vendor default passwords.

8.1.9. Prevent phishing

Phishing is a major concern for users, and especially for vulnerable categories, like in the case of older people or foreigners. To reduce the risk of phishing it is possible to register domains under the company name that are suitable for phishing. Users need to be able to easily report phishing or malicious activities by adding contact and easy to use reporting form in apps, also linking with local cybersecurity associations can be useful (e.g. in Belgium www.safeonweb.be). Providing information and training to users is also another possibility to reduce the risk of phishing, as also already emerged directly from users in the INDIMO pilots, which asked for specific training sessions about the use of digital mobility services.

8.1.10. Design for inclusivity means design for security

Design for inclusivity means also that the designed service will be more secure for all the user groups, also the most vulnerable ones. Implementing inclusive design features to make authentic sources easy to distinguish from malicious ones, means that also vulnerable groups such as reduced vision users, would be able to act and recognise threats. The INDIMO Toolbox, with the Universal Design Manual, the Universal Interface Language Icons and the Policy Evaluation tool, together with these recommendations

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

and guidelines are a perfect starting point to design a secure and inclusive digital mobility service.

9. Lessons Learnt

This section includes key lessons learnt in the process, from the collection of data, research bottlenecks, and challenges encountered during the work.

Key-lessons

- In general, in each pilot, we found a high sensitivity toward security and data protection.
- Pilots should learn more from each other, the more mature context could be of inspiration for the others.
- In some case language has been a barrier for the data collection, involvement of local partners has been important to collect data, and documentation.
- Human-factors are relevant part in tackling security and data protection issues, preparing the organisation for that is an important aspect. Sometimes there is the tendency to look on the technological side (e.g. new software for monitoring, anti-intrusion detection, etc.) while not focusing on organisational and human aspects.
- In some cases, confidentiality has been an issue for the data collection. Following the whole work of the pilots helped in understanding the possible concern, and to establish a good relationship with pilots partners.

Suggestions for future research

- Discuss possible confidentiality issues in an earlier stage would help in also adapting the methodology in a better way.
- Promote moment of peer sharing experience between the pilots to engage them in sharing their best practices.

10. Conclusions

In this deliverable, we presented the activity of T2.4 Cybersecurity and privacy assessment guidelines. Furthermore, during the project the theme of cybersecurity and privacy has been addressed in other tasks, and analysed in other deliverables, that is why a summary of those results are presented also in this document, and to make clear that they informed the compilation of the recommendations and guidelines. The work done for creating D1.2, D1.3, and D1.4 (2021) had also a major impact on the work done in T2.4.

The cybersecurity scenario is continuously evolving to adapt to the new threats posed by the development of new advanced technologies. The review of literature concerning four main identified topics such as IoT, phishing, mobile applications and human factor just showed how security pose a big issue for every digital mobility service from very

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

different perspectives (e.g. the threats from IoT security, or threats from phishing, from mobile application security, and the internal human factors threats).

Ethics concerning privacy and data security has been discussed presenting the main principles and strategies for an effective privacy by design implementation, which also has been highlighted in the pilots' description and recommendations.

A risk assessment has been performed in each of the 5 pilots of INDIMO project, following the methodology presented in Section 4. The risk assessment provided the data to define specific recommendations for each pilot to be considered for discussion in the next pilot phases when there will be a redesign (Task 3.4) and implementation (Task 3.5) of the services. A second assessment will be carried out after phase 3, within the work of T4.5 and the results will be presented in D4.3 Synthesized evaluation report for pilots. It is important to highlight the role and the effort of the pilots in all of the work done, they participated in the risk assessment, and also validated the recommendations written in this deliverable, making them a solid base for the next steps of the project.

Together with the pilots' perspective, the baseline questionnaires have been analysed for presenting the results of the specific questions related to cybersecurity and personal data protection, which highlighted the importance of a clear presentation of data collection and usage to the users, showing possible ethical concerns. Privacy is another major issue; users do not feel always protected because of issues such as spamming. In the pilots, the trustworthiness is in general high, from what emerges from the questionnaires, even though the number of respondents in some of the pilots prevent to make significant conclusions.

The guidelines and recommendations presented in the deliverable as part of the INDIMO Toolbox will inform the re-design phase of the INDIMO pilots, but also can be used in connection with the Toolbox to re-design and evaluate inclusivity and security in digital mobility services. The recommendations will be built into the INDIMO Policy Evaluation Tool (Task 2.5).

Focusing on inclusion, means also focusing on security, and at the same time focusing on security means focusing on inclusion, they are deeply connected, and they must be considered together.

11. References

Alwanain, M. I. (2020). Phishing Awareness and Elderly Users in Social Media. IJCSNS International Journal of Computer Science and Network Security, 20(9).

Ammar, M., Daniels, W., Crispo, B., and Hughes, D. (2018). SPEED: Secure Provable Erasure for Class-1 IoT Devices. In Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy (CODASPY '18). Association for Computing Machinery, New York, NY, USA, 111–118. DOI:https://doi.org/10.1145/3176258.3176337

Auditboard, (2021), NIST vs. ISO: What's the Difference? https://www.auditboard.com/blog/nist-vs-iso-whats-the-difference/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

Besnard, D., & Arief, B. (2004). Computer security impaired by legitimate users. Computers & Security, 23(3), 253–264. https://doi.org/10.1016/j.cose.2003.09.002

Cavoukian, A. (2011). Privacy by design. The 7 Foundational Principles. 2.

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., & Robinson, W. (2008). Performance Measurement Guide for Information Security. US department of Commerce.

Christen, M., Gordijn, B., & Loi, M. (A c. Di). (2020). The Ethics of Cybersecurity (Vol. 21). Springer International Publishing. https://doi.org/10.1007/978-3-030-29053-5

Correa, T., Pavez, I., & Contreras, J. (2020). Digital inclusion through mobile phones?: A comparison between mobile-only and computer users in internet access, skills and use. Information, Communication & Society, 23(7), 1074–1091. https://doi.org/10.1080/1369118X.2018.1555270

Di Ciommo F., G. Rondinella, T. Ruiz, R. Arroyo 2020: Travel Behavior of Care Trips: Data Analysis, Modeling and Transport Policy Insights, TRB 2020.

ENISA (2020). Main incidents in the EU and worldwide. ENISA Threat Landscape.

Guberek, T., McDonald, A., Simioni, S., Mhaidli, A. H., Toyama, K., & Schaub, F. (2018). Keeping a Low Profile? Technology, Risk and Privacy among Undocumented Immigrants. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (pagg. 1–15). Association for Computing Machinery. https://doi.org/10.1145/3173574.3173688

Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyberphysical system deployments in smart cities. Sustainable Cities and Society, 50, 101660. https://doi.org/10.1016/j.scs.2019.101660

Hoepman, J.-H. (2014). Privacy Design Strategies. In N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, & T. Sans (A c. Di), ICT Systems Security and Privacy Protection (Vol. 428, pagg. 446–459). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-55415-5_38

INDIMO project. (2021). D1.2. Users needs and requirements on a digital transport system.

INDIMO project. (2021). D1.3. User capabilities and requirement of a digital transport system on users.

INDIMO project. (2021). D1.4. Barriers to the design, planning, deployment and operation of accessible and inclusive digital personalised mobility and logistics services recommendations.

INDIMO project. (2021). D2.1. Universal Design Manual (UDM) - Version 1.

INDIMO project. (2021). D2.3 Universal Interface Language (UIL) for digital transport services

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

INDIMO project. (2021). D2.5. Enhancing appropriation of digital mobility soultions.

INDIMO project. (2021). D2.6. Guidelines for cybersecurity and personal data protection.

INDIMO project. (2021). D2.7. Policy evaluation tool and recommendations for policy makers

INDIMO project. (2021). D3.1. INDIMO Pilots handbook.

INDIMO project. (2020). D4.1 INDIMO evaluation framework.

INDIMO project. (2021). D4.2 Baseline data reports for pilots.

Jakobsson, M. (2007). The Human Factor in Phishing. In Privacy & Security of Consumer Information '07,.

Jang-Jaccard, J., Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5).

Martiniello, N., Eisenbarth, W., Lehane, C., Johnson, A., & Wittich, W. (2019). Exploring the use of smartphones and tablets among people with visual impairments: Are mainstream devices replacing the use of traditional visual aids? Assistive Technology: The Official Journal of RESNA, 1–12. https://doi.org/10.1080/10400435.2019.1682084

Macnish, K., & van der Ham, J. (2020). Ethics in cybersecurity research and practice. Technology in Society, 63, 101382. https://doi.org/10.1016/j.techsoc.2020.101382

Nai Fovino I., Barry G., Chaudron S., Coisel I., Dewar M., Junklewitz H., Kambourakis G., Kounelis I., Mortara B., Nordvik J.p., Sanchez I. (Eds.), Baldini G., Barrero J., Coisel I., Draper G., Duch-Brown N., Eulaerts O., Geneiatakis D., Joanny G., Kerckhof S., Lewis A., Martin T., Nativi S., Neisse R., Papameletiou D., Ramos J., Reina V., Ruzzante G., Sportiello L., Steri G., Tirendi S., Cybersecurity, our digital anchor, EUR 30276 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-19957-1, doi:10.2760/352218, JRC121051.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers & Security, 66, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

Pakianathan, P. V. S., & Perrault, S. (2020). Towards Inclusive Design for Privacy and Security Perspectives from an Aging Society. arXiv:2007.13117 [cs]. http://arxiv.org/abs/2007.13117

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2021). Leveraging human factors in cybersecurity: An integrated methodological approach. Cognition, Technology & Work. https://doi.org/10.1007/s10111-021-00683-y

Sapolsky, R. M. (2017). Behave: The biology of humans at our best and worse. Penguin Books.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

Sonowal, G., Kuppusamy, K. S., & Kumar, A. (2017). Usability evaluation of active anti-phishing browser extensions for persons with visual impairments. 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), 1–6. https://doi.org/10.1109/ICACCS.2017.8014654

The Prime Minister's Office – Israel National Cyber Directorate (2021), Organizational Preparedness for a Cyber Crisis Characterization & Requirements from Crisis Management Team and IR Team.

Turner, A. (2021). *How many smartphones are in the world?* Retrieved from Bankmycell: https://www.bankmycell.com/blog/how-many-phones-are-in-the-world

Weijters, B., & Baumgartner, H. (2012). Misresponse to Reversed and Negated Items in Surveys: A Review. Journal of Marketing Research, 49(5), 737–747. https://doi.org/10.1509/jmr.11.0368

Zhang, H., & Li, M. (2011). Security vulnerabilities of an remote password authentication scheme with smart card. 2011 International Conference on Consumer Electronics, Communications and Networks (CECNet), 698–701. https://doi.org/10.1109/CECNET.2011.5768515

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

Annex 1 – Risk assessment questionnaire

Interview questions (target: pilot, possibly expertise / position in cyber security, risk management)

1. Do you have any managerial improvement cycle applied for cybersecurity / risk management? If so, can you illustrate the activities in the following phases, *PLAN-DO-CHECK-ACT* (see figure below)? If a formal process cycle does not exist, what is the rationale? What tacitly defined informal steps are usually taken to respond to cyber security challenges?

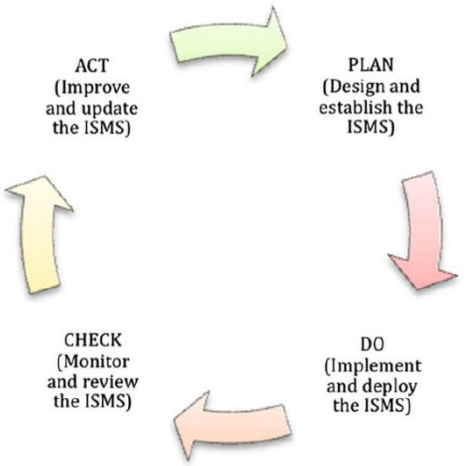


Figure 12. Information Security Management Systems (ISMS), Plan-Do-Check-Act (ISO/IEC 27001)

2. Describe the 3rd parties' actors enabling the pilot's services, and (if possible) what sensitive data is exchanged?
3. Rate the following risks for your pilot:
   (PROB, probability of occurrence; IMPACT, possible monetary impacts. Likert Scale: 1, Very low; 2, Low; 3. Neither High nor Low; 4. High; 5. Very high)

RISK	PROB 1 – Very Low to 5 Very High	IMPACT 1 – Very Low to 5 Very High
Risks related to human failures / mistakes of resources employed, e.g. -In-house staff deviating from the process (mistakes, including falling for social engineering attack) -Staff at supplier side making mistakes/falling for social engineering attack. -Failure of processes (e.g., background screening)		
Corruption / malware mobile devices at work/home		
Malware / virus in media devices, e.g. physical media transfer devices used by employees		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

Unauthorized access to network and network services.		
Risk for physical access, damage and interference to the organization's information and information processing facilities.		
Sabotage of equipment/devices used for the storing / exchange of information.		
Backup system failure.		
Lack of redundant systems causing a major disruption or data breach[10]		
Unauthorised use of credentials allowing access to information systems.		
Risk for eavesdropping[11], intrusion via wireless networks and information theft.		
Lack of security requirements in purchasing/procuring of new information systems or updates of existing ones.		
Unauthorized access to information shared with suppliers.		
Lack of response practices in case of cyber security / breach into the system.		
Unauthorized physical access to premises (to steal or destroy devices or data)		

4. Are there any additional cyberthreats (including data loss / privacy issues) that you would like to add? Are there any specific threats targeting users with specific needs and limited access to the services implemented in your pilot? (Estimate threats probability and impact as in the previous question and write your answer in the table)

Any additional Cyberthreat	**Please describe the Threat**	**Probability (1 – Very Low to 5 - Very High)**	**Impact (1 – Very Low to 5 - Very High)**
Specific threats for specific user needs	**Please describe the Threat**	**Probability (1 – Very Low to 5 - Very High)**	**Impact (1 – Very Low to 5 - Very High)**

[10] Data breach: confidential, sensitive, or protected information becomes exposed to an unauthorized person (Kaspersky, 2020).

[11] Eavesdropping: theft of data / information while transmitted in network communications (Teng et al., 2012).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.

5. What protective measures are being adopted by your organization to prevent and counteract cyberthreats / unauthorized access to your systems / data loss?
    a. Are there any additional security measures that should be implemented to protect more vulnerable segment of users, i.e., specific needs and limited access.
6. Can you elaborate how the following KPIs can be affected in case of a successful cybersecurity attack against your pilot?
    a. COSTS.
    b. BRAND IMAGE.
    c. SALES / PROFITS.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875533.