Definition hot topics of internet safety, country difference

Summary Report of all partial reports

BE SAFE ON THE INTERNET

Co-funded by the Erasmus+ Programme of the European Union

INTRODUCTION

This summary report contains the definition of hot Internet security issues, country differences and most relevant aspects of the five previous reports:

- The current situation of the personal data protection literacy on european level.
- The current situation of the personal data protection literacy on national level.
- Impact of the INDUSTRY 4.0 on the internet and personal data protection.
- Implementation of the web security and personal data protection in educational systems.
- Questionnaires about web security and personal data protection.

In the first place it is put in context on data protection and web security, its regulation, status, etc. Next, this same information is provided for the countries of the partners (Portugal, Czech Republic, Spain and Austria).

The technological developments which are at the base of Industry 4.0 do raise at the same time a vast number of associated of security concerns. The changes that Industry 4.0 bring are having an important impact on web security and data protection on the internet.

The next point discussed is its current implementation in educational systems, with its differentiation by country.

Finally, this summary includes the main conclusions drawn from the questionnaire, carried out as part of the project in different countries and for different user segments.

Sumary

1. THE CURRENT SITUATION OF THE PERSONAL DATA PROTECTION LITERACY ON EUROPEAN LEVEL

1.1. DATA PROTECTION

Regulation and Data Protection

The legal reference is "**Regulation (EU) 2018/1725**" of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data", repealing Regulation (EC) 45/2001 and Decision No 1247/2002/EC.

Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

The General Data Protection Regulation (GDPR) applies to the processing of personal data wholly or partly by automated means as well as to non-automated processing, if it is part of a structured filing system.

Data Protection Authorities (DPAs) are independent public authorities that supervise, through investigative and corrective powers, the application of the data protection law.

Rights for Citizens

You have the right to:

- Information about the processing of your personal data.
- Obtain access to the personal data held about you; ask for incorrect, inaccurate or incomplete personal data to be corrected.
- Request that personal data be erased when it’s no longer needed or if processing it is unlawful.
- Object to the processing of your personal data for marketing purposes or on grounds relating to your particular situation.
- Request the restriction of the processing of your personal data in specific cases.
- Receive your personal data in a machine-readable format and send it to another controller (‘data portability’).

- Request that decisions based on automated processing concerning you or significantly affecting you and based on your personal data are made by natural persons, not only by computers.

The following are the basic concepts that should be known about citizens' rights:

You have a **right to ask for** and obtain from the company/organisation confirmation as to whether or not it holds any personal data which concerns you.

If you believe that your personal data might be **incorrect, incomplete or inaccurate** you can ask the company or organisation to correct your data.

If a company is processing your personal data on the basis of your consent or a contract, you can **ask the company to transfer** your personal data to you.

If you object to **direct marketing**, the company must stop using your personal data and comply with your request without asking for a fee.

This right also applies online and is often referred to as the '**right to be forgotten**'. In specific circumstances, you may ask companies that have made your personal data available online to delete it.

Any information addressed **specifically to a child** should be adapted to be easily accessible, using clear and plain language. The age threshold for obtaining parental consent is established by each EU Member State and can be between 13 and 16 years.

A **consent request** needs to be presented in a clear and concise way, using language that is easy to understand, and be clearly distinguishable from other pieces of information such as terms and conditions.

If you think your **data protection rights have been breached**, you have three options:

- Lodge a complaint with your national Data Protection Authority (DPA).
- Take legal action against the company or organisation.
- Take legal action against the DPA.

You can claim compensation if a company or organisation hasn't respected the data protection law and you've suffered material damages (for example financial loss) or non-material damages (for example distress or loss of reputation).

Rules for Business and Organisations

The following are the basic concepts that should be known about the rules for business and organisations:

If your company is a small and medium-sized enterprise ('SME') that processes personal data as described above you have to comply with the GDPR. However, if processing personal data isn't a core part of your business and your activity doesn't create risks for individuals, then some obligations of the GDPR will not apply to you (for example the appointment of a Data Protection Officer ('DPO')).

The rules only **apply to personal data about individuals**, they don't govern data about companies or any other legal entities.

The **type and amount** of personal data you may process depends on the reason you're processing it (legal reason used) and what you want to do with it. The purpose for processing of personal data must be known and the individuals whose data you're processing must be informed. This is known as the 'purpose limitation' principle.

If your company/organisation has collected data on the basis of legitimate interest, a contract or vital interests it can be used for **another purpose** but only after checking that the new purpose is compatible with the original purpose.

It's your company/organisation's responsibility as controller to assess how much data is needed and ensure that irrelevant data isn't collected.

You must store data for the shortest time possible. Your company/organisation should establish time limits to erase or review the data stored.

The following personal data is considered 'sensitive' and is subject to specific processing conditions:

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;
- trade-union membership;
- genetic data, biometric data processed solely to identify a human being;
- health-related data;
- data concerning a person's sex life or sexual orientation.

Your company / organization can only process **confidential data** if certain conditions exist.

Your company/organisation can only process a **child's personal data** on grounds of consent with the explicit consent of their parent or guardian up to a certain age.

Your company/organisation must also ensure that the list or database is **up-to-date** and that you **don't send advertising** to individuals who objected to the processing of their personal data for direct marketing purposes.

The **data controller** determines the purposes for which and the means by which personal data is processed. The **data processor** processes personal data only on behalf of the controller.

Someone else (a natural or legal person or any other body) may process personal data on your behalf provided there is a **contract or other legal act**.

The **General Data Protection Regulation (GDPR)** is based on the risk-based approach. In other words, companies/organisations processing personal data are encouraged to implement protective measures corresponding to the level of risk of their data processing activities.

Companies/organisations are encouraged to implement **technical and organisational measures**, at the earliest stages of the design of the processing operations, in such a way that safeguards privacy and data protection principles right from the start ('data protection by design').

1.2. WEB SAFETY INITIATIVES

The 'Strategy for a Better Internet for Children' proposes a series of actions to be undertaken by the Commission, Member States and by the whole industry value chain.

Some strategic activities:

- Guide to online services
- Safer Internet Day
- #SaferInternet4EU campaign
- Online Safety MOOC
- Safer internet centers network
- Safer Internet Forum
- Alliance to better protect minors online

The **European Union Agency for Network and Information Security (ENISA)** is a centre of expertise for cyber security in Europe. ENISA is actively contributing to a high level of network and information security (NIS) within the Union, since it was set up in 2004, to the development of a culture of NIS in society and in order to raise awareness of NIS, thus contributing to proper functioning of the internal market.

1.3. FAKE NEWS

Disinformation -or fake news- consists of verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm.

73% of internet users in the EU are concerned about disinformation in pre election periods. Given its cross-border dimension, the adverse effects of disinformation in the European Union require a coordinated and long-term approach to respond to the challenge at both EU and national level.

The **Action Plan** proposes a set of actions that should further enable a joint and coordinated EU approach to addressing disinformation. The EU institutions have already built an **internal network against disinformation** and are in parallel working on strengthening their strategic communication capacities.

The **strategic communication budget** of the European External Action Service (EEAS) to address disinformation and raise awareness of its adverse impact is expected to be more than double, from € 1.9 million in 2018 to € 5 million in 2019. The Commission also proposed a dedicated budget of €61 million under the next Creative Europe programme to support journalism, media freedom, media pluralism and media literacy.

The Action Plan sets out **key actions** to tackle disinformation in a coordinated approach among the EU institutions and in cooperation with the Member States. When democracy in one Member State is under attack, European democracy as a whole is under attack.

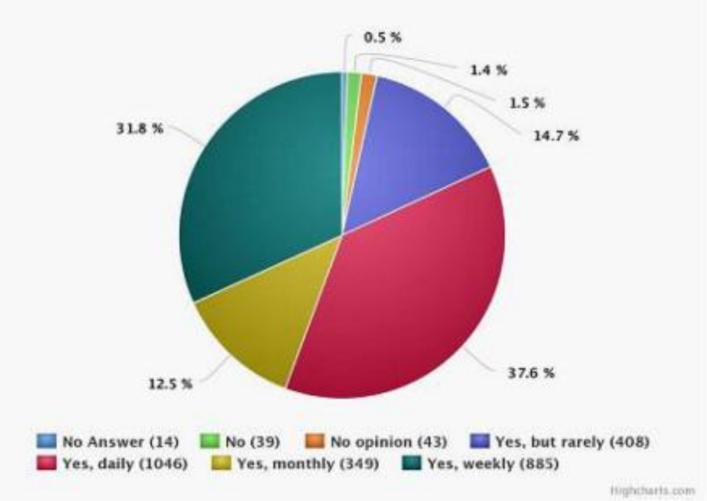
Cooperation on threat analysis and situational awareness with NATO is ongoing. G7 partners are in the process of establishing a Rapid Response Mechanism to reinforce the defences of democracies.

As part of the Media Literacy Week in March 2019, in cooperation with the Member States, the Commission will support cross-border cooperation amongst **media literacy** practitioners as well as the launch of practical tools for the promotion of media literacy to the public.

Fact-checkers are essential in tackling disinformation. They verify and assess the veracity of content based on facts and evidence thus helping the information ecosystem to be cleaner and more robust.

The online platforms which have signed the **Code of Practice** have provided individual roadmaps detailing the key tools and policies they will apply in all EU Member States ahead of the elections. Subscription to the Code is **voluntary**. However, there are growing expectations that online platforms should not only comply with legal obligations under EU and national laws, but also act with appropriate responsibility to protect users from disinformation.

1. Have you ever come across fake news?

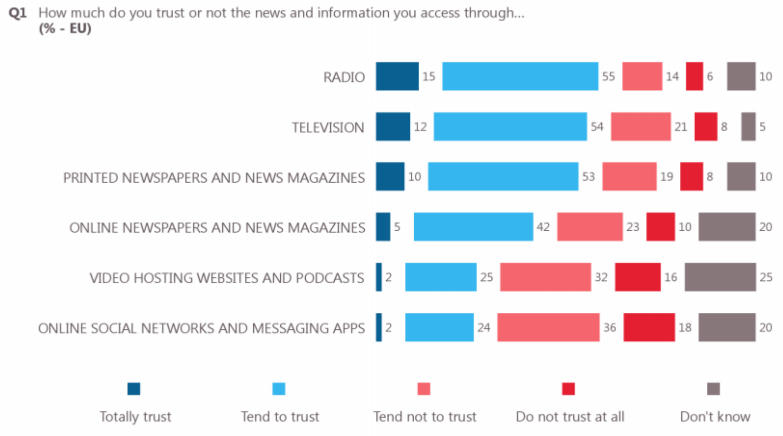


Source: European Commision (2018)

The **Eurobarometer survey** was conducted via telephone interviews early February in all EU Member States. Over 26.000 citizens were interviewed about their perception of fake news and their trust in news media sources.

The results show that fake news are widely spread across the EU with 83% of respondents saying that fake news represent a danger to democracy.

2. How much do you trust or not the news and information you access throught…?



Base: All Respondents (N=26,576)

Source: Flash Eurobarometer (2018)

- Respondents perceive traditional media as the most trusted source of news: radio (70%), television (66%) and printed newspapers and news magazines (63%);
- 37% of the respondents come across fake news every day or almost everyday and 71% feel confident on identifying them;
- 85% of respondents perceive fake news as a problem in their country and 83% perceive it as a problem for democracy in general;
- In respondents’ view, journalists (45%), national authorities (39%) and the press and broadcasting management (36%) should be the main responsible for stopping the spread of fake news.

2. THE CURRENT SITUATION OF THE PERSONAL DATA PROTECTION LITERACY ON NATIONAL LEVEL

2.1. AUSTRIA

As an implementing instance in connection with web security and data protection, there is the data protection authority in Austria, which both provides information and with which one can submit complaints and offences against the guidelines and GDPR.

The digitalization study 2018 has captured digital development in SMEs and identified the key issues:

- Relevance of digitization in SMEs has increased
- Strong visibility of data protection for SMEs in 2018
- Increase awareness of the challenges posed by digital transformation

Digital business solutions have become an indispensable part of everyday professional life, and in some industries the importance of digitization has grown enormously. However, measures such as the DSGVO have made knowledge gaps visible and the digital transformation of other business areas poses new challenges for SMEs.

New indices have identified industry dynamics, proactivity and financial resources as key drivers to meet these challenges.

The results of the 2018 Digitization Study show that SMEs actually need support and there are some initiatives and places that provide information. As in every other European country there is of course still further need for action in consideration to data protection and security in the Internet - nevertheless Austria is already on a good way.

2.2. CZECH REPUBLIC

The Cyber Security Strategy for the Czech Republic covers the years 2015 to 2020. The Cyber Security Council (CSC) came into being through the Decision of the Government of the Czech Republic n. 781 (19 October 2011). The CSC advises the Prime Minister on cybernetic security.

The Action Plan 2015-2020 sets out two actions on risk assessment with the aim of developing a methodology at the state level. The two actions are:

1. Choose a risk and a threat assessment methodology for the cyber security field at the state level.
2. Assess, on a continuous basis, cyber security risks and threats at the state level.

In the Czech Republic the issue of web security and its legislation is considered very important and the various public and private institutions carried out many activities, projects and surveys on that subject.

Most EU countries claim that relevant data for the topic of Internet safe are collected at national level (exceptions are Bulgaria, Ireland, Romania, Slovenia and Slovakia). Among these EU countries, 11 declare that data collection has an impact on policy design. Most of these EU countries have a policy design indicator score that is higher than the average (Czech Republic, Estonia, Finland, Latvia, Norway, Portugal, Sweden, and UK). However, only six EU countries are collecting data annually: Austria, Czech Republic, Italy, Portugal, Sweden and UK.

Public sector is a key driver for non-public stakeholder involvement of web security and internet safety.

2.3. PORTUGAL

In Portugal, several studies and news confirm that the legislation system is being adapted very slowly regarding the needs of web security and personal data protection. This fact confirms the need to implement more measures to inform the society and also the companies.

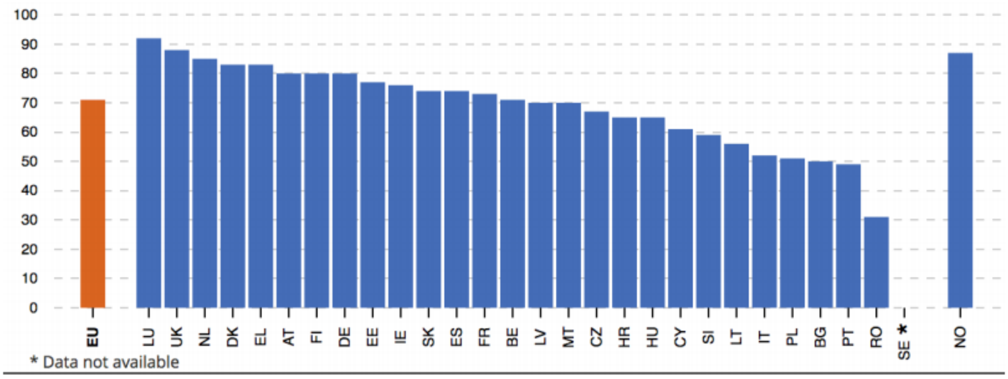
Portuguese companies are doing more efforts to assure a correct application of the GPDR there are still some doubts, questions and disagreements. The sectors that are more prepared are: financial and insurance sector, human health and social support activities and retail and wholesale trade.

According with Eurostat, in 2016, 36% of Portuguese have already experienced some trouble in the internet and about 26% decided to stop using online bank transferences. The most common problems are: virus ("worm" and "trojan"); the abusive utilization of personal information; financial losses; and children access to inappropriate digital content. The study carried out by Eurostat also confirms that Portugal is the third country in the UE where 30% of internet users gave up or didn't shop online because of online security issues.

Another study carried out by "msn content portal" in 2012, indicates that 78% of Portuguese internet users surveyed have some basic online protection but they are poorly informed about what they should do to protect themselves against cybercrime threats based on fraud, such as phishing, identity theft and fraudulent links. According with this investigation, 23% of respondents don’t search information about identity theft or have some knowledge to protect their online reputation and 53% refer that they use passwords with uppercase and lowercase letters, symbols and numbers.

Portugal is one of the countries that shares less personal information over the internet. Younger generations seem to be more willing to provide personal information online (almost 80% of internet users aged 16 to 24 years had shared some kind of personal information online) compared with 57% of users aged 65 to 74 years.

3. People who provided any personal information online (2016) (as% of internet users aged 16-74 years)

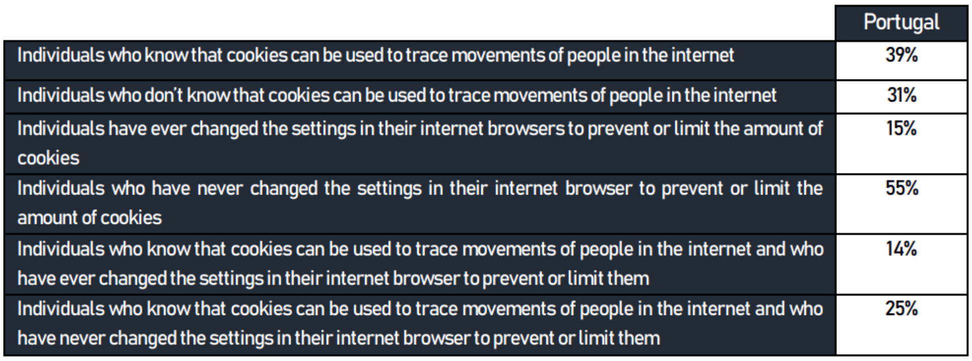


Source: Eurostat

Although Portugal is one of the countries that shares less personal information, in 2018, CNPD - Comissão de Proteção de Dados warned that the Portuguese people that provide personal information on the internet do it in a very “negligent and naive” way as do companies and public entities.

The knowledge of cookies in Portugal is also a problem. Although 39% of the people know that cookies can be used to trace movements of people in the internet almost the same amount of the people (31%) don’t know what cookies are. In addition, 55% of the individuals have never changed the settings in their internet browsers to prevent or limit the amount of cookies and 25% of the individuals have never changed the settings in their internet browser to prevent or limit them.

4. Cookies in Portugal (2016)



	Portugal
Individuals who know that cookies can be used to trace movements of people in the internet	39%
Individuals who don’t know that cookies can be used to trace movements of people in the internet	31%
Individuals have ever changed the settings in their internet browsers to prevent or limit the amount of cookies	15%
Individuals who have never changed the settings in their internet browser to prevent or limit the amount of cookies	55%
Individuals who know that cookies can be used to trace movements of people in the internet and who have ever changed the settings in their internet browser to prevent or limit them	14%
Individuals who know that cookies can be used to trace movements of people in the internet and who have never changed the settings in their internet browser to prevent or limit them	25%

Source: Eurostat

In Portugal, there is a lot to do when it comes to have a safer behaviour in the internet and several studies confirm the importance of having access to a more clear and simple information. In this context, there are some things that can and must be done in order to improve digital transformation

2.4. SPAIN

In Spain there is a Code for the Cybersecurity Law, published in the Official State Bulletin (BOE - Boletín Oficial del Estado), which states the main rules to be taken into account regarding the protection of cyberspace and to ensure the aforementioned cybersecurity.

The General Data Protection Regulation (GDPR) aims to establish a more solid, coherent framework for data protection in the European Union, and is applicable from 25 May 2018. The GDPR states that measures designed to ensure compliance must take into account the nature, scope, context, and purposes of the processing, as well as the risk to individuals' rights and freedoms.

Any legal subject, business owner, business, organization, etc., in the public or private sector, that, in the course of its business collects personal data for an economic, professional or business objective, must adapt to the current Organic Law on Data Protection (LOPD) in Spain. The LOPD establishes a set of principles, rights and duties that organizations must abide by. Its principal objective is to ensure that data provided by users are dealt with in the correct manner.

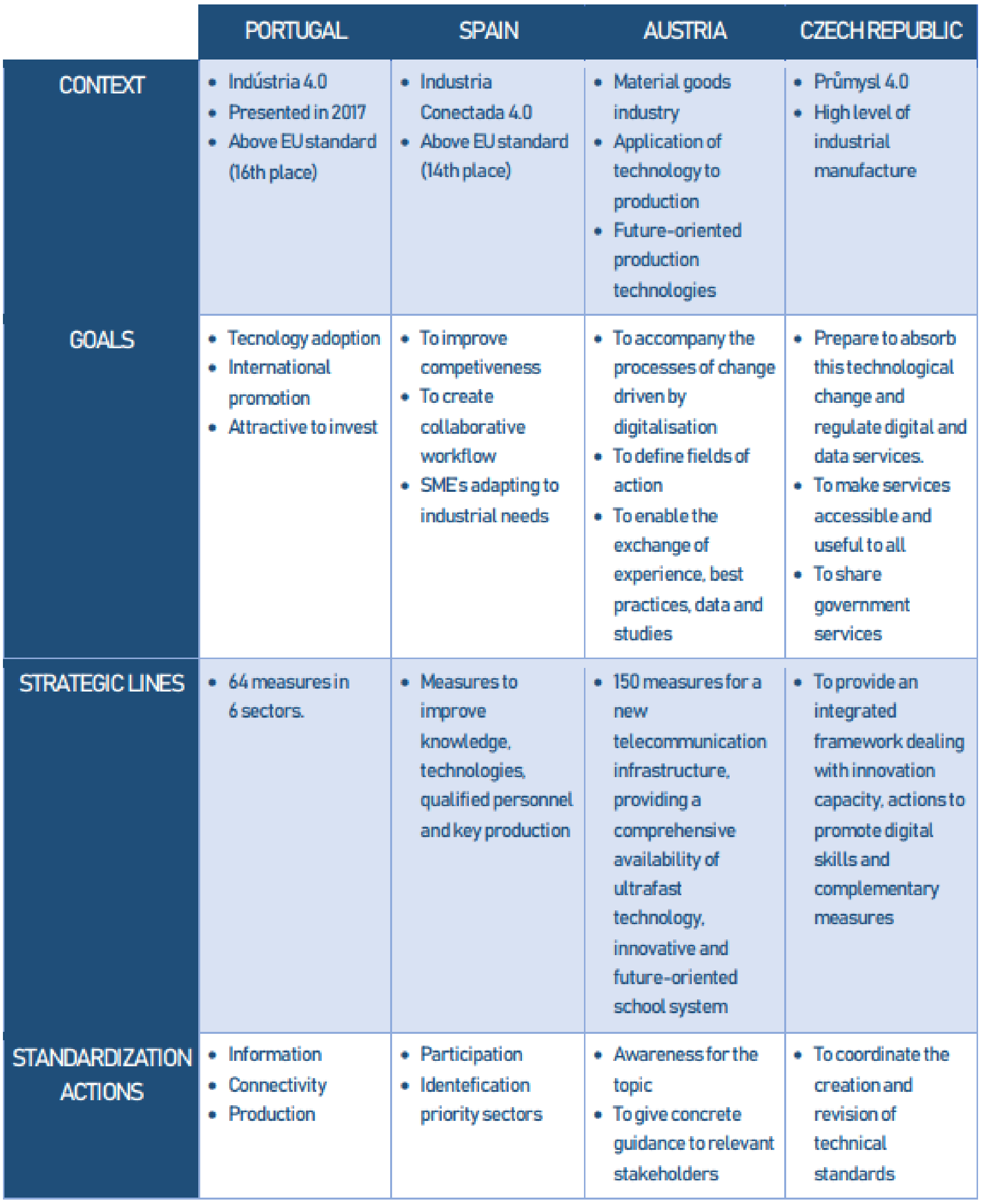
While many of the concepts and principles of the LOPD are similar to the current standard, the RGPD introduces new elements, which entail new obligations for EU companies and organizations.

In conclusion, the LOPDGDD has gone a step further and has not limited itself to specifying or restricting the provisions of the GDPR, but has incorporated a series of digital rights to citizens, which a priori covers the needs favored by the rapid evolution of new technologies, but on which it will be necessary to analyze whether their practical application reflects the reality and needs of the public in relation to these issues, and the impact they could have on the information society and Internet service providers, such as these are also the main affected by the introduction of these new rights.

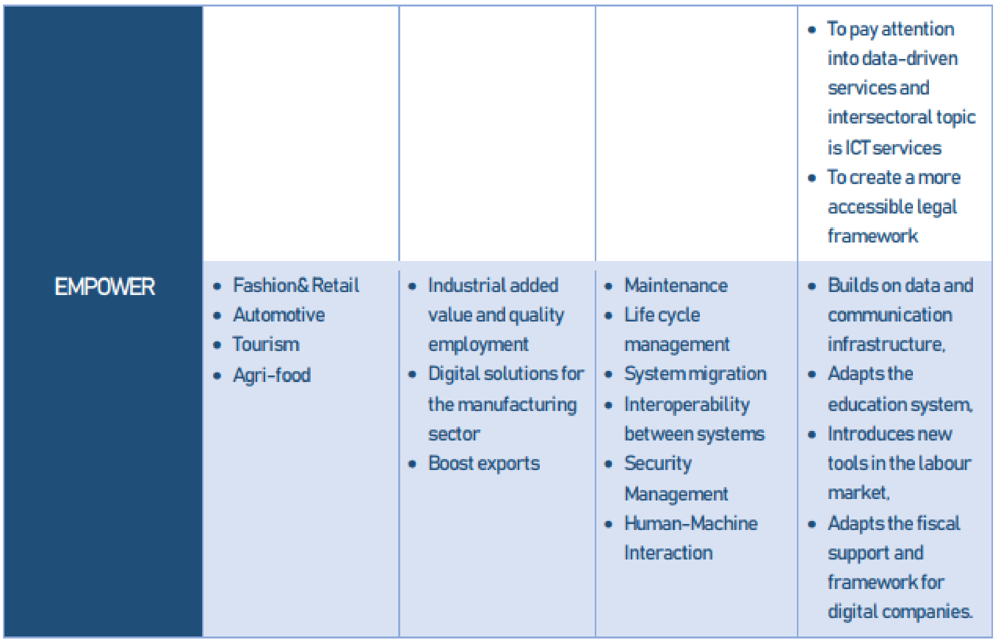
3. IMPACT OF THE INDUSTRY 4.0 ON THE INTERNET AND PERSONAL DATA PROTECTION

The Industry 4.0 market is poised to grow significantly in the coming years. The increasing adoption of the IoT in the digital transformation of manufacturing and related industries, the rise of industrial robotics and the proportionally higher spend in the Industrial Internet of Things are just some contributing factors.

Below is a comparative table of certain concepts analyzed with respect to Industry 4.0, such as the context, goals, strategic lines, standard actions and empowerment of the countries: Portugal, Spain, Austria and the Czech Republic.



	PORTUGAL	SPAIN	AUSTRIA	CZECH REPUBLIC
CONTEXT	• Indústria 4.0 • Presented in 2017 • Above EU standard (16th place)	• Industria Conectada 4.0 • Above EU standard (14th place)	• Material goods industry • Application of technology to production • Future-oriented production technologies	• Průmysl 4.0 • High level of industrial manufacture
GOALS	• Tecnology adoption • International promotion • Attractive to invest	• To improve competiveness • To create collaborative workflow • SME's adapting to industrial needs	• To accompany the processes of change driven by digitalisation • To define fields of action • To enable the exchange of experience, best practices, data and studies	• Prepare to absorb this technological change and regulate digital and data services. • To make services accessible and useful to all • To share government services
STRATEGIC LINES	• 64 measures in 6 sectors.	• Measures to improve knowledge, technologies, qualified personnel and key production	• 150 measures for a new telecommunication infrastructure, providing a comprehensive availability of ultrafast technology, innovative and future-oriented school system	• To provide an integrated framework dealing with innovation capacity, actions to promote digital skills and complementary measures
STANDARDIZATION ACTIONS	• Information • Connectivity • Production	• Participation • Identefication priority sectors	• Awareness for the topic • To give concrete guidance to relevant stakeholders	• To coordinate the creation and revision of technical standards



EMPOWER				To pay attention into data-driven services and intersectoral topic is ICT services To create a more accessible legal framework
	Fashion& Retail Automotive Tourism Agri-food	Industrial added value and quality employment Digital solutions for the manufacturing sector Boost exports	Maintenance Life cycle management System migration Interoperability between systems Security Management Human-Machine Interaction	Builds on data and communication infrastructure, Adapts the education system, Introduces new tools in the labour market, Adapts the fiscal support and framework for digital companies.

The Digital Single Market Strategy outlined the path for the EU to build the right digital environment: one in which a high level of privacy, protection of personal data and consumer rights are ensured, businesses can innovate and compete, and cybersecurity strengthens the fabric that weaves our societies together.

The strategy for a Digital Single Market is about transforming European society and ensuring that it can face the future with confidence.

The opening of the European market must be maintained and further developed in the digital sphere and must continue to press for our commercial partners to exercise the same openness and effective application of intellectual property rights.

The diffusion of open data is a promising development. While digitization is everywhere, adoption is uneven across companies, sectors, and economies.

This scenario predicts that the current positive economic climate and growth dynamics of the European Data Market will continue towards 2025, driven by a healthy growth of the European data industry, a continuing improvement of the offering of data products and services, and a corresponding gradual development of demand, especially by the most advanced, competitive and innovative enterprises, large and small.

Building a Digital Single Market is a key part of the EU's strategy to prepare itself for the future and to continue to deliver high living standards for its population, however the European Commission's initiatives aim to improve online security, trust and inclusion.

Where there is already sufficient evidence of barriers that need to be removed the Commission will table legislative proposals and take initiatives to put the scale of the single market at the service of the consumer and business. Where further consultation and evidence gathering is needed in order to identify the right course of action the Commission will engage stakeholders in discussing the options available.

4. IMPLEMENTATION OF THE WEB SECURITY AND PERSONAL DATA PROTECTION IN EDUCATIONAL SYSTEMS

4.1. AUSTRIA

There are currently many new developments in the Austrian education system with regard to data security and Internet security. With the introduction of digital basic education, the lower secondary schools are already laying the foundations for an understanding of this topic. Furthermore, the master plan for digitization in education raises hopes that this will be closely integrated into the system in the future. The Austrian Cyber Security Strategy, which will provide a national unit for the implementation of security on the Internet in the future, is fundamental to the whole.

Thus, many different ways have already been identified for dealing with the new challenge of "security on and within the Internet" for all age groups - it is now up to the individual actors to ensure that this also works.

4.2. CZECH REPUBLIC

During recent years the protection of image on the Internet has become the issue as significant as other, more recognized, e-threats such as: media addiction or cyberbullying. Conscious and efficient alleviation of e-threats in countries, in which social media have become popular in the last few years should include the following principles: diagnosis (also on the international level), actions based on current school curricula and actions of non-governmental organizations, exchange of experiences between institutions involved in media prevention (also on international level) as well as evaluation of the conducted activities.

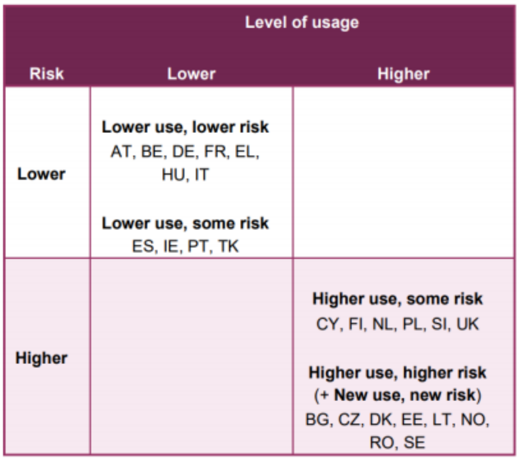
Teachers are prevented from the safest possible use of ICT by obstacles that originate from the type of person they are, the way they feel and the amount of time they have.

Although in EU countries are subtly graded in terms of amounts and types of use and risk, we here group them for ease into four categories or ‘ideal types’:

- Lower use, lower risk’ countries (Austria, Belgium, France, Germany, Greece, Italy, Hungary)
- Lower use, some risk’ countries (Ireland, Portugal, Spain, Turkey)
- Higher use, some risk’ countries (Cyprus, Finland, the Netherlands, Poland, Slovenia, the UK)
- Higher use, higher risk’ countries (Bulgaria, Czech Republic, Denmark, Estonia, Lithuania, Norway, Romania, Sweden)

Wealthier Nordic countries, the UK and the Netherlands have the highest usage across Europe, along with the countries with a lower GDP but more recent introduction of broadband, such as Bulgaria, Romania, Lithuania, Estonia and the Czech Republic.

Neither the expected years of schooling nor the percentage of schools that offer and use computers in classrooms has any significant effect on online usage or online risks. However, education has a positive and significant effect on children’s digital skills.



	Level of usage	
Risk	Lower	Higher
Lower	**Lower use, lower risk** AT, BE, DE, FR, EL, HU, IT **Lower use, some risk** ES, IE, PT, TK	
Higher		**Higher use, some risk** CY, FI, NL, PL, SI, UK **Higher use, higher risk** (+ **New use, new risk**) BG, CZ, DK, EE, LT, NO, RO, SE

4.3. PORTUGAL

There are in Portugal some initiatives regarding web security and data personal protection not all schools have access or implement those activities. Besides that, although some schools talk about these themes in some classes (such as Society and Citizenship and ICT) each school doesn’t have a plan to teach and talk about it.

The main challenge is to provide to all learners’ needs, aligning programmes with the acquisition of 21st century skills because the “one-size-fits-all” approach doesn’t work and teachers have an important task to play because they shape the future generations.

The main barriers in Portugal in the field of education and web security are:

- Schools don’t have a plan and resources to know how to teach and talk about web security and personal data protection;

- The education in Portugal needs more young teachers because, especially in public schools, 80% of the teachers have between 40-59 years;
- The number of computers available for each student is reducing and the acquisition of technological material is made by each school. In 2016/2017, the number of computers in schools dropped by 31% compared to 2014/2015;
- Digital technologies are constantly changing and teachers need to receive constant training that is not happening.
- The Portuguese early drop out of school is higher than in their European counterparts. There are fewer adults between the ages of 30 and 34 to complete higher education which means that they are more likely to have fewer digital competences;
- In Portugal there are a lot of students with economic needs and the use of computers can help students to become educated;
- Portuguese teachers have very little support, resources and training in web security and personal data protection.
- Without both good technical supports in the classroom and whole-school resources, teachers cannot be expected to overcome the barriers regarding the lack of knowledge related to web security and personal data protection.

Therefore, educators, teachers, the government and schools need to collaborate to overcome the barriers because the teaching of web security and personal data protection in classes varies from curriculum to curriculum, place to place and depends on several factors. Additionally, teachers need to be open minded towards new ways of teaching, prepare themselves by self-training and self-research.

4.3. SPAIN

According to the present Spanish Educational Law, ICT competence involves the creative, critical and secure use of information and communications technologies to achieve objectives related to work, employability, learning, use of free time, promote inclusion and participation in the society.

The hyperconnectivity of today’s world exacerbates some of the security system vulnerabilities and requires greater protection of networks and systems, as well as the public’s privacy and digital rights. Spain must adapt to this permanent transformation by stepping up its efforts to digitize and technify the State and society, based on an educational and training system adapted to this new reality. In this context, Spain must foster a culture of national security, supported primarily by a comprehensive educational system, which strengthens awareness of the prevailing threats and challenges, and their possible impact on the way of life and the prosperity of the Spanish people. Effective national security requires both social awareness among citizens and the participation of their representatives.

As schools are classified as a public authority for the purposes of data protection and GDPR, they must assign a Data Protection Officer who is solely responsible for any data protection and compliance with the GDPR regulation. It is important to consider where this role will sit in line with the school's structure and governance arrangements.

It is therefore crucial to sensitize the children about the practices that could be followed, providing:

- A digital education from a very early age in order to face the possible threats when using the Internet.
- Protecting measures in their devices to ensure children's privacy and protection.
- Files and documents must also be controlled and protected by using passwords or additional encryption systems
- Children's trust must be increased and this will increase their confidence regarding any security incident.
- Schools are spaces that we must ensure against the threats that arise through the use of the Internet.

A specific training about computer safety and security for them is already fundamental in a world that is moving towards digital.

5. QUESTIONNAIRES ABOUT WEB SECURITY AND PERSONAL DATA PROTECTION

The objective of the questionnaire is to find conclusions and applicable recommendations for future phases of the project based on the data and information collected.

This questionnaire aims to provide relevant information about the impact that security and privacy have in society by analyzing the following aspects:

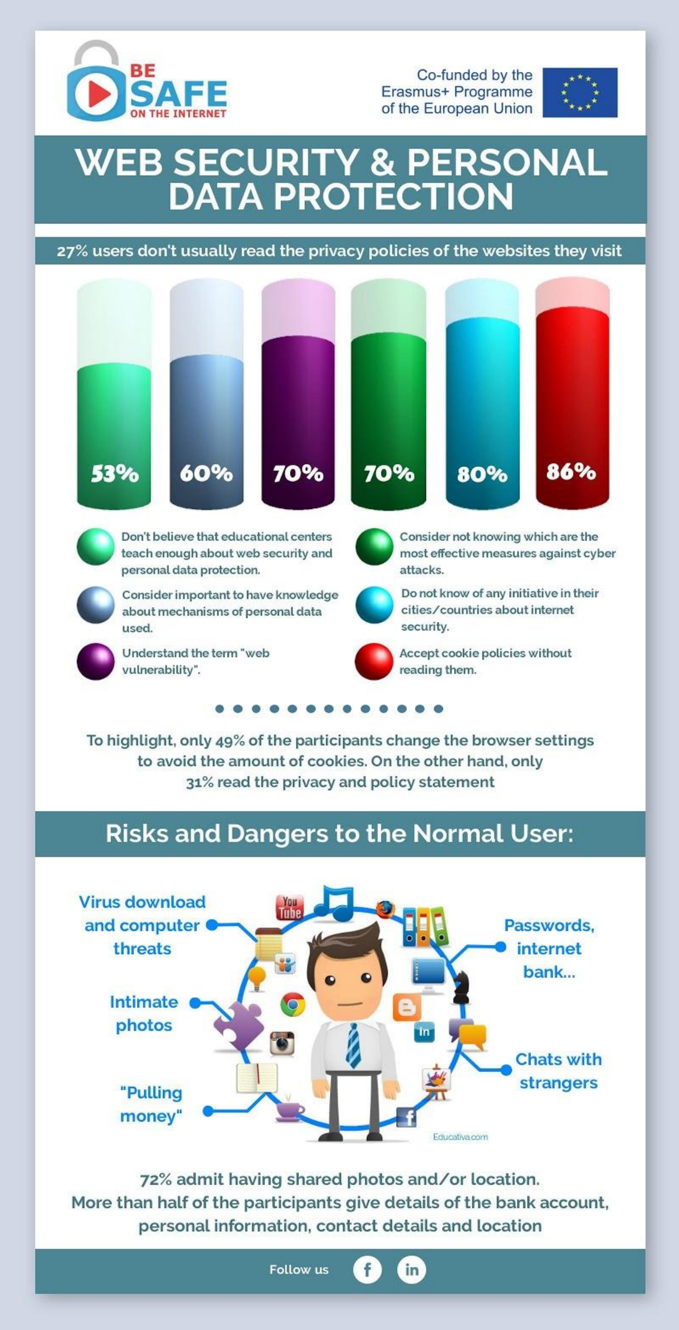
- The level of skills/experience of the target group.
- Learning methods and preferences of the target group to short it out with these issues.
- Interesting topics and contents of the target group.

To obtain a complete image of the whole society, three types of public have been considered: University/VET Students, University/VET teachers or trainers and General Public.

1. When planning the questionnaire, 5 main distinctions were made:
2. Introduction. Knowing age, professional sector, sex, nationality and IT use of the participants.

3. Level of skills/experience on web security and personal data protection.
4. How to learn about web security and personal data protection (learning methods).
5. Topics from web security interesting for the public in general.
6. Test Experience. The experience of the participants' use, their behavior in front of certain situations and main interests.

In general, respondents have not suffered many problems related to internet security and personal data protection, but there is always a percentage of them that have suffered various problems related to the subject. Most of the participants consider it important to have knowledge about web security and protection of personal data, even though many of them already take protective measures and have sufficient knowledge.



BE SAFE ON THE INTERNET

Co-funded by the Erasmus+ Programme of the European Union

WEB SECURITY & PERSONAL DATA PROTECTION

27% users don't usually read the privacy policies of the websites they visit

- Don't believe that educational centers teach enough about web security and personal data protection.
- Consider important to have knowledge about mechanisms of personal data used.
- Understand the term "web vulnerability".
- Consider not knowing which are the most effective measures against cyber attacks.
- Do not know of any initiative in their cities/countries about internet security.
- Accept cookie policies without reading them.

To highlight, only 49% of the participants change the browser settings to avoid the amount of cookies. On the other hand, only 31% read the privacy and policy statement

Risks and Dangers to the Normal User:

72% admit having shared photos and/or location.
More than half of the participants give details of the bank account, personal information, contact details and location

Follow us

On several occasions, users say they do not usually read the privacy policies of the websites they visit. The majority of the participants in the survey consider not knowing which are the most effective measures against cyber-attacks. Many, in fact, do not know exactly what consequences it may have.

Most respondents do not know of any initiative in their cities / countries on Internet security, and if they receive information, they would prefer it to be for news, tutorials and online / e-learning platforms.

It would be good to provide more information about cyberbullying, sexting, inappropriate content or excessive use of ICT. These concepts are known, but knowledge about them is not very high. On the other hand, the concept of grooming and cyberstalking are quite unknown.

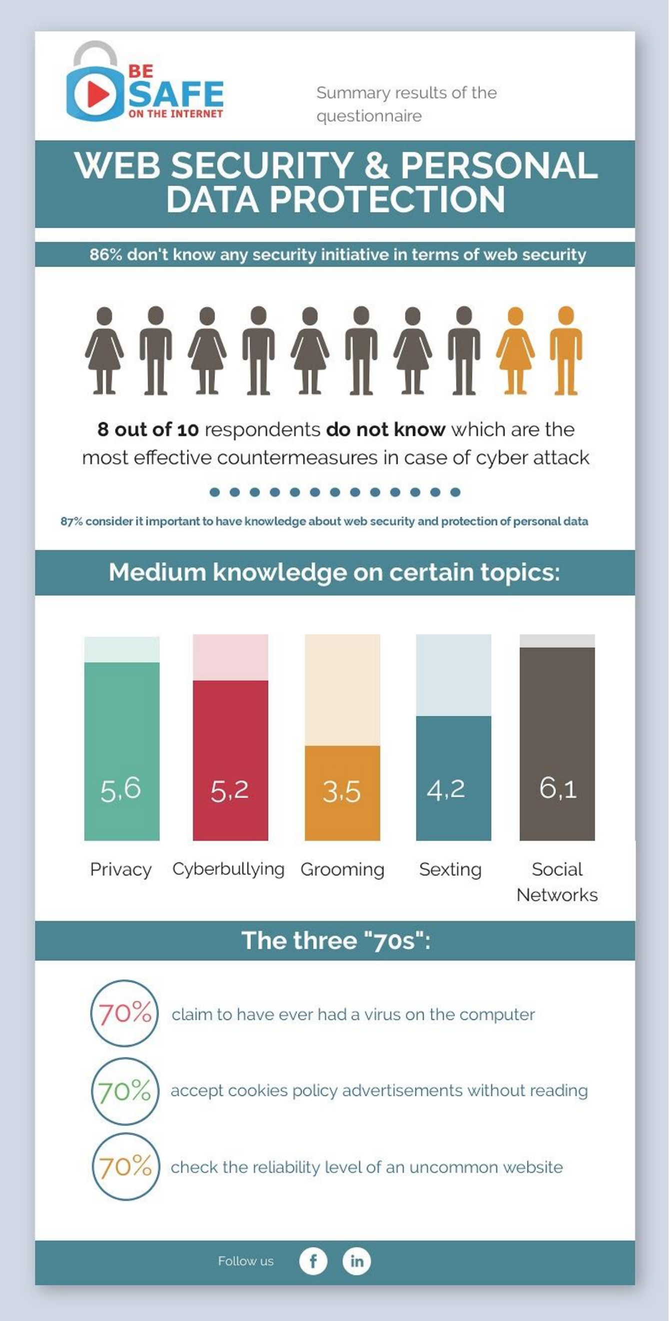
Most of the participants take some measures for the protection of personal data. Many create passwords that are difficult to decipher, block cookies, etc.

The options of more risk and danger for a normal user are as follows:

- Inappropriate and easily passwords,
- Chat with strangers,
- Possibly of virus downloads and computer threats
- “Pulling money” free of charge and publish intimate photos.

In general, participants have ever had a virus. The majority of them use some method to check the reliability and security of the website, but in general they don’t read the cookie policies.

The three most interesting topics for the participants are: Personal data management, Computer protection and Smartphone protection.



BE SAFE ON THE INTERNET

Summary results of the questionnaire

WEB SECURITY & PERSONAL DATA PROTECTION

86% don't know any security initiative in terms of web security

8 out of 10 respondents **do not know** which are the most effective countermeasures in case of cyber attack

87% consider it important to have knowledge about web security and protection of personal data

Medium knowledge on certain topics:

The three "70s":

70% claim to have ever had a virus on the computer

70% accept cookies policy advertisements without reading

70% check the reliability level of an uncommon website

Follow us