The current situation of the personal data protection literacy on national level

BE SAFE ON THE INTERNET

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

Sumary

Figures and tables

1. HOW HAS EUROPEAN LEGISLATION ON WEB SECURITY AND PERSONAL DATA PROTECTION BEEN ADAPTED IN YOUR COUNTRY?

1.1. AUSTRIA

On 4 May 2016 the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) was announced.

Since 25 May 2018, the **European General Data Protection Regulation (GDPR)** - in German DSVGO (Datenschutz-Grundverordung) - has been in force in Austria.

Figure 1. Announcement of the implementation of DSGVO (GDPR)

Source: Own representation

The Austrian data protection act (Datenschutzgesetz, short DSG) supplements the Data Protection Regulation (GDPR). The Datenschutzgesetz was extensively modified. Older versions are no longer useful. The title of the older version of the law was "Datenschutzgesetz 2000" (DSG 2000). As a national data protection law, the DSG in its current version is only of a supplementary nature.

Although the basic data protection regulation is directly applicable as an EU regulation in every EU Member State, it contains numerous opening clauses and leaves the national legislator some leeway. In Austria, two amendments to the Data Protection Act (the "Data Protection Adaptation Act 2018" and the "Data Protection Deregulation Act 2018") were adopted to implement these opening clauses and margins (in addition to amendments to numerous material laws).

The Data Protection Adaptation Act 2018 was published in BGBl I No. 120/2017, the Data Protection Deregulation Act 2018 in BGBl I No. 24/2018. Both came into force on 25 May 2018. Since this date, both the provisions of the Data Protection Basic Regulation and the Austrian Data Protection Act as amended by the Data Protection Adaptation Act 2018 and the Data Protection Deregulation Act 2018 have to be observed (Österreichische Datenschutzbehörde[1] 2019).

Legal basis of the data protection law in Austria are:

- the European Data Protection Basic Regulation (GDPR) and
- the Austrian Data Protection Act (DSG - österreichisches Datenschutzgesetz) as amended by the Data Protection Adaptation Act 2018 and the Data Protection Deregulation Act 2018.

The European General Data Protection Regulation (full title: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data, on the free movement of such data and repealing Directive 95/46/EC) will be the basis of general data protection law in the EU and Austria from 25 May 2018 (Österreichische Datenschutzbehörde[1] 2019).

In contrast to the old Data Protection Directive, the European General Data Protection Regulation (GDPR) is directly applicable in Austria. The Data Protection Act only supplements the GDPR. The data protection authority is the national supervisory authority in Austria (Österreichische Datenschutzbehörde1 2019).

1.2. CZECH REPUBLIC

The only legislation concerning the topic of web security is focused on Cyber security. The law understands cyber security in a much narrower sense than it must be viewed by company practices. As the existing law stands, we must separate cyber security of the state from other forms of information security of the individual, that is personal data protection, commercial secrets protection, protection from standard criminal activities directed to information (information criminality) etc. Security manager must therefore employ not only legislation directly concerned with cyber security but also a vast criminal, administrative and civil legislation defining those legal obligations which bear upon various forms of obtaining, processing, storing and communication of information.

Hence, the law perceives cyber security as the defence of the national cyberspace against security threats. Isolated security incidents can of course achieve such intensity as to have a negative impact on a national scale, e.g. failure of a trunk network. However, majority of normally occurring incidents do not attain such an intensity to warrant a response on the national

cyber security – these phenomena are then dealt with legally using standard protection statutes of the criminal, administrative and civil legislation. A typical example can be a leak of personal data or penetration into a company information system.

In the relation of cyber security in the narrower sense of the word (that is, as it is perceived by existing law) it is necessary in company practice to tackle primarily the issues of protecting company information infrastructure from external attacks and this includes also the appropriate detection of such attacks. Of equal importance, from the legal point of view, is also the prevention of company information infrastructure to be used for an outside attack. Under existing law it is short of impossible to punish a company for not using appropriate security measures in an own network (the only exceptions in this direction are related to secret information). However, in some definite cases a company can be made legally responsible for damage caused to the employees, customers or third parties due to insufficient security of the information infrastructure. Similar to other Euro-Atlantic countries, intensive work has been underway in the Czech Republic in the area of specific legal framework of national cyber security. This framework shall primarily and newly demand that providers of electronic services implement in their networks certified security technologies. At the same time, under the coordination of the National Security Authority, a supervisory government body will be created and this will operate as the centre of the protection for the state and critical communication infrastructure as well as a body for critical management in case of a massive attack on a national scope. Furthermore, the activities of the national supervisory body will be amended to include information evaluation of security incidents coming from the private sphere and to coordinate protection modes with the providers of concrete networks (the national body is in a work-in-progress operation at present, as based on a memorandum between CZ.NIC and Ministry of the Interior of the Czech Republic.

1.3. PORTUGAL

The general data protection regulation (Regulation EU - European Union 2016/679) became directly applicable in Portugal.

Since this day, processing personal data in Portugal is mainly governed by the GDPR and while there is no general cybersecurity or cyber defence legal framework, there is sectoral legislation concerning the security of communication services and networks.

In Portugal, several studies confirm that the majority of the Portuguese companies are bad prepared for the requirements arising from the GDPR. This regulation aims to increase public confidence in public and private entities, creating a more stable, clear and predictable legal regime, ending the differences between the EU - European Union member states.

Because of this, the GDPR has a major impact on public authorities and companies. The most important ones for the Portuguese companies are described bellow:

1. **Changing the paradigm of the regulation model:** the responsibility for ensuring the legal treatment of information is passed on to the controller. Thus, in addition to ensuring the legal treatment, the controller must still be able to demonstrate compliance with the requirements of the new regulation. With this new model, CNPD - Comissão Nacional de Proteção de Dados and all European control authorities are responsible for inspect and analyze potential violations related to the application of GDPR.

2. **Strengthening the rights of data subjects:** this new regulation implies two more rights to the holders: the right to forgetfulness and the right to portability of data. Also, the titular can ask for the delete of his/her personal data without undue delay in some situations. Besides this, all data must be erased as soon as it is no longer needed to offer the proposed service or if it has been obtained (or processed) in a way that is not in accordance with the law. All the personal information in paper doesn't have the portability right.

3. **Obtain consent:** the consent needs to be translated into a positive act, through which the data owner consents to the processing of his/her personal data. In this way, a simple tacit consent by the holder is not enough and we need an act or declaration. Thus, silence, pre-validated options or omission should not constitute a valid consent.

4. **Need to assign a data protection officer:** the election of a DPO - Data Protection Officer is one of the biggest news. All public entities, as well as a big part of private entities, should elect a DPO that will have to control an adequate personal data treatment in the organizations that he/she is responsible for. There is no obligation to notify regulators of any processing under the GDPR.

5. **Assessments on the impact on personal data:** if the treatment is likely to involve a high risk for the rights and the liberty of the data owners, the person responsible for the treatment should elaborate one impact assessment on data. This evaluation will happen every time that there is a new treatment related to personal data.

6. **Violation of personal data:** the violation of personal data implies, if accidentally or illicit, the unauthorized destruction, loss, alteration, disclosure or access to personal data. In these cases, the responsible should notify the responsible control authority in the next 72 hours after the violation of personal data happens. On the other hand, if the personal data violation implies a high risk regarding the rights and freedom of the data owners this information should be communicated to the personal data owners.

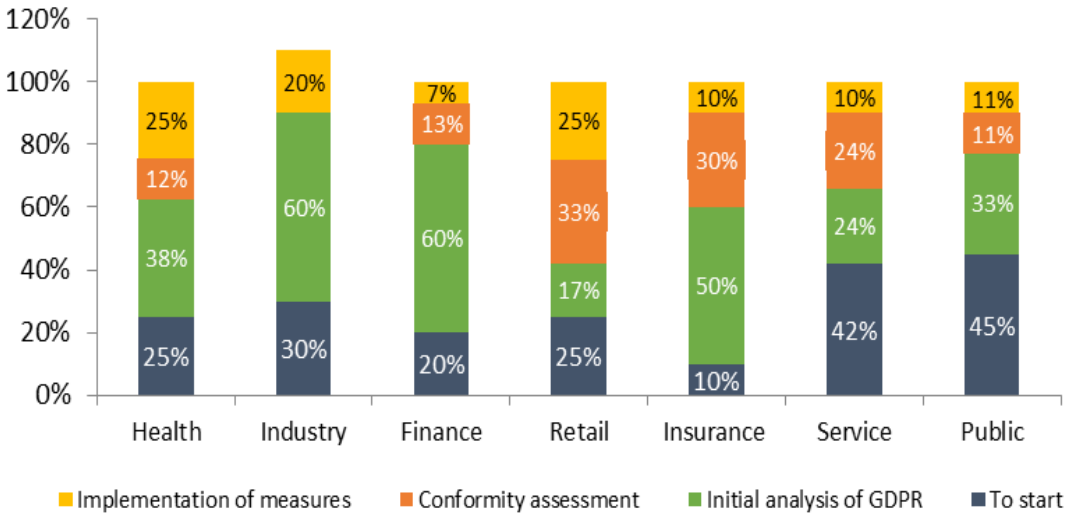
7. **Sanctioning regime:** with this new regulation the fines can reach up to 20 millions euros or 4% of the annual invoicing (whichever is greater). Besides this, a violation of the GDPR will have also reputational and commercial damages at the end of the procedure.

8. **Procedures for the fulfilment of the rights of holders:** the figure of the DPO has an important role in this stage because he/she will act as a link between the data holder of the data and the company that he/she is responsible for. The DPO should also guarantee that all the procedures for the exercise of rights by the data subjects are also created.

According to a study carried out by the consultant KPMG in 2017, some Portuguese companies are more aware of their obligations and challenges regarding the implementation of the GDPR. The companies also anticipate a significant impact on its implementation and 85% pf the companies in 2017 hadn't started the process of implementing effective measures to meet the requirements of the GDPR a little over a year after the regulation came into force.

Health and retail sector were the two sectors more exposed to bigger volumes of personal data. The sector that is more regulated is the PSD2 - Payment Service Directive 2 (finance sector).

Figure 2. Awareness session with GDPR, by sector (2017)



Source: KPMG "O Impacto do Regulamento Geral de Proteção de Dados em Portugal"

In Portugal, the results also show that:

- Only **23%** of the companies fully comply with the requirements set by GDPR;
- **15%** of the companies have institutional practices that ensure the right to forgetfulness regarding personal data collection consent;
- **5%** have practices to address the right to data portability.

The main conclusions of this study also indicate that:

- The **GDPR doesn't define in an objective way** what should be implemented for the personal data protection and each organization is responsible for the identification and implementation of these measures depending on the risk to which personal data are exposed;
- **65%** of the companies consider that they have a high or medium degree of consciousness about the obligations and the impact of GDPR;
- **53%** predict a high or very high impact regarding the implementation of GDPR;
- **65%** consider that the multiplicity of data processing process as one of the biggest challenges regarding the conformity of GDPR;
- **85%** still didn't start to implement effective measures to ensure the conformity with GDPR;
- **43%** selected one responsible person to ensure all the conformity with the legal obligations of personal data protection;
- **32%** have contracts with clauses related to data protection with all third entities that are responsible for personal data treatment;
- **10%** consider that they promote proper awareness and training actions about personal data protection;
- **43%** have procedures implemented if they have a personal data incident.

In 2018, the public organism that supports SMEs - Small and Medium-sized Enterprises - IAPMEI - Agência para a Inovação - did a questionnaire along with the consultant LCG Consultoria, S.A. that aimed to promote attention about the RGDP for companies. This survey included 1.375 answers and was carried out between March and April 2018.

The **main results** of this survey are as follows:

- **27%** of the survey respondents said that they know in detail the RGDP;
- **49%** of the companies affirm that they are partially prepared for the application of RGDP;
- **35%** confirm that their company may have a financial penalization;
- **8%** of the companies said that they have all proper measures to respond the requirements of the RGDP;
- **17%** confirm that they already have a plan that guarantees the proper application of RGDP;
- **3%** of the organizations consider that they need to increase the number of workers dedicated to personal data protection;

- **39%** of the companies recognize the need to enhance the information and promote training for the workers about the RGDP and the main impacts;
- **62%** of the companies consider that they have a basic knowledge (without big details) about the RGDP. The financial and insurance sector, human health and social support activities and retail and wholesale trade are the ones that have more knowledge;
- **50%** of the companies consider that a data protection program is a priority for the information management especially for medium and big enterprises;
- **33%** know the existence of punishments in case of some breach related to RGDP;
- **44%** of the companies consider that they have formal policies implemented in some areas and departments in their organization while **29%** consider that they don't have any data protection policies.

1.4. SPAIN

On December 6, 2018, the Official Gazette of Spain published the Organic Law 3/2018, of December 5, on the Protection of Personal Data and the Guarantee of Digital Rights.

According to Article 1, this law has a double object. First, it adapts the Spanish legal system to the General Data Protection Regulation and further provides specifications or restrictions of its rules as explained in the GDPR.

In this sense, the law states that the fundamental right to data protection of natural persons, under Article 18.4 of the Spanish Constitution, shall be exercised under the GDPR and this law.

Second, the law guarantees the digital rights of citizens and employees, beyond the GDPR. For example, the law includes provisions on the right to internet access, the right to digital education, the right to correction on the internet and the right to digital disconnection in the workplace.

The law entered into force Dec. 7, 2018, the day following its publication on the Official Gazette.

The Organic Law 15/1999, of December 13, on the Protection of Personal Data is repealed, except with regard to several articles related to the processing of personal data in the police and judicial sectors until a law adopts the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

As well, the Royal Decree-Law 5/2018, of July 27, on urgent measures for the adaptation of Spanish Law to European Union regulations on data protection is repealed, along with any regulations that contradict, oppose or are incompatible with the GDPR and this law.

2. WHAT REGULATIONS COMPLEMENT THE EUROPEAN REGULATIONS IN YOUR COUNTRY? INCLUDE A BRIEF SUMMARY OF THE LAWS

2.1. AUSTRIA

In contrast to the old Data Protection Directive, the European General Data Protection Regulation (GDPR) is directly applicable in Austria. The Data Protection Act only supplements the GDPR.

The Data Protection Directive for the area of Justice and Home Affairs is a directive, not a regulation, and must therefore be implemented, which was also done in the DSG (see §§ 36-61 DSG). This Directive is based on EU Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by the competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or of the enforcement of sentences, on the free movement of data and repealing Council Framework Decision 2008/977/JHA (Österreichische Datenschutzbehörde[1], 2019).

In this section you will not find complete legal texts, but individual provisions from laws and regulations relating to data protection:

§ 16 General Civil Code (ABGB), JGS No. 946/1811

I. From the character of the personality / Congenital rights

Every human being has innate rights which are plausible even by reason and is therefore to be regarded as one person. Slavery or serfdom, and the exercise of any related power, is not permitted in these countries (Bundesministerium für Digitalisierung und Wirtschaftsstandort[1] 2019).

§ 1328a General Civil Code (ABGB), JGS No. 946/1811

1b. the right to privacy

§ 1328a. (1) Anyone who unlawfully and culpably encroaches upon the privacy of a person or discloses or exploits circumstances from the privacy of a person shall compensate him for the resulting damage. In the case of substantial violations of the private sphere, for

example if circumstances arising therefrom are exploited in such a way as to expose the person in public, the claim for compensation also includes compensation for the personal impairment suffered.

(2) Para. 1 shall not apply if an invasion of privacy is to be assessed in accordance with special provisions. Responsibility for violations of privacy by the media shall be governed solely by the provisions of the Media Act, Federal Law Gazette No. 314/1981, as amended (Bundesministerium für Digitalisierung und Wirtschaftsstandort[2] 2019).

§ 10 Employment Contract Law Adaptation Act (AVRAG), BGBl. No. 459/1993

control measures

§ (1) The introduction and use of control measures and technical systems which affect human dignity is not permitted unless these measures are regulated by a works agreement within the meaning of § 96 Para. 1 No. 3 ArbVG or are carried out in establishments in which no works council is established with the consent of the employee.

(2) The employee's consent may be terminated in writing at any time without notice, unless there is a written agreement with the employer on the duration of the agreement (Bundesministerium für Digitalisierung und Wirtschaftsstandort[3] 2019).

§ 91 Labour Constitution Act, Federal Law Gazette No. 22/1974

General Information

§ 91 (1) The employer is obliged to inform the works council about all matters affecting the economic, social, health or cultural interests of the employees of the enterprise.

(2) The company owner shall inform the works council of the types of personal employee data which he records automatically and which processing and transmissions he provides for. Upon request, the works council shall be enabled to check the basis for processing and transmission. Unless an unlimited right of inspection of the works council results from § 89 or other legal regulations, the consent of the works council is required to inspect the data of individual employees.

(3) If a works agreement pursuant to § 97 para. 1 no. 18a has been concluded, the company owner shall submit the audit report or its abridged version (§ 21 para. 6 Pensionskassengesetz) and the accountability report (§ 30 para. 5 Pensionskassengesetz) to the works council immediately after contributions from the pension fund (Bundesministerium für Digitalisierung und Wirtschaftsstandort[4] 2019).

§ 96 Labour Constitution Act, Federal Law Gazette No. 22/1974

Measures requiring consent

§ 96 (1) The following measures taken by the holder shall require the agreement of the works council in order to be legally effective:

1. The introduction of a company disciplinary system;

2. the introduction of personnel questionnaires, insofar as these do not merely contain general personal data and information on the technical prerequisites for the intended use of the employee;

3. the introduction of control measures and technical systems to control workers where such measures (systems) affect human dignity;

4. insofar as there is no regulation by collective agreement or articles of association, the introduction and regulation of piecework and low wages as well as piecework-like premiums and salaries - with the exception of homework salaries - based on statistical procedures, data recording procedures, micro time procedures or similar remuneration calculation methods, as well as the relevant principles (systems and methods) for determining and calculating these wages and salaries.

(2) Company agreements in the matters referred to in para. 1 may be terminated in writing at any time without notice by either of the contracting parties, provided that they do not contain any provisions on their period of validity. § 32 (3), second sentence, shall not apply (Bundesministerium für Digitalisierung und Wirtschaftsstandort[5] 2019).

§ 96a Labour Constitution Act, BGBl. No. 22/1974

Replaceable consent

§ 96a. (1) The following measures of the holder require the approval of the works council in order to be legally effective:

1. The introduction of systems for the automated determination, processing and transmission of the employee's personal data, which go beyond the determination of general personal data and technical requirements. An agreement is not necessary, as far as the actual or intended use of these data does not go beyond the fulfilment of obligations, which result from law, standards of the collective right organization or work contract;

2. the introduction of systems for the evaluation of employees of the establishment, insofar as such data are collected which are not justified by the use of the establishment.

(2) The agreement of the works council pursuant to subsection 1 may be replaced by a decision of the conciliation body. In all other respects §§ 32 and 97 Para. 2 shall apply mutatis mutandis.

(3) Paragraphs 1 and 2 shall not affect the rights of approval of the works council resulting from § 96 (Bundesministerium für Digitalisierung und Wirtschaftsstandort[6] 2019).

§ 132 Federal Tax Code Federal Law Gazette No. 194/1961

§ 132 (1) Books and records as well as the supporting documents belonging to the books and records shall be kept for seven years; in addition, they shall be kept for as long as they are of significance for proceedings pending for the levying of duties in respect of which those party positions are held for which the books and records were to be kept on the basis of tax regulations or for which books were kept without a statutory obligation. If business papers

and other documents are important for the collection of duties, they shall be kept for seven years. These periods shall run, in respect of books and records, from the end of the calendar year for which the entries have been made in the books or records and, in respect of supporting documents, business documents and other records, from the end of the calendar year to which they relate; in the case of a marketing year other than the calendar year, the periods shall run from the end of the calendar year in which the marketing year ends.

(2) With regard to the documents, business papers and other records referred to in paragraph 1, storage may be on data carriers if the complete, orderly, identical and true to original reproduction is guaranteed at all times until expiry of the statutory storage period. If such documents are only available on data carriers, the requirement of faithful reproduction shall not apply.

(3) Whoever has carried out storage in the form of para. 2 must, insofar as he is obliged to grant inspection, make available at his own expense within a reasonable period those aids which are necessary to make the documents legible and, insofar as necessary, provide durable reproductions which can be read without aids. Where durable reproductions are produced, they shall be made available on data carriers (Bundesministerium für Digitalisierung und Wirtschaftsstandort[7] 2019).

Article 8 Federal Constitution Act (B-VG);

Art. 8. (1) German is the official language of the Republic without prejudice to the rights provided by Federal law for linguistic minorities.

(2) The Republic (the Federation, member states and municipalities) is committed to its linguistic and cultural diversity which has evolved in the course of time and finds its expression in the autochthonous ethnic groups. The language and culture, continued existence and protection of these ethnic groups shall be respected, safeguarded and promoted.

(3) The Austrian sign language is recognized as an independent language. The laws shall determine the details (Bundesministerium für Digitalisierung und Wirtschaftsstandort[8] 2019).

§ 5 E-Commerce Act (ECG), BGBl. I No. 152/2001

information duties / General Information

§ 5 (1) A service provider shall at all times make available to users at least the following information easily and directly accessible:

1. his name or company name;
2. the geographical address at which he is established;
3. Information enabling users to contact him quickly and directly, including his electronic mail address;
4. where available, the commercial register number and the commercial register court;
5. if the activity is subject to official supervision, the supervisory authority responsible for it;

6. in the case of a service provider subject to commercial or professional regulations, the chamber, professional association or similar body to which he belongs, the professional title and the Member State in which it was awarded, and a reference to the applicable commercial or professional regulations and access to them;

7. the VAT identification number, if any.

(2) Where prices are quoted in information society services, they shall be displayed in such a way that they can be easily read and identified by an observant average viewer. It must be clearly identifiable whether the prices, including value added tax and all other levies and surcharges, are labelled (gross prices) or not. In addition, it must also be indicated whether shipping costs are included.

(3) Other information obligations shall remain unaffected (Bundesministerium für Digitalisierung und Wirtschaftsstandort[9] 2019).

§ 6 E-Commerce Act (ECG), BGBl. I No. 152/2001

Information on commercial communication

§ 6. (1) A service provider shall ensure that commercial communications which are part of or constitute a service of the information society are clearly and unambiguously

1. is recognizable as such,

2. the natural or legal person who commissioned the commercial communication is identifiable,

3. promotional offers such as premiums and gifts are recognizable as such and include easy access to the conditions for their use, and

4. contests and sweepstakes are identified as such and include easy access to the conditions of participation.

(2) Other obligations to provide information for commercial communication and legal provisions concerning the admissibility of offers for sales promotion and prize contests and sweepstakes shall remain unaffected (Bundesministerium für Digitalisierung und Wirtschaftsstandort[10] 2019).

§ 7 E-Commerce Act (ECG), BGBl. I No. 152/2001

Unsolicited commercial communication

§ 7 (1) A service provider who legitimately sends a commercial communication by electronic mail without the prior consent of the recipient shall ensure that the commercial communication is clearly and unambiguously identifiable as such upon its receipt by the user.

(2) Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH) shall maintain a list in which those persons and companies may register free of charge who have excluded themselves from receiving commercial communications by electronic mail. The service providers mentioned in Par. 1 shall observe this list.

(3) Legal provisions regarding the admissibility and inadmissibility of the transmission of commercial communications by electronic mail shall remain unaffected (Bundesministerium für Digitalisierung und Wirtschaftsstandort[11] 2019).

§ 8 E-Commerce Act (ECG), BGBl. I No. 152/2001

Commercial communication for members of regulated professions

§ 8 (1) For service providers who are subject to professional regulations, commercial communication which is part of or constitutes a service provided by them for the information society shall be permissible.

(2) Professional regulations restricting commercial communication for members of these professions, in particular in order to safeguard the independence, dignity and honor of the profession, to safeguard professional secrecy and to observe fair conduct towards customers and other members of the profession, shall remain unaffected (Bundesministerium für Digitalisierung und Wirtschaftsstandort[12] 2019).

§ 67 Genetic Engineering Act, Federal Law Gazette No. 510/1994; § 67 Genetic Engineering Act

Prohibition of the collection and use of data from genetic tests for certain purposes

Sect. 67. Employers and insurers including authorized representatives and coworkers thereof are prohibited to collect, to demand, to accept or else to make use of results from genetic tests of their employees, job applicants or insurees or insurance canvassers. This prohibition also covers the demand for delivery and the acceptance of body substances for genetic test purposes (Bundesministerium für Digitalisierung und Wirtschaftsstandort[13] 2019).

§ 152 Industrial Code 1994, Federal Law Gazette No. 194/1994

credit bureaus about credit conditions

§ 152 (1) Tradespeople who are entitled to exercise the trade of credit agencies on credit relationships are not entitled to provide information on private relationships that are not related to creditworthiness.

(2) The tradesmen referred to in para. 1 shall be obliged to keep their business correspondence and books of account for seven years. The period of seven years shall run from the end of the calendar year in which the correspondence took place or the last entry was made in the business register. If the trade licence is terminated, the correspondence and business records must be destroyed, even if the period of seven years has not yet expired (Bundesministerium für Digitalisierung und Wirtschaftsstandort[14] 2019).

§ 18 Reporting Act 1991, BGBl. No. /1992

reporting information

§ 18 (1) Upon request, the registry authority shall provide information, against proof of identity, as to whether and, if applicable, where within the territory of the Federal Republic a clearly identifiable person is registered. If the person sought does not appear to be registered or if there is a ban on providing information about him or her, the information provided by the registration authority shall read as follows: "No data is available on the person or persons sought for registration information". If the information of the person

who submitted the request cannot be attributed to only one person, the information of the registration authority must read: "On the basis of the information on identity, the person sought cannot be clearly identified; no information can be provided". For the competence to provide information, the domicile (registered office) or residence (§ 3 no. 3 AVG) of the person making the request is decisive.

(1a) Depending on the technical possibilities, registration information may also be requested and issued in long-distance data traffic from the Central Register of Residents using the citizen card (E-GovG, Federal Law Gazette I No. 10/2004). The amount of the administrative fee to be paid for this is to be determined in the ordinance pursuant to § 16a Para. 8.

(2) Any registered person may apply to the registration authority for information not to be provided (information embargo). The application shall be granted if a legitimate interest is substantiated. If such an interest is manifest, the information embargo may also be imposed ex officio or extended. The information embargo may be ordered or extended for a maximum period of two years; during this period it shall also apply in the event of deregistration.

(2a) A ban on the provision of information shall apply ex officio to notifications based on detention slips (release slips).

(3) An application for waiver or extension of an information ban may also be submitted to the registration authority of a previous accommodation subject to registration; in all other respects, subsection 2 shall apply.

(4) The information block shall be revoked as soon as it becomes apparent that

1. the applicant wishes to evade legal obligations by blocking information, or
2. the reason for the release of the information block has ceased to apply.

(5) Insofar as an information block exists with regard to a person, the information of the registration authority shall read as follows: "There are no data available on the person(s) sought for registration information". Information pursuant to para. 1 shall be provided in such cases if the applicant proves that he can assert a legal obligation of the person concerned. In such a case, the registry office must notify the person obliged to provide the information and give him the opportunity to make a statement before issuing the information.

(6) Administrative charges shall be payable for the provision of reporting information pursuant to subsection (1) above which shall be determined by the Federal Minister of the Interior in agreement with the Federal Minister of Finance by ordinance (Bundesministerium für Digitalisierung und Wirtschaftsstandort[15] 2019).

§ 20 Reporting Act 1991, BGBl. No. 9/1992

Other transmissions

§ (1) If the registration authority uses the address as a selection criterion for the population register, it shall, upon request and upon proof of ownership, disclose to the owner of a house the name and address of all persons registered in the house, staircase or apartment

from the population register. § Section 18 (5) shall apply subject to the proviso that in the event of a ban on access to information

1. the naming of this person is omitted however
2. the information is also given if the applicant proves that he can assert with the information a legal obligation in connection with the dwelling concerned.

The information is to be introduced with the sentence: "The obligation to provide information refers to the following residents of the house". The homeowner may only use the registration data transmitted to him in order to fulfil obligations imposed on him by this federal law and to assert rights against house occupants.

Note: Paragraph 2 shall cease to apply with the commencement of the operation of the Central Register of Residents (cf. § 23 Paragraph 5 in conjunction with § 16b Paragraph 4 as amended by Art. I BGBl. I No. 28/2001).

(3) The registration data contained in the register of residents or in the central register of residents shall be transmitted to the organs of the regional or local authorities upon request, whereby the request may only be made in the specific case if it constitutes an essential prerequisite for the recipient to perform the tasks assigned to him; transmissions on the basis of requests for linkage (§ 16a para. 3) are moreover only permissible if the proportionality to the cause and the desired success is maintained. The mayors are authorized to use the registration data contained in their register of residents or transmitted to them pursuant to para. 2, insofar as these form an essential prerequisite for the performance of the tasks assigned to them by law.

(4) In the case of a query authorization granted to the district administrative authorities or provincial police directorates pursuant to § 16a, Sub-Clause 4, it shall be provided that all those registered with non-Austrian citizenship in their local area of activity may be selected for purposes of alien police.

(5) In the case of a right to query granted to the military command of each country pursuant to § 16a para. 4, provision shall be made for the eligibility of all conscripts registered in their local area of activity who have not yet reached the age of 50.

(6) The registration authorities shall be obliged to notify an administrative authority of the reason for such notification on the basis of a reference to a person (§ 14 para. 2).

(7) The mayors shall be obliged to provide the legally recognized religious societies, upon request, with the registration data of all persons registered in the municipality who have committed themselves to these religious societies. A request for a link to a particular religious creed may only be processed on the basis of a corresponding request.

(Note: para. 8 repealed by § 23 para. 4 as amended by BGBl. I No. 28/2001).

(Bundesministerium für Digitalisierung und Wirtschaftsstandort[16] 2019).

§ 57 Military Powers Act, BGBl. I No. 86/2000

Legal protection in the field of intelligence services

§ 57 (1) In order to examine the legality of intelligence and defense measures, a legal protection commissioner with two deputies has been set up at the Federal Ministry of

Defense and Sport, who are independent and not bound by instructions and are bound by official secrecy in performing the duties assigned to them under this Act. The legal protection commissioner and his deputies shall have the same rights and duties. They are appointed by the Federal President at the recommendation of the Federal Government after hearing the Presidents of the National Council and the Presidents of the Constitutional Court and the Administrative Court for a term of five years. Re-appointments are permissible.

(2) The legal protection commissioner and his deputies shall have special knowledge and experience in the fields of fundamental rights and freedoms as well as military defense. They must have worked for at least five years in a profession in which a degree in law is a prerequisite for a profession. Soldiers and all federal employees serving in the area of responsibility of the Federal Minister of Defense and Sport may not be appointed outside the presence stand. The appointment expires in the event of renunciation or death or when the new appointment or reappointment becomes effective. If there is a reason to doubt the full impartiality of the legal protection commissioner, the commissioner must refrain from intervening in the matter.

(3) The Federal Minister of Defense and Sport shall provide the legal protection commissioner with the personnel necessary to carry out his administrative duties and shall meet his material requirements. The personnel made available shall be bound exclusively by the instructions of the legal protection commissioner for activities in the affairs of the legal protection commissioner. The Legal Officer shall be entitled to compensation for the performance of his duties. The Federal Minister of Defense and Sport shall issue an ordinance setting lump-sum rates for the assessment of this compensation.

(4) To perform his duties, the legal protection commissioner shall at all times be granted access to all necessary documents and records, shall be provided with copies or duplicates of individual documents free of charge upon request and shall provide all necessary information. Insofar, official secrecy cannot be asserted against him. However, this shall not apply to information and documents concerning the identity of persons or sources whose disclosure would jeopardize national security or human security, and to copies if disclosure would jeopardize national security or human security.

(4a) The ombudsman shall at all times be given the opportunity to monitor the implementation of the measures he/she is to control and to enter any room where recordings or other monitoring results are stored. In addition, he shall monitor compliance with the obligation to correct or delete records in accordance with the provisions of data protection law.

(5) The legal protection commissioner shall report to the Federal Minister of Defense and Sport by 31 March each year at the latest on his activities in the past year. This report shall be made available by the Federal Minister of Defense and Sport to the Standing Subcommittee of the National Council for the Investigation of Intelligence Measures to Secure the Military Defense of the Federal Republic of Germany at the latter's request within the framework of the right to information and inspection pursuant to Art. 52a para. 2 B-VG.

(6) If the legal protection commissioner notices that the use of data has violated the rights of a data subject who is not aware of this use of data, he shall be entitled to do so,

1. to inform the data subject or

2. to file a complaint to the data protection authority pursuant to section 54 subsection 4.

A complaint under no. 2 shall only be admissible if the data subject's knowledge of the existence or content of the data record would jeopardize or significantly impede the safeguarding of the operational readiness of the armed forces or the interests of comprehensive national defense and information under no. 1 therefore cannot be provided. In proceedings before the data protection authority under no. 2, consideration shall be given to Article 26 (2) DSG 2000 on the restriction of the right of access.

(7) (Constitutional provision) A restriction of the powers, rights and duties of the legal protection commissioner may only be decided by the National Council in the presence of at least half of the members with a two-thirds majority of the votes cast (Bundesministerium für Digitalisierung und Wirtschaftsstandort[17] 2019).

§ 53 Security Police Act, BGBl. No. 566/1991

Permissibility of processing

§ 53. (1) The security authorities may ascertain and process personal data

1. for the fulfilment of the first general obligation to provide assistance (§ 19);

2. for the defense against criminal connections (§§ 16 par. 1 fig. 2 and 21);

2a. for extended hazard research (§ 21 para. 3) under the conditions of § 91c para. 3;

3. for the defense against dangerous attacks (§§ 16 paras. 2 and 3 as well as 21 para. 2); including the necessary danger research within the framework of danger defense (§ 16 paras. 4 and 28a);

4. for the prevention of probable dangerous attacks against life, health, morality, freedom, property or the environment (§ 22 paras. 2 and 3) or for the prevention of dangerous attacks by means of crime analysis, if a repeated commission is probable according to the nature of the attack;

5. for search purposes (section 24);

6. in order to maintain public order in the event of a particular event;

7. for the analysis and evaluation of the probability of endangerment of constitutional institutions and their capacity to act through the implementation of an offence in accordance with the Fourteenth and Fifteenth Sections of the Penal Code.

(2) The security authorities may ascertain and further process data which they have processed in execution of federal or Land laws for the purposes and under the conditions set forth in para. 1; however, they are prohibited from carrying out an automated data comparison within the meaning of § 141 of the Code of Criminal Procedure. Existing transmission prohibitions remain unaffected.

(3) The security authorities shall be entitled to demand information from the authorities of the regional authorities, other public corporations and the institutions operated by them which they require for the defense against dangerous attacks, for extended risk research

under the conditions set out in para. 1 or for the defense against criminal connections. A refusal of information is only permissible if other public interests outweigh the defensive interests or if there is any other legal obligation of secrecy going beyond official secrecy (Art. 20 para. 3 B-VG).

(3a) The security authorities are entitled to demand information from operators of public telecommunications services (§ 92 Par. 3 No. 1 Telecommunications Act 2003 - TKG 2003, BGBl. I No. 70) and other service providers (§ 3 No. 2 E-Commerce Act - ECG, BGBl. I No. 152/2001):

1. on the name, address and subscriber number of a specific connection if this is necessary to fulfill the tasks assigned to them under this Federal Act,
2. via the Internet protocol address (IP address) to a specific message and the time of its transmission, if you have used this data as an essential prerequisite for the defense
    a) a concrete danger to a person's life, health or freedom within the framework of the first general obligation to provide assistance (§ 19),
    b) a dangerous attack (§ 16 par. 1 fig. 1) or
    c) of a criminal connection (§ 16 Paragraph 1 No. 2),
3. the name and address of a user to whom an IP address was assigned at a certain point in time, if this data was used as an essential prerequisite for the defense against the use of IP addresses by third parties.
    a) a concrete danger to a person's life, health or freedom within the framework of the first general obligation to provide assistance (§19),
    b) a dangerous attack (§ 16 par. 1 fig. 1) or
    c) a criminal connection (Art. 16 Par. 1 No. 2),even if this requires the use of retention data pursuant to Art. 99 Par. 5 No. 4 in conjunction with Art. 102a TKG 2003,
4. the name, address and subscriber number of a particular line by reference to a call conducted by that line by indicating the most accurate time period possible and the passive subscriber number, if this is necessary to fulfil the first general obligation to provide assistance or to ward off dangerous attacks.

(3b) If, on the basis of certain facts, it can be assumed that there is a present danger to a person's life, health or freedom, the security authorities shall be entitled to request information from operators of public telecommunications services regarding location data and the international mobile subscriber identification (IMSI) of the terminal equipment carried by the person at risk or accompanying him in order to assist or avert this danger, even if the use of data retention in accordance with section 99 subsection (2) of the Basic Data shall not be required for this purpose. 5 No. 3 in conjunction with Art. 102a TKG 2003, as well as technical means for localizing the terminal equipment.

(3c) In the cases of subsections 3a and 3b, the safety authority shall be responsible for the legal admissibility of the request for information. The requested body is obliged to provide the information immediately and, in the case of para. 3b, against reimbursement of costs in accordance with the Surveillance Costs Ordinance - ÜKVO, BGBl. II No. 322/2004. In the

case of para. 3b, the safety authority must also submit written documentation to the operator without delay, at the latest within 24 hours. In the cases of Paragraph 3a(3) and Paragraph 3b, the safety authority is obliged to inform the person concerned that information has been obtained on the assignment of his name or address to a specific IP address (§ 53 Paragraph 3a(3)) or on location information (§ 53 Paragraph 3b) if the use of retention data pursuant to § 99 Paragraph 5(3) or (4) in conjunction with § 102a TKG 2003 was required for this purpose. The person concerned must be informed of the legal basis as well as the date and time of the request as soon as possible and in a verifiable manner. The information of the data subject may be postponed as long as it would endanger the purpose of the investigation and may be omitted if the data subject has already demonstrably gained knowledge or the information of the data subject is impossible.

(3d) In order to prevent and ward off dangerous attacks against the environment, the safety authorities shall be entitled to demand information from the authorities of the Federal Government, the Länder and local authorities on installations and facilities approved by them where, due to the use of machinery or equipment, the storage, use or production of substances, the mode of operation, the equipment or for other reasons, it is particularly to be feared that, in the event of a deviation of the installation or facility from the state in which it is in conformity with the legal system, a danger to the life or health of several people or, to a large extent, a danger to property or the environment may arise. The requested authority shall be obliged to provide the information.

(4) Apart from the cases of paras. 2 to 3b and 3d, the safety authorities shall be entitled for the purposes of par. 1 to determine and process personal data from all other available sources by using appropriate means, in particular by accessing generally accessible data.

(5) The security authorities shall be authorized, in individual cases and subject to the conditions of § 54 Para. 3, to use personal image data for the defense against dangerous attacks and criminal connections, if certain facts indicate a serious danger to public security, for extended risk research (§ 21 Para. 3) and for searches (§ 24), which legal entities of the public or private sector have legitimately identified by means of image and sound recording equipment and transmitted to the security authorities. Particular care shall be taken to ensure that any interference with the privacy of the persons concerned is proportionate (§ 29) to the cause. The use of data on non-public conduct is not permitted (Bundesministerium für Digitalisierung und Wirtschaftsstandort[18] 2019).

§ 53a Security Police Act, BGBl. No. 566/1991

Data applications of the security authorities

§ 53a. (1) The security authorities may process data on natural and legal persons as well as property and buildings for the management, administration and coordination of operations, in particular of focal security police actions, searches or orderly events as well as for the protection of persons and property and the fulfilment of the first general duty to provide assistance. The necessary identification and accessibility data may be processed for persons who are affected by an official act, for those who submit applications, notifications

or other communications, for endangered persons or institutions and for witnesses and other persons who are to be informed in the course of an official act, as well as for persons who are wanted, including a photograph and any existing description of their appearance and clothing. In addition, the necessary factual data including vehicle registration number, information on time, place, reason and type of intervention as well as administrative data may be processed.

(2) The security authorities may, for the defence against criminal connections or dangerous attacks as well as for the prevention of dangerous attacks, if the nature of the attack makes repeated perpetration probable, by means of operational or strategic analysis

1. to suspects
   a) Names,
   b) former names,
   c) Alias data,
   d) Names of parents,
   e) Sex,
   f) Date and place of birth,
   g) Nationality,
   h) Residential address/stay,
   i) other data required for personal description,
   j) Document data,
   k) Occupation and qualification/employment/living conditions,
   l) I've got some I.D. data,
   m) information on economic and financial circumstances, including related data of legal persons; and
   n) pertinent data on means of communication and transport and weapons, including registration numbers/markings,
2. victims or persons for whom certain facts give reason to believe that they may become victims of an offence punishable by a serious penalty, data types 1. a) to k) and reasons for victimization and damage sustained,
3. for witnesses, data types 1. a) to j) and data relevant to witness protection,
4. for contact persons or escorts who are not only in accidental contact with suspects and for whom there are sufficient grounds to believe that information on suspects can be obtained via them, data types 1. a) to n) until the relationship with the suspect has been clarified as quickly as possible, and
5. for informants and other persons providing information, data types 1. a) to j),

as well as factual and case-related information and administrative data, even if the data concerned is particularly worthy of protection within the meaning of § 4 no. 2 DSG 2000.

(3) The security authorities shall be authorized to keep records of removal orders, prohibitions to enter and interim injunctions to protect against violence in the family for persons against whom such a measure has been ordered, names, date and place of birth,

sex, relationship to the person at risk, nationality, residential address, names, date and place of birth, sex, nationality, relationship to the person at risk, address and accessibility data as well as type of measure, previous measures, area (address, detailed description) to which the measure relates, certain facts on which the measure is based (in particular previous dangerous attack), period of validity of the measure, infringements of ordered measures, place of delivery for the purpose of service of the lifting of the prohibition of entry or an interim injunction according to § 382b EO, and administrative data. The data of victims shall be deleted after one year at the latest. In the case of more than one storage, the deletion is determined by the time of the last storage.

(4) In order to keep evidence of directions and prohibitions to enter in protection zones, the security authorities shall be authorized to process names, date and place of birth, gender, nationality, residential address, type of measure, area (address, detailed description) to which the measure relates, certain facts on which the measure is based (in particular previous dangerous attack), duration of validity of the measure and administrative data for persons against whom such a measure has been ordered.

(5) Where a joint processing by several security authorities is necessary due to a use involving several explosives, data applications in accordance with para. 1 may be managed in the information network system. The data shall be deleted after completion and evaluation of the deployment, but at the latest after one year. Transmission of the data processed pursuant to para. 1 shall only be permitted if expressly authorized by law.

(6) Where joint processing by several security authorities is required, data applications in accordance with para. 2 may be maintained in the information network system. Data pursuant to par. 2 fig. 1 shall be deleted at the latest after three years, data pursuant to par. 2 fig. 2 and 3 at the latest after one year, data pursuant to par. 2 fig. 4 shall be deleted at the latest after three years if there are no sufficient grounds for acceptance pursuant to this item, but at the latest after three years and data pursuant to par. 2 fig. 5 shall be deleted at the latest after three years. In the case of several storage operations under the same number, the deletion shall be determined by the time of the last storage operation. Transfers to security authorities, public prosecutors' offices and ordinary courts for the purposes of criminal justice and other purposes are only permissible if there is an express statutory authorization to do so (Bundesministerium für Digitalisierung und Wirtschaftsstandort[19] 2019).

§ 56 Security Police Act, BGBl. Nr. 566/1991

Admissibility of transmission

§ 56. (1) The security authorities may transmit personal data only if

1. if the data subject has expressly consented to the transfer in the case of sensitive data, whereby revocation is possible at any time and results in the inadmissibility of further use of the data;
2. domestic authorities, insofar as this is expressly provided for by law or constitutes an essential prerequisite for the recipient to perform a task assigned to him by law;

3. to suitable victim protection institutions (§ 25 Para. 3), insofar as this is necessary for the protection of endangered persons, whereby personal data are to be transmitted only on endangered persons and persons at risk as well as the documentation (§ 38a Para. 5);

3a. to the Austrian Football Association as well as the Austrian Football League for the examination and initiation of a prohibition of entering sports venues if the person concerned has committed a dangerous attack against life, health or property using force in connection with a major football event. Only the name, date of birth, residential address and details of the reason for the intervention and, if applicable, information on the outcome of the criminal proceedings are to be provided for this purpose;

4. to a person whose legal interest is threatened by a dangerous attack, insofar as this is necessary for his knowledge of the nature and extent of the threat (§ 22 para. 4);

5. if vital interests of a person require the transmission, sensitive data only if the consent of the person concerned cannot be obtained in good time;

6. for the purposes of section 71 subsection 3 line 1 to media companies or by publication by the security authority itself;

7. for the purposes of scientific research and statistics in accordance with § 46 DSG 2000;

8. in the event of an order to prohibit access pursuant to § 38a par. 1 fig. 2, to the head of the respective institution to initiate measures required within the scope of the supervisory duty for the protection of minors at risk. Only the name of the endangered person and the endangered minor as well as the duration of the prohibition of entry and the information about a possible lifting of the prohibition of entry shall be transmitted.

§§ 8 and 9 DSG 2000 shall not apply. For the transmission of personal data for the purposes of international police administrative assistance, the provisions of the Police Cooperation Act, Federal Law Gazette I No. 104/1997, shall apply.

(2) The transmission of personal data shall be recorded. Instead, transmissions from an automated evidence system can be logged; the log records can be deleted after three years. Automated queries in accordance with § 54 Para. 4b are excluded from logging, except in the case of a hit.

(3) If transmitted personal data subsequently prove to be incomplete or incorrect, they shall be corrected vis-à-vis the recipient if this appears necessary to safeguard the interests of the data subject worthy of protection.

(4) The transfer of personal data to authorities other than security authorities is inadmissible if there are indications for the transferring authority that this would circumvent the protection of editorial secrecy (Section 31 (1) Media Act).

(5) The transmission of personal data pursuant to subsection 1(3a) shall only be permissible if the Austrian Football Association and the Austrian Football League have contractually committed themselves to the Federal Minister of the Interior,

1. to use the data only for the specified purpose, within its scope and in accordance with the provisions of the Data Protection Act 2000,
2. to secure the data against unauthorised use in accordance with the provisions of § 14 of the Data Protection Act 2000, in particular by taking organisational and technical precautions to ensure that access to rooms in which the transmitted data can be accessed is only possible by persons acting on their behalf,
3. to comply with their cancellation obligations,
4. to record every query and transmission of the data within their sphere of activity and
5. to grant the security authorities access to rooms and access to data processing equipment and to provide them with the necessary information upon request, insofar as this is necessary to verify compliance with the obligations standardized in subsections 1 to 4.

The Data Protection Council shall be consulted before the Federal Minister of the Interior concludes the contract. Data transmitted by the authority pursuant to para. 1 no. 3a and protocols prepared by the contracting party pursuant to no. 4 shall be deleted by the Austrian Football Association and the Austrian Football Bundesliga upon expiry of a prohibition to enter sports facilities imposed pursuant to para. 1 no. 3a, but no later than two years after the date of transmission. If the respective (Bundesministerium für Digitalisierung und Wirtschaftsstandort[20] 2019).

§ 58d Security Police Act, BGBl. Nr. 566/1991

Central analysis file on violent offences threatened with significant penalty, in particular sexually motivated offences

§ 58d. (1) The security authorities shall be authorized to process personal data in an information network system operated by the Federal Minister of the Interior for the purpose of preventing and preventing acts threatened with punishment against life and limb as well as against sexual integrity and self-determination under threat or use of force and for the early recognition of related serial relationships by means of analysis. Information on homicides, sexual offences involving the use of force, missing persons, if the overall circumstances indicate a crime, and suspicious contact with persons, if there are concrete indications of an act threatened with punishment planned with sexual motive, may be processed. The following types of data may be processed into the identified categories of data subjects, even if they are data requiring special protection within the meaning of § 4 no. 2 DSG 2000:

1. to suspects
   a) Names,
   b) former names,
   c) Sex,
   d) Date and place of birth,
   e) Nationality,
   f) Residential addresses,
   g) Alias data,

h) Reference to judicial convictions and measures as well as previous police knowledge,
i) Occupation and qualification/employment/living conditions,
j) Personal description,
k) identification data and
l) Behavior,

2. for missing data types Z 1. a) to f), i) to k) and

3. for victims the data types Z 1. c) to e), i) and j) as well as f) without door or house number designation, as far as these designations are not necessary for the purpose of the data application.

In addition, factual and case-related data including traces, relationship data and references, object data and other factual data such as weapons or motor vehicles as well as administrative data may be processed. The access rights are to be limited to the group of persons concerned with the processing of the crime areas to be recorded.

(2) The transmission of data to public prosecutors' offices and ordinary courts for the purposes of criminal justice and to prisons is permissible in accordance with the Prison Execution Act. For the rest, transmissions are only permissible if there is an express statutory authorization to do so.

(3) The data of missing persons shall be deleted when the reason for their storage has ceased to exist, but at the latest after 20 years. Data of victims shall be deleted for a maximum of 20 years, of suspects for a maximum of 30 years after inclusion in the file (Bundesministerium für Digitalisierung und Wirtschaftsstandort[21] 2019).

§ 76 Security Police Act, BGBl. No. 566/1991

Special authority responsibility

§ 76. (1). Recognition measures on application (§ 68 para. 1) shall be taken by the district administrative authority, within its local sphere of action by the Provincial Police Directorate as the security authority of first instance (§ 8) to which the intervener addresses himself.

(2) Recognition measures with the consent of the person concerned (§ 68 paras. 3 and 4) shall be taken by the district administrative authority, within its local area of activity by the State Police Headquarters as the security authority of first instance (§ 8), in whose district the person has his main residence or is engaged in the activity relevant to his endangerment.

(3) In the case of Section 72, the Federal Minister of the Interior shall be responsible for the transmission of identification data, and in the cases of Section 71 (4) and (5), for the transmission of identification data to the security authority which carries out the relevant official act.

(4) Notification pursuant to section 73 subs. 3 shall be the responsibility of the security authority which processes the identification data pursuant to section 70. The notification of the deletion of the data from the Central Recognition Service Record shall be the responsibility of the authority which transmitted it to it.

(Note: Paragraph 5 repealed by BGBl. I No. 104/2002)

(6) The deletion of identification data concerning the request of the data subject shall be initiated by the National Police Directorate in whose area of activity the data are processed. If the processing is carried out on behalf of the Federal Minister of the Interior, the latter shall be responsible for handling the application and the communication in accordance with Article 27 (4) DSG 2000.
(Note: Paragraph 7 repealed by BGBl. I No. 13/2012)
(Bundesministerium für Digitalisierung und Wirtschaftsstandort[22] 2019).

§ 7 Consumer Credit Act, BGBl. I No. 28/2010

Checking the creditworthiness of the consumer

§ 7. (1) Before concluding the credit agreement, the creditor shall check the creditworthiness of the consumer on the basis of sufficient information which he requests from the consumer, if necessary; if necessary, he shall also obtain information from an available database.
(2) If this examination reveals considerable doubts as to the consumer's ability to fulfil his obligations under the credit agreement in full, the creditor shall draw the consumer's attention to these doubts as to his creditworthiness.
3. Where creditors and consumers agree to modify the total amount of credit after the conclusion of the credit agreement, the creditor shall update the financial information available to him concerning the consumer and verify the creditworthiness of the consumer before any significant increase in the total amount of credit. Paragraph 2 shall apply mutatis mutandis.
(4) If a credit application is rejected on the basis of a database search, the creditor shall inform the consumer immediately and free of charge of the result of this search and of the information in the database concerned, unless this would be contrary to public policy or public security. The provisions of the Data Protection Act 2000 remain unaffected.
(5) Section 28 (2) of the Data Protection Act 2000 - DSG 2000, Federal Law Gazette I No. 165/1999, as amended, shall not apply to information network systems of lending institutions registered with the data protection authority for credit assessment purposes, the use of which is based on Section 8 (1) (2) or (4) DSG 2000 (Bundesministerium für Digitalisierung und Wirtschaftsstandort[23] 2019).

§ 11a Insurance Contract Act 1958, Federal Law Gazette No. 2/1959

§ 11a. (1) The insurer may use personal health data in connection with insurance relationships in which the state of health of the insured person or of an injured party is considerable, provided that this is done

1. to assess whether and under what conditions an insurance contract is concluded or amended, or
2. for the administration of existing insurance contracts or
3. for the assessment and fulfilment of claims arising from an insurance contract

is indispensable. The prohibition of the determination of gene analytical data according to § 67 Genetic Engineering Act remains unaffected.

(2) Insurers may only determine personal health data for the purposes specified in para. 1 in the following manner:

1. by interviewing the person to be insured or already insured, or by interviewing the injured party, or

2. on the basis of the documents provided by the policyholder or the injured party, or

3. by information from third parties in the presence of an express consent of the person concerned granted for the individual case, or

4. for the assessment and fulfilment of claims arising from a specific insured event by information from examining or treating physicians, hospitals or other health care institutions (health service providers) on the diagnosis and type and duration of treatment, provided that the person concerned has expressly consented to the investigation in written form and in a separate declaration, which he can revoke at any time, after the insurer has drawn his attention to the possibility of individual consent (item 3) and has instructed him clearly and comprehensibly about the consequences of consent as well as the refusal of consent and about his right of revocation in the event of consent; such information may only be obtained after the data subject has been informed of the intended collection of information, including the disclosure of the specifically requested data and the purpose of the data determination, and has been clearly and comprehensibly informed of his right of objection and the consequences of the objection, and has not objected to the data determination within 14 days (receipt of the objection); or

5. by using other data lawfully made known to the insurer; this data must be communicated to the person concerned; he has the right of objection pursuant to § 28 Data Protection Act 2000 (Bundesministerium für Digitalisierung und Wirtschaftsstandort[24] 2019).

§ 107 Telecommunications Act 2003 (TKG 2003), BGBl. I No. 70/2003 as amended. Federal Law Gazette I No. 102/2011

Unsolicited messages

§ 107 (1) Calls - including the sending of faxes - for advertising purposes without the prior consent of the subscriber shall be prohibited. The consent of the subscriber is equal to the consent of a person authorised by the subscriber to use his connection. The given consent can be revoked at any time; the revocation of the consent has no influence on a contractual relationship with the addressee of the consent.

1a) In the case of telephone calls for advertising purposes, the caller's calling line identification may not be suppressed or falsified and the service provider may not be induced to suppress or falsify it.

2. The sending of electronic mail - including SMS - shall be prohibited without the prior consent of the recipient if the consignment is sent for the purpose of direct marketing, or is addressed to more than 50 recipients.

(3) Prior consent for the sending of electronic mail in accordance with paragraph 2 shall not be required where the sender has received the contact information for the message related to the sale or service to its customers, and this message is for direct marketing of own similar products or services, and the recipient has been given a clear and unequivocal opportunity to refuse such use of electronic contact information free of charge and without any problems when it is collected and additionally when it is transmitted; and the addressee has not refused the mailing from the outset, in particular by entry in the list referred to in Section 7(2) of the E-Commerce Act.
(4) [Remark: repealed by BGBl. I No. 133/2005]
5. The sending of electronic mail for direct marketing purposes shall in any case be prohibited if the identity of the sender on whose behalf the message is transmitted is disguised or concealed, or the provisions of Section 6 (1) of the E-Commerce Act are infringed, or the recipient is requested to visit websites which violate this provision, or there is no authentic address to which the recipient can send a request to stop such messages.
(6) If administrative offences pursuant to paragraphs 1, 2 or 5 have not been committed domestically, they shall be deemed to have been committed at the place where the unsolicited message reaches the subscriber's connection (Österreichische Datenschutzbehörde[1] 2019).

2.2. CZECH REPUBLIC

The Government of the Czech Republic on 15 March 2010 passed a resolution No. 205 to address cyber security issues and has established the Ministry of Interior of the Czech Republic as a coordinator of cyber security issues and the national authority for the area.

On 24 May 2010 the Czech Government adopted resolution No. 380, which established the Interdepartmental Coordination Council for the area of cyber security.

On 9 December 2010 Ministry of Interior of the Czech Republic with CZ.NIC signed memorandum, and established the National CSIRT.

Currently, the National CSIRT performs the role of "Point of Contact" for the information technology contributes to the solution of incidents relating to cyber security in the networks operated in the Czech Republic. Until the establishment of government CSIRTs also play the role of "Point of contact" for the network of public and state administration in the Czech Republic.

On 20 July 2011 The Czech Government passed a resolution No. 564 to approve Czech Cyber Security Strategy for the period of 2011 - 2015.

On 19 October 2011 the Czech Government adopted Resolution No. 781 which established the Authority as a coordinator for cyber security affairs as well as the national authority for the Cyber Security area.

On 13 May 2014 the National Security Authority of the Czech Republic opened National Cyber Security Centre in Brno.

On 13 August 2014 president of the Czech Republic signed **Cyber Security Law** of the Czech Republic. The law is effective since 1st January 2015.

8.12.2017 was accepted in the Czech Republic the Decree No 437/2017 Coll. on the criteria for the determination of an operator of essential service came into force. This Decree transposes the relevant legislation of the European Union and regulates sectoral and impact criteria for the determination of an operator of essential service and specifications for determining the importance of an impact of the disruption of an essential service on the security of social and economic activities according to Section 22a, paragraph 1 of the Act on Cyber Security.

On 19 December 2014 the regulations implementing the Act No 181/2014 Coll. on Cyber Security and change of related acts were published in the Collection of Laws:

- Decree No 316/2014 Coll. on Security Measures, Cyber Security Incidents and Reactive Measures ("Cyber Security Regulation").
- Decree No 317/2014 Coll. on Important Information Systems and their Determination Criteria.
- Governmental order No 315/2014 Coll. which amends the Governmental order No 432/2010 Coll. on the Criteria for the Identification of a Critical Infrastructure Element.

21.5.2018 The Decree No 82/2018 Coll. on Security Measures, Cybersecurity Incidents, Reactive Measures, Cybersecurity Reporting Requirements, and Data Disposal (the Cybersecurity Decree).This Decree incorporates the relevant European Union law and for a critical information infrastructure information system, a critical information infrastructure communication system, an important information system, an essential service information system, or for an information system or an electronic communications network used by a digital service provider (hereinafter referred to as the “information and communication system”) it establishes

a) the content and structure of security documentation
b) the content and scope of security measures
c) the types, categories and significance assessments of cybersecurity incidents
d) the requirements and method for reporting a cybersecurity incident
e) the details of notification of the implementation of a reactive measure and its outcome

f) a sample notification of contact details and its form;
g) the method of the disposal of data, operational data, information and copies thereof

2.3. PORTUGAL

In Portugal, the **legal data protection** framework is regulated by:

a) Constitution of the Portuguese Republic - article 35;
b) The **data protection act** (approved by Law 67/98 of 26th October) the legal framework that generally applies to both private and public sectors as well as to any sector activity;
c) The **ePrivacy act** (approved by law 46/2012 on 29th August) concerning the processing of personal data and privacy protection;
d) Law 32/2008 on 18 July which sets out the data retention obligations imposed on providers of publicly avaiable electronic communications services.

The **Constitution of the Portuguese Republic - article 35** stablish that all citizens have the right of access to any computerized data related to them and the right to be informed of the use for which the data is intended, therefore, under this law, they are entitled to require that the contents of the files and records be corrected and up to date. This law determines what personal data is, as well as the conditions applicable to automatic processing, connection, transmission and use and should guarantee its protection by means of an independent administrative body.

The **Data Protection Act (approved by Law 67/98 of 26 October)** aims to protect an individual's right to private life while processing personal data establishing the rights and associated procedures of natural persons (data subjects) and the rights, duties and liabilities of legal and natural persons when processing personal data. The Data Protection Act also sets out principles and obligations that data handlers must comply with when carrying out personal data processing. The general principle of this law stablish that the processing of personal data shall be carried out transparently and in strict for privacy and for other fundamental rights, freedoms and guarantees

The **ePrivacy** act should be applied to the processing of personal data in connection with the provision of public available electronic communications services in public communications networks, including public communications networks supporting data collection and identification devices, specifying and complementing the provisions of Law nº 67/98 of 26th October. Companies providing public available electronic communications services should establish internal procedures for responding to requests for access to user's personal data presented by the competent judicial authorities in compliance with the referred special legislation.

Under the ePrivacy Act, the delivery of unsolicited communications for direct marketing is subject to prior consent of the subscriber that is an individual or the user.

Regarding electronic communication sector, Portugal has approved Law 46/2012 of 29th August concerning the processing of personal data and the protection of privacy.

The **law 32/2008** of 18th July is related to the retention of data generated or processed in connection with the provision of public available electronic communications services or public communications networks.

This statutory instrument governs the retention and transmission of traffic and geographical data on both natural persons and legal entities and the related data necessary to identify the subscriber or registered user for the purpose of the investigation, detection and prosecution of serious crime by competent authorities.

Regarding the **cybersecurity** there is no general cybersecurity legislation in Portugal. However, there is legislation concerning the security of communication services and networks in the electronic communication sector.

Entities providing public available electronic communications services in public communications networks must comply with Law 5/2004 of 10th February (the electronic communications law) and the ePrivacy Law. Under these laws, in the event of a security or integrity breach, these providers should notify the regulator (the National Communications Authority or ANACOM), the CNPD and, in some circumstances, service subscribers and users.

The most important event in the context of cybersecurity in 2016 consisted of the approval of EU Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the EU on July 2016. This directive allows the extension to other entities of the obligation to implement security measures and to notify security breaches.

Recently it was launched by the Economy minister the initiative “Portugal i4.0” that will generate the conditions for the development of industry and national services in the digital era.

2.4. SPAIN

The legal framework for the protection of personal data in Spain is regulated by the Lisbon Treaty; Article 18(4) of the Spanish Constitution; the GDPR and the Protection of Personal Data Law 3/2018.

Sector-specific regulations may also contain data protection provisions, such as the E-Commerce Law 34/2002 (LSSI), the General Telecommunications Law 9/2014 (GTL), anti-money

laundering legislation or the regulations on biomedical research. However, they generally refer to the DP Regulations and, now that the GDPR is in force, will either be subject to review or should at least be reinterpreted according to GDPR rules.

Finally, we have we have the Cybersecurity Code that is a tool that brings together all the updated rules that directly affect cybersecurity.

3. ARE THERE INITIATIVES TO MAKE SOCIETY AWARE OF NATIONAL AND EUROPEAN REGULATIONS REGARDING WEB SECURITY AND PERSONAL DATA PROTECTION?

3.1. AUSTRIA

1. saferinternet.at

The initiative **Saferinternet.at** supports above all children, young people, parents and teachers in the safe, competent and responsible use of digital media.

Figure 3. Logo saferinternet.at

Source: saferinternet.at

The initiative is implemented by the European Union ("Connecting Europe" facility) as part of the CEF Telecom/Safer Internet programme.

Saferinternet.at forms the "Safer Internet Centre Austria" together with the Stopline (Reporting Office against Child Pornography and National Socialist Re-activation) and the "Rat auf Draht" (Telephone Help for Children, Young People and their Relatives). It is the Austrian partner in the EU's Safer Internet Network (Insafe) (saferinternet.at[1], 2019).

The target group of this initiative is diverse: from teachers to parents, young people, people in youth work and senior citizens.

Topics of this initiative are for example:

- cyberbullying
- Digital Games,
- data protection,
- information literacy,
- copyrights,
- self-expression and many more
  (saferinternet.at[1], 2019).

The Austrian Institute for Applied Telecommunications (ÖIAT) coordinates Saferinternet.at. The cooperation partner is the Association of Internet Service Providers Austria (ISPA).

The Austria-wide project is implemented in close cooperation with:

- the public sector,
- NGOs and
- of the economy
  (saferinternet.at[1], 2019).

The Austrian Institute for Applied Telecommunications (ÖIAT) coordinates the Saferinternet.at initiative. ÖIAT was founded in 1997 and is an independent, non-profit association. It supports companies, private individuals, NGOs and the public sector in the competent, safe and responsible handling of digital media. ÖIAT is a member of Austrian Cooperative Research (ACR), the umbrella organization of cooperative research institutions. Other well-known ÖIAT projects include the Internet Ombudsman, the Watchlist Internet and the Austrian E-Commerce Quality Mark (saferinternet.at[2], 2019).

2. IPSA – Internet Service Providers Austria

Figure 4. Logo IPSA Internet Sercie Providers Austria

Souce: ispa.at

The ISPA was founded in 1997 as an association and represents more than 200 members from all areas around the Internet as a voluntary lobby (IPSA, 2019).

ISPA - Internet Service Providers Austria - is the umbrella organisation of the Internet industry. Its aim is to create optimal economic and legal conditions for the development of the Internet. The ISPA regards the use of the Internet as a decisive cultural technique and accepts the resulting socio-political responsibility (IPSA, 2019).

The association provides their members with expertise and know-how - also in legal matters -, develop statements in working groups for example on relevant draft laws or templates for general terms and conditions or security concepts and offer their members free further education within the framework of the ISPA Academy. In addition, they inform their members about developments at national and European level and host events such as the ISPA Forum or the Internet Summit Austria (IPSA, 2019).

The association fulfils their socio-political responsibility, for example, with the Stopline founded by them (reporting office against child pornography and National Socialism on the Internet) or with free information material to promote online media competence, especially for children and young people. The ISPA has become an important contact point for all Internet matters due to its long-standing active role as the umbrella organisation of the Austrian Internet industry and its constant interaction with public authorities and relevant interlocutors (IPSA, 2019).

3. Digitalisierungsagentur (digitalization agency) – DIA

Figure 5. Logo Digitalisierungsagentur DIA

Source: linkedin.com - Digitalisierungsagentur

The Digitization Agency is the national and international contact for digitization issues and organizes a dialogue between business, society and administration on the various facets of digitization. It networks the relevant bodies, advises the Federal Government and thus generates important concerns and ideas in the comprehensive field of digitization (Österreichische Forschungsförderungsgesellschaft mbH[2], 2019).

The DIA is financed by two ministries (Federal Ministry for Digitization and Economic Location, Federal Ministry for Transport, Innovation and Technology) and established as a division of the Austrian Research Promotion Agency (Österreichische Forschungsförderungsgesellschaft[1] FFG).

The digitization agency operates in five fields (digital infrastructure, business, education and society, research, development and innovation as well as data protection and data management) and creates a platform for the coordination and coordination of different actors (Österreichische Forschungsförderungsgesellschaft mbH[2], 2019).

The Digitization Agency is to serve as a central platform for important digitization measures, in order to master the challenges of digital transformation in a targeted and joint manner.

The task: Making digitization a success story

The Federal Government's Digitization Agency is making concrete contributions to making digital change a success story for Austria:

- they implement specific projects.
- they provide expertise and know-how.
- they communicate the opportunities offered by digitization.
- they network and coordinate stakeholders and actors
- (Österreichische Forschungsförderungsgesellschaft mbH[1], 2019).

The target groups: Platform for communication and coordination

The Digitization Agency is available throughout Austria as a platform for knowledge and projects:

- They show what digitization really brings and thus also take away fears of change.
- They open up concrete new economic opportunities and projects for our SMEs.
- They advise the Federal Government and politicians on the right decisions for the future.
- You coordinate activities and projects in the following areas
  - digital infrastructure,
  - Economy,
  - Education and Society,
  - research, development and innovation, and
  - Data protection and data management.
- They are Austria's international contact for digitization

(Österreichische Forschungsförderungsgesellschaft mbH[1], 2019).

The goal: to bring Austria and its SMEs forward

Successful digitization and innovative strength are the foundations for growth and prosperity in the future. Our SMEs and their employees in particular benefit from this:

- Austria should be a leader in Europe in terms of innovative strength.
- Austria's SMEs should
  - increase their productivity,
  - reduce their costs,
  - generate new sales,
  - make their employees digitally fit and
  - be internationally successful
- The DIA wants to open up a positive awareness for the opportunities of the future so that they can make the most of them
- (Österreichische Forschungsförderungsgesellschaft mbH[1], 2019).

3.2. CZECH REPUBLIC

Cyber security standards have been created recently because sensitive information is now frequently stored on computers that are attached to the Internet. Also, many tasks that were once done by hand are carried out by computer; therefore, there is a need for Information Assurance and security. Cyber security is important in order to guard against identity theft. Businesses also have a need for cyber security because they need to protect their trade secrets, proprietary information, and personally identifiable information of their customers or employees. The government also has the need to secure its information. One of the most widely used security standards today is ISO/IEC 27002 which started in 1995. This standard consists of two basic parts. BS 7799 part 1 and BS 7799 part 2 both of which were created by British Standards Institute (BSI). Recently this standard has become ISO 27001. The National Institute of Standards and Technology (NIST) has released several special publications addressing cyber security. Two of these special papers are very relevant to cyber security: the 800-12 titled "Computer Security Handbook" and 800-14 titled "Generally Accepted Principles and Practices for Securing Information Technology".

3.3. PORTUGAL

In Portugal there are some initiatives regarding web security and personal data protection, promoted by different organizations that aims to support the security of the Portuguese population.

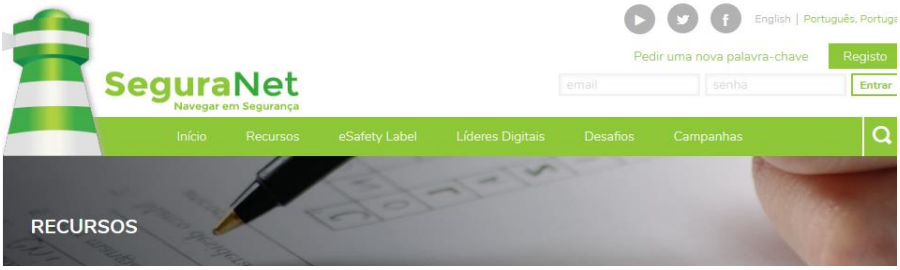
Some of these examples include:

- **Consortium "Centro Internet mais segura em Portugal".** This consortium includes several organizations (FCT - Fundação para a Ciência e a Tecnologia; DGE - Direção Geral da Educação; IPDJ - Instituto Português do Desporto e Juventude, I.P.; APAV - Associação Portuguesa de Apoio à Vítima; Fundação Portugal Telecom; and, Microsoft), has two lines (linha internet segura and linha aberta) and three websites (SeguraNet - Navegar em segurança; Better internet for kids and Inhope).

  – **Line "Linha internet segura".** APAV is responsible for the management and operationalization of this line. The main purpose of this telephone and online line is to help and respond to doubts and problems related to online security, cyberbullying, bullying and unworthy exposure for young people, adults, teachers and children. The full support is confidential and anonymous. More info in the website: www.internetsegura.pt/linha-internet-segura.
  – **Line "Linha aberta".** This telephone line is focused on illegal content (child porn, violence and racism) and criminal prosecution of those who publish this type of content. More info in the website: linhaalerta.internetsegura.pt.

- **Website "SegurançaNet - Navegar em segurança**": this online website is similar to a data base oriented for children, schools, young people, fathers and teachers and includes several information about web safety. The main topics covered in this platform are: digital citizenship; online shopping; cyberbullying; and, author rights. Here we can find: animations; games; information; applications; guides; activities; and, billboards. The main formats include presentations, audio, pdfs and videos. The digital security stamp (eSafety label) is an initiative developed by European Schoolnet launched in 2012. This service gives a certification and supports schools and aims to promote a secure environment related to digital technology as an experience of teaching and learning. Last, but not least, in this website we can find the initiative "Líderes digitais 2018-2019" that aims to motivate the students for the promotion of different subjects that leads to a more responsible utilization of technology, digital environment. More info in the website: www.seguranet.pt/index.php/pt.

Figure 6. SeguraNet – Navegar em Segurança



Source: www.seguranet.pt

- **Website "Ensina RTP":** this is an online website that has information (videos and short news) for multiple themes such as internet security. More info in the link: ensina.rtp.pt/dossie/seguranca-na-internet/.

- **Project "Net Segura e Viva":** this projects aims to offer a very useful repository (with information organized in Frequently Asked Questions) with advices from all areas related to cybersecurity. This project was created by Google and Deco Proteste in 2017. Besides being an online platform, Google and Deco Protest carried out multiple conferences "NETtalks" about cybersecurity in several Portugal cities. These conferences can be seen as spaces for information, knowledge, debate and reflection about themes related to the digital world, with a very dynamic and interactive format especially for young people. This national initiative also invites all the young people to produce some videos that shows the importance of participating in social media with safety and with respect for privacy. The videos produced by the students should promote secure internet utilization in a creative way especially in social media. The best videos became public in the online website. More info in the website: www.deco.proteste.pt/netvivaesegura/index.html.

Figure 7. Project "Net Segura e Viva"

Source: deco.proteste.pt

- **Project "Internet Segura":** regarding the "European Safe Internet Day" that happens every year, usually in February, two companies (Microsoft and GNR - Guarda Nacional Republicana) organize an event related to this topic with a lot of activities all over the country during one week. Last year, the campaign had the following subject "Create and share one responsibility: a better internet starts with you" that had with main target children and young adult, care takers, the senior population and educational agents. The topics from the last year covered some themes such as cyberbullying; identity robbery; inaccuracy of information sources; virus; and, internet addiction. In 2019, the "European Safe Internet Day" was celebrated in Madeira through the realization of a seminar with the theme "Online for human rights". This event was oriented for educational communities, for children and young people and all the different stakeholders of "Centro Internet Segura".

- **Project "Miúdos seguros na NET":** this was a project that helped families, schools and communities to promote online security for children and young people. The main

resources available are articles (between 2003 and 2008) and a blog. More info in the website: www.miudossegurosna.net.

Besides these initiatives, some companies promote the divulgation of information related to internet security in their own websites or blogs. In Portugal, there are also multiple books related to web safety.

3.4. SPAIN

The Spanish Data Protection Agency (AEPD in the Spanish acronym) is the public law authority overseeing compliance with the legal provisions on the protection of personal data, enjoying as such an absolute independence from the Public Administration.

The AEPD is of the understanding that its functions must always be conducted with a priority objective, that of guaranteeing the protection of individual rights.

Accordingly, it undertakes actions specifically aimed at enhancing citizens' capacity to effectively contribute to that protection. In particular, the following could be pointed out:

- Dissemination of its activities and of the right to the protection of personal data Information is a key element in fostering awareness among citizens of their right to the protection of personal data. Bearing this in mind and with the purpose of satisfying the increasing demand for information and extending its public dissemination actions, the AEPD has intensified its relations with the media, increasing its personnel and material means dedicated to dissemination
- Direct assistance in response to citizens' queries. From a qualitative standpoint, focusing on citizens' major doubts and concerns, the issues that are most frequently queried have to do with:
  - The scope of application of the system of guarantees of the LOPD (Organic Act on Data Protection);
  - Functions of the AEPD;
  - Queries on the exercise of rights, especially the rights of access and cancellation;
  - The obligation that entities collecting data have of informing citizens of their rights and where they may exercise them.
- Procedures to protect rights of individuals: of access, to rectify, to cancel and to object Citizens not only want to know what their rights are, they also want the effective exercise

of those rights to be guaranteed, either directly by the data controllers or by requesting the intervention of the AEPD

The Spanish Data Protection Agency made and continues to make a fundamental effort to facilitate the adequately implementation of the measures required by the GDPR. Among many other initiatives, it has brought forward a new Guide by creating an efficient and innovative tool to help organisations to comply with the requirements stipulated by the GDPR. They are available to citizens and public and private organisations and was developed for a wide range of different purposes: to help data controllers to carry out their work, comply with the duty to inform, prepare the contract between a controller and a processor, perform risk analysis and Privacy Impact Assessment (PIAs) and to implement relevant techniques to facilitate public authorities switching to the GDPR.

4. HAS A COMMISSION, ENTITY OR INSTITUTION BEEN CREATED RESPONSIBLE FOR ALL MATTERS RELATED TO THIS MATTER? MAKE A LIST OF THESE INSTITUTIONS.

4.1. AUSTRIA

The Austrian Data Protection Authority is the national supervisory authority for data protection in the Republic of Austria. The data protection authority (Datenschutzbehörde) ensures compliance with data protection in Austria.

Figure 8. Logo Datenschutzbehörde Österreich/Data Protection Authority Austria

Souce: dbs.gv.at

Austria was one of the first European countries with an authority for data protection, the Data Protection Commission. It was created with the first Data Protection Act, Federal Law Gazette No. 565/1978. With the EU Data Protection Directive 95/46/EC, data protection law throughout

Europe was placed on a new footing. In Austria, this Directive was implemented by the Data Protection Act 2000 (DSG 2000), Federal Law Gazette I No. 165/1999. After 25 May 2018, the Data Protection Basic Regulation (DSGVO) and the revised Data Protection Act (DSG) form the basis of data protection law (Österreichische Datenschutzbehörde[2] 2019).

The Data Protection Authority (formerly the Data Protection Commission) ensures compliance with data protection in Austria.

The data protection authority is a federal authority and a state organ of the Republic of Austria (§§ 35 ff DSG 2000). It is the independent data protection supervisory authority pursuant to Art. 8 para. 3 GRC and Art. 28 para. 1 Directive 95/46/EC (Österreichische Datenschutzbehörde[3] 2019).

The data protection authority is an authority which is not bound by instructions and which also independently organises internal tasks.

The tasks of the data protection authority according to DSG:

§ 21 (1-3) regulates the tasks of the data protection authority (DPO). What can be found here is essentially limited to advisory duties vis-à-vis the National Council, the Federal Council, the Federal Government, etc. pp. Then there are publication obligations.

1. The data protection authority advises the committees of the National Council and the Federal Council, the Federal Government and the Land governments on legislative and administrative measures at their request. The data protection authority must be consulted before federal laws are enacted or ordinances in the area of implementation of the Confederation that directly concern data protection issues are issued.
2. The data protection authority shall publish the lists pursuant to Art. 35 para. 4 and 5 DSGVO in the Federal Law Gazette by means of an ordinance.
3. The data protection authority shall publish the criteria to be established pursuant to Art. 57 para. 1 lit. p DSGVO by means of an ordinance. It also acts as the only national accreditation body pursuant to Art. 43 para. 1 lit. a DSGVO.

The task of the data protection authority under the DSGVO

In order to gain an insight into the comprehensive tasks of the data protection authority, one has to look up Art. 57 DSGVO. The following central tasks can be found here:
paragraph. 1 (selection):

Without prejudice to other tasks set out in this Regulation, each supervisory authority must

- the monitoring and enforcement of the DSGVO

- raise public awareness and awareness of the risks, rules, guarantees and rights associated with processing. Particular attention will be paid to specific measures for children;
- in accordance with the law of the Member State, advise the national parliament, the government and other institutions and bodies on legislative and administrative measures to protect the rights and freedoms of individuals with regard to processing;
- raise awareness among data controllers and processors of their obligations under this Regulation;
- provide, at the request of any data subject, information on the exercise of their rights under this Regulation and, where appropriate, cooperate to that end with supervisory authorities in other Member States;
- deal with complaints from a data subject or from a body, organization or association referred to in Article 80, investigate the subject of the complaint to an appropriate extent and inform the complainant within a reasonable time of the progress and outcome of the investigation, in particular where further investigation or coordination with another supervisory authority is necessary;
- cooperate with and assist other supervisory authorities, including by exchanging information, to ensure the uniform application and enforcement of this Regulation;
- conduct investigations into the application of this Regulation, including on the basis of information from another supervisory authority or authority;
- follow relevant developments insofar as they affect the protection of personal data, in particular the development of information and communication technology and business practices;
- lay down standard contractual clauses within the meaning of Article 28(8) and Article 46(2)(d);
- establish and maintain a list of processing types for which a data protection impact assessment is to be carried out in accordance with Article 35(4);
- advise on the processing operations referred to in Article 36(2);
- encourage the development of codes of conduct referred to in Article 40(1) and give opinions and approve them on those codes of conduct, which must offer sufficient guarantees within the meaning of Article 40(5);
- encourage the introduction of data protection certification mechanisms and of data protection seals and marks in accordance with Article 42(1) and approve certification criteria in accordance with Article 42(5);
- review regularly, where appropriate, the certifications granted under Article 42(7);
- ...

Sections 2-4 set out:

- Each supervisory authority shall facilitate the submission of complaints referred to in paragraph 1(f) by means of measures such as the provision of a complaint form, which may also be completed electronically, without excluding other means of communication.
- The performance of the tasks of each supervisory authority shall be free of charge to the data subject and, where appropriate, to the Data Protection Officer.
- In the case of requests which are manifestly unfounded or, in particular, excessive in frequency, the supervisory authority may charge a reasonable fee based on administrative costs or refuse to act on the request. In this case, the supervisory authority shall bear the burden of proving the manifestly unfounded or excessive nature of the request.

4.2. CZECH REPUBLIC

According to the Decision n. 781 of the Government of the Czech Republic from 19th October 2011, the National Security Authority was established as a competent national authority for the issues of cybernetic security.

According to the Law n. 205/2017, the National Cyber and Information Security Agency (NCISA, in Czech: NÚKIB) was established as a competent national authority for the issues of cyber and information security.

Main areas of activity of NCISA:

- operate the Government CERT (GovCERT.CZ)
- cooperation with other Czech CERT® teams and CSIRTs
- cooperation with international CERT® teams and CSIRTs
- drafting of security standards for different categories of entities in the Czech Republic
- support of education in the field of cyber security
- research and development in the area of cyber security

Government CERT (GovCERT.CZ) and other CSIRT teams play a key role in safeguarding the critical information infrastructure. Each country having its critical systems connected to the internet has to be able to effectively face security challenges, react on the incidents, coordinate actions to solve them and effectively prevent them. The task of these teams is to provide the security information and assistance to the state bodies, private entities and citizens. It plays a key role in enhancing the knowledge about internet security.

Czech Cyber Security Working Group was founded by AFCEA Czech chapter in 2018, officially started its activities in 2011. The mission of the working group is the identification and definition of joint, existing and developing open standards, rules, processes, principles, processes and techniques to achieve abilities for mutual cooperation of the public sector, business entities and the academia, in the area of cyber security and defence.

NATIONAL CENTER SAFER INTERNET conducted awareness and promote safer use of online technologies and training in this area. It uses its experience from the implementation of a number of national and international projects, the most important project was run by the Safer Internet Center and coordinated by NCBI from 2006 to 2018 with the support of the European Commission and other partners.

They are currently implementing a project eSafety Label +to support the safety of school IT environment, and finalizing the project DS4Y offering digital skills course for youth workers from disadvantaged groups.

4.3. PORTUGAL

In Portugal, there are four entities that promote web security and personal data protection:

- **CNPD:** the first one and the most well-known is CNPD that is an independent administrative entity with powers of authority which works with the Assembly of the Republic.

  The CNPD cooperates with the data protection supervisory authorities of other states, namely in the defence and exercise of the rights of the persons that live abroad.

  In addiction, the CNPD is the empowered body to supervise and monitor the compliance with the laws and regulations within the area of personal data protection with strict respect for human rights and freedom.

  The CNPD (its members or delegated staff) have powers to require personal information, both from public or private bodies, as well as to all documentation related to the processing and transmission of personal information.

Figure 9. Comissão Nacional de Proteção de Dados

Source: www.cnpd.pt

- **Center "CNCS - Centro Nacional de Cibersegurança Portugal":** CNSC promotes the utilization of the cyberspace in a free, reliable and secure way in order to promote a continuous improvement of national cybersecurity and international cooperation. This center acts like an operational coordinator and national authority specialized in cybersecurity together with other entities, national infrastructures, essential operators and digital services. CNSC wants to guarantee freedom, security and a justice cyberspace for everyone. In the short term this consortium gives some answers to prevent adverse events. In a medium/long term the goal is to develop good practices regarding cybersecurity. More info in: www.cncs.gov.pt.

Figure 10. Centro Nacional de Cibersegurança Portugal

Source: cncs.gov.pt

- **Center "Centro de Segurança Google":** since 2018 Google gave access to "Centro de Segurança Google" in order to protect their users from threats such as spam, malicious software or virus.

  This center gives useful information to help Portuguese people have a better control, security and privacy about the online navigation and with this initiative Google aims to give information about many subjects especially for families. With this center, parental control allows the limitation of screens, block websites or videos that can be considered inappropriate for children. The parents can also find information about how they can use some tools such as "Family link" and "YouTube Kids" that help them define some rules for digital utilization for the family and how to stay safe online. More info in the website: safety.google/security.

Figure 11. Centro de Segurança Google

Source: cncs.gov.pt

- **Association "APDPO Portugal - Associação dos Profissionais de Proteção e de Segurança de Dados":** this is a professional association that represents individuals and organizations that deals with protection and data security, privacy and electronic communication regulation or who hold the position of data protection officers in organizations operating in Portuguese territory.

4.4. SPAIN

Earlier initiatives related to the development of the Cyber Security contractual Public Private Partnership in 2016. These brought together the European Cybersecurity Industry, Member States' representatives, Regions and Research Community to drive the European Cybersecurity research agenda, support skills development, support industrial cybersecurity development, and align on certifications amongst many other topics. Today, ECSO brings together more than 241 organisations. In 2017 the European Commission launched the Cybersecurity Act, aiming towards continuing and enforcing ENISA as the European Cyber Security Agency and setting a certification mechanism for components, software, systems and services, which is currently being further debated. In 2018 both GDPR and the NIS Directive (Directive on security of network and information systems) were transposed into national law and came into effect throughout the Member States.

Recent initiatives from the European Commission were to support a strong cybersecurity in Europe, by developing a Network of National Coordination Centres, building on the development of National Competence Centres, the Competence Community and the European Centres of Excellence.

Ongoing are the development of the proposed Cybersecurity Act on the ENISA agency (today the European Union Agency for Network and Information Security) as the EU Cybersecurity Agency and on Information and Communication Technology cybersecurity certification. While these policy proposals are at the end of 2018 being debated amongst industry, European Member States and within the European Commission, it can be expected that they will have a major impact on Cybersecurity in manufacturing and industrial environment all together.

These include ongoing works in the domain of certification and standardization, specifically in the domain of improvements on cybersecurity and on the roles from government. Through the participation of Member States' representatives, governments can play a significant role in international standardization bodies such as ISO, IEC, CEN/CENELEC, and ETSI.

Reference was also made to publications by ENISA as a reference architecture in the concept of Security by Design, by Default, Security through Life, and Verifiable Secure in the Baseline

Security Recommendations for IoT and – published after the workshop – the Good Practices for Security of Internet of Things in the context of Smart Manufacturing.

Data protection and privacy are distinct rights under Spanish law, but both are deemed fundamental rights derived from respect for the dignity of human beings. They are primarily based on the free choice of individuals to decide whether to share with others (public authorities included) information that relates to them (personal data) or that belongs to their private and family life, home and communications (privacy). Both fundamental rights are recognised in the Lisbon Treaty (the Charter of Fundamental Rights of the European Union) and the Spanish Constitution of 1978. Data protection rules address, *inter alia*, security principles and concrete measures that are helpful to address some cybersecurity issues, in particular, because specific cybersecurity legislation (which not only covers personal data and private information but rather any information) is new and not sufficiently developed yet. Personal data and private data are not synonymous. Personal data are any kind of information (alphanumeric, graphic, photographic, acoustic, etc.) concerning an identified or identifiable natural person, irrespective of whether or not this information is private. However, data regarding ideology, trade union membership, religion, beliefs, racial origin, health or sex life as well as criminal and administrative offences are deemed more sensitive and require specific protection.

The National Security Council has included Cybersecurity as a priority for the National Security Strategy developed by the Ministry of Foreign Affairs and Cooperation. The National Security Policy is being developed through two key components: the National Cybersecurity Strategy, which aims to create an adequate capacity for prevention, defence, detection, response and recovery in the event of cyber-threats; and the National Cybersecurity Plan, which sets out the lines of action developed by the Strategy.

There is no legislation or policy in place in Spain that requires a public report on cyber security capacity for the government. There is no legislation in place in Spain that requires each agency to have a chief information officer or chief security officer. There is no legislation or policy in place in Spain that requires mandatory reporting of cyber security incidents. However, the strategy states that enforced incident reporting is a line of action that the Spanish government will pursue.

The agencies and bodies with competences on cybersecurity are numerous:

- The CCN, which is part of the National Intelligence Centre;
- The CCN Computer Emergency Response Team;
- The CNPIC;
- The Cybersecurity Coordinator's Office (which is part of the CNPIC);

- The Secretary of State for Telecommunications and Information Society; and
- INCIBE (previously known as the National Institute of Communication Technologies), which is the public sector company in charge of developing cybersecurity.

INCIBE (Spanish National Cybersecurity Institute) has a mission to strengthen digital confidence, improve cyber security and resilience and contribute to the digital market so that the safe use of cyberspace is encouraged in Spain. Its activities are based on three fundamental pillars: service delivery, research, and coordination. This entity in cooperation with the cybersecurity research ecosystem is promoting the creation of a network of centres of excellence on cybersecurity research and innovation. The initiative to launch grants for advanced cybersecurity research team excellence has emerged to meet the current need to retain and attract cybersecurity-research talent. INCIBE provides dedicated services for businesses, such as:

- Corporate security guidelines dossier.
- Dossier on the development of a corporate cyber security culture.
- Dossier on corporate web protection.
- Dossier on corporate information protection.
- Dossier on corporate contingency plan and business continuity.

INCIBE also provides complete and detailed awareness fostering programme for a broad range of companies. It includes lots of materials developed with training purposes, as well as a detailed manual to follow the necessary steps when applying the plan to a particular company case. Also, talks on different aspects of cybersecurity may be scheduled to supplement the documentation.

Under the direction of the Prime Minister, the Spanish national cyber security strategy is implemented by three bodies:

- The National Security Council as the Government Delegated Commission for National Security.
- The Specialised Cyber Security Committee, which will support the National Security Council by assisting the direction and coordination of the National Security Policy in cyber security matters and by fostering coordination, cooperation and collaboration among Public Authorities and between them and the private sector.
- *The Specialised Situation Committee which, with the support of the Situation Centre of the National Security Department, will manage cyber security crisis situations which, on account of their cross-cutting nature or extent, exceed the response capabilities of the usual mechanisms*

The spanish strategy is divided into six specific objectives:

OB 1 - for the Public Authorities, to ensure that the Information and Telecommunications Systems used by them have the appropriate level of security and resilience.

OB 2 - for companies and critical infrastructures, to foster the security and resilience of the networks and information systems used by the business sector in general and by operators of critical infrastructures in particular.

OB 3 - in the judicial and police field operations, to enhance prevention, detection, response, investigation and coordination capabilities vis-à-vis terrorist activities and crime in cyberspace.

OB 4 - in the field of sensitisation, to raise the awareness of citizens, professionals, companies and Spanish Public Authorities about the risks derived from cyberspace.

OB 5 - in capacity building, to gain and maintain the knowledge, skills, experience and technological capabilities Spain needs to underpin all its cyber security objectives.

OB 6 - with respect to international collaboration, to contribute to improving cyber security, supporting the development of a coordinated cyber security policy in the European Union and in international organisations, and to collaborate in the capacity building of States that so require through the development cooperation policy.

Spain has several national and regional computer emergency response teams (CERTs).

The National Centre for Critical Infrastructure Protection (CNPIC) acts as the national competent authority for network and information security in Spain (NIS).

CERTSI is the national accredited CSIRT for security and industry. This accredited CSIRT is in charge of coordinating response measures across Spanish networks

CCN-CERT is the national alert and reporting system for Public administration, company and organisation of strategic interest, such as those essential for Spanish security and economy

CSUC-CSIRT is one of the computer emergency response teams for the University of Catalanya

EsCERT is the second computer emergency response team for the regional academic network

RedIRIS is the third computer emergency response team for the Academia and Research network

CSIRT-CV is the security centre of the Valencian community

CCN-CERT Tools

Collaborative tool: REYES ('Kings' in Spanish) is a collaborative tool to exchange information about cyber threats. Access will be granted upon request to those organisations that are users of the Early Alert System of the Spanish CERT. It is based on MISP (Malware Information Sharing Platform) technology. There is also coordination with similar systems in other countries.

CCN-CERT Analysis tool: MARTA is the name of an advanced sandboxing platform devoted to the automated analysis of files which may have a malicious behaviour. It can be used by those organizations being part of the Early Alert System of the Spanish CERT. This tool analyses several kinds of files (.doc and .pdf among others).

CCN-CERT Analysis tool: MARIA is a detection tool developed for static analysis of harming code by means of multiple antivirus and antimalware engines for Windows and Linux platforms.

CCN-CERT Analysis tool: LUCIA is a tool developed aiming at the management of cyber incidents at the entities for which the national security schema is applied. This tool pursues to improve the communication between the governmental CERT and the organisms and organisations it collaborates with.

Both AENOR and AEI Ciberseguridad provide a trust seal. The AENOR seal validates good practices for e-commerce companies, while the “AEI Ciberseguridad” is a certification framework to check that a company is compliant with security requirements. Any company owning this certificate has passed a test to prove that they have in place the necessary physical and logical measures to protect their assets against several threats that could be damaging. This certification schema has a training programme associated.

The ISMS Forum is a company cluster established as a non-profit in 2007 to promote the development of information security in Spain and benefit the whole community involved in the sector. It is a specialised discussion forum for companies and public/private organisations to collaborate share and get to know the latest innovations concerning information security. Upwards of 150 companies and 850 independent professionals are part of it. The Forum also provides training courses at affordable prices. Currently they offer two different courses: one on GDPR and another one on certified data protection.

- Participation of EMPACT projects in coordination with EUROPOL. Operative actions fostering the collaboration with the private sector and awarenss raising.
- Participation in CyberEurope, the pan-European cyber exercise organised by ENISA.
- Participation in CyberEx, international cybersecurity exercise in cooperation with the Organisation of American States.

- Participation in the European Cyber Security Challenge, organised by the European Commission and ENISA, with INCIBE and other 9 members in the Organisation Committee. Spain ranked first in the competition.

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities. The GDPR creates the concept of "lead supervisory authority". Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority".

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory.

The DPA (Data Protection Authority) is the entity in charge of supervising compliance with the data protection duties imposed by the GDPR and DP Regulations (fair information, legitimate ground, security, notification, proportionality and quality, etc.). The DPA has carried out ex officio audits of specific sectors (including online recruitment procedures, TV games and contests, hotels, department stores, distance banking, hospitals, schools, webcams and mobile apps). However, the DPA's activity in terms of individual compliance investigations has significantly increased over the past 10 years, as has the number of fines imposed. Indeed, failure to comply with the GDPR and DP Regulations may result in the imposition of administrative fines depending on the severity of the offence (and regardless of whether civil or criminal offences are also committed, if applicable). Neither harm nor injury is required (i.e., the infringement itself suffices for the offender to be deemed liable), but the lack of any harm or injury is considered an attenuating circumstance to grade the amount of the administrative fine. However, harm or injury will be required to claim damages arising from breaches of data protection rights before civil and criminal courts.

The Spanish competent national supervisory authority is the Agencia Española de Protección de Datos (“AEPD”), which also represents Spain on the European Data Protection Board.

The AEPD is a public law authority enjoying "absolute independence from the Public Administration". It is responsible for:

- Information awareness about its activities and the right to protection of personal data (including 450 interviews and 850 "impacts" on media).
- Direct assistance in response to citizen queries (47,741 in 2007).

- Procedures to protect rights of individuals to access, rectify, cancel, and object. Most common are processes to cancel (62%) and access (32%).
- Registry of filing systems (1,017,266 total entries).
- Inspection and sanction procedures (399 sanction procedures resolved with €19.6 million in fines).
- Advocacy leading to Royal Decree 1720/2007.
- Cooperation with international agencies and those of the autonomous communities of Catalonia, the Basque Country, and Madrid.
- Evaluation of emerging risks, including personal data on the Internet, generalisation of video surveillance systems, employer monitoring of labor by video surveillance, biometrics, and Internet usage, and intensification of international data flows.

In response to the latter point, the AEPD advocated:

- Developing procedures allowing copyright protection in a manner compatible with the fundamental right to data protection.
- Regulating the anonymized publication of judgements passed by Courts of Law.
- Regulating internal whistleblowing systems available to workers within companies, outlining the activities in which it may be necessary to establish these systems and guaranteeing the confidentiality of those reporting and the rights of those being reported on.
- Development of specific public policy plans for the protection of minors on the Internet.
- Increased caution in order to prevent the undesirable exchange of sensitive personal data on the Internet via P2P networks.
- Fostering of self-regulation among the media to guarantee privacy and the protection of personal data, by encouraging more respect for the usage in relation to the data protection provisions.
- Citizen guideline actions regarding the use of guarantees of confidentiality for the recipients of emails.
- Plan for the Fostering of Good Practices in terms of guaranteeing privacy in Official Gazettes and Journals, by adopting measures that, without affecting their purpose, will limit the gathering of personal information by Internet search engines.
- Local Strategy aimed at conforming the installation of traffic control cameras to the provisions on the protection of personal data.

Protecting personal data is achieved by allocating specific duties to both 'controllers' (i.e., those who decide on the data processing purposes and means) and 'processors' (i.e., those who process the data only on behalf of a controller to render a service).

5. ARE THERE STUDIES CONDUCTED BY ANY PUBLIC ENTITY IN YOUR COUNTRY RELATED TO THE DEGREE OF ACCEPTANCE OR KNOWLEDGE OF THE REGULATIONS BY SOCIETY?

5.1. AUSTRIA

In Austria until today no study was carried out in which the acceptance of the GDPR was tested. In relation to the knowledge about the regulations, derivations can be drawn from the digitization study 2018.

The study initiated by the professional association UBIT of the Austrian Federal Economic Chamber on the state of digital transformation of Austrian SMEs with strong participation of the Austrian Federal Economic Chambers, Hutchison Drei Austria and the Institute for SME Management of the Vienna University of Economics and Business Administration was carried out by Arthur D. Little Austria for the second time (Little, 2018).

Top Topic 2018: DSGVO (GDPR) has created awareness for data backup

For 54 percent of the SMEs surveyed, the greatest challenge in 2018 was and is the new European Data Protection Basic Regulation (DSGVO), which came into force at the end of May 2018. For comparison: In the 2017 study, the DSGVO was not yet an issue as a challenge. The study also impressively shows that with the introduction of the DSGVO, awareness of responsible data handling and its security has moved to the top of corporate awareness. In 2017, only 32 percent stated that they were affected by the DSGVO; this figure rose to 83 percent in 2018. Data protection is a top priority for 40 percent of companies compared to their own websites (39 percent) and Internet banking (34 percent). 53 percent of the companies state that they store their data in their own business premises, another 21 percent attach importance to data storage in Austria and 17 percent want data storage in Europe. However, the study also shows that there is still great uncertainty regarding the DSGVO; many companies (43 percent in 2018 versus 34 percent in 2017) need advice and expect the legal framework to improve (Little, 2018).

Figure 12. Companies affected by the GDPR 2017

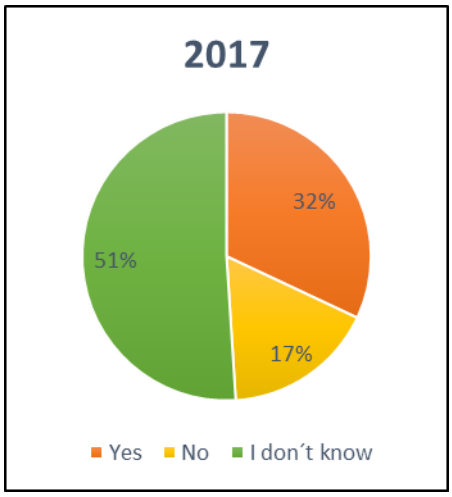
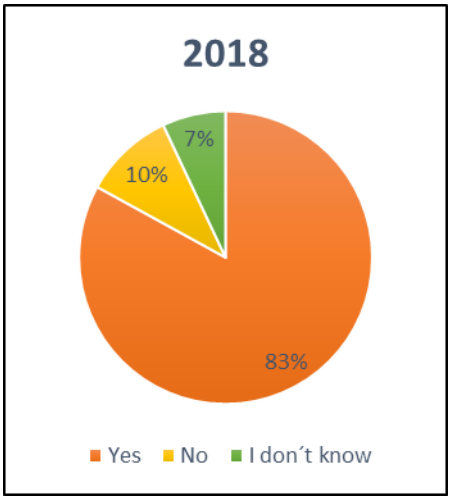


Figure 13. Companies affected by the GDPR 2018



Source: Little, 2018

5.2. CZECH REPUBLIC

The Cyber Security Glossary has been presented during the international Cyber Security and Defence conference - ITTE 2011.

In occasion of the international conference TechNet Europe & ITTE 2012, AFCEA Czech Chapter and Police Academy of the Czech Republic published first official Czech Dictionary on Cyber Security under ISBN 978-80-7251-378-9. This issue was published under patronage of National Security Authority of the Czech Republic and new National Centre for Cyber Security. In July 2012 the first electronical PDF version was published under ISBN 978-80-7251-377-2.

In 2014 the Czech Republic implemented new Cyber Security Law. As a reaction to new legislation in year 2015 the original publication was extended and updated in cooperation with AFCEA Czech Chapter and Police Academy of the Czech Republic in Prague published third edition under ISBN 978-80-7251-436-6.

5.3. PORTUGAL

The studies are very scarce when it comes to the degree of acceptance or knowledge of the regulations by society carried out by CNPD and ANDPO.

In 2018, the CNPD warned that Portuguese people provide personal information in the internet in a very “negligent and naive” way as well as companies and public entities. Due to this fact, it

is very easy to steal someone identity because the majority of people give to much personal information in the internet.

Also in 2018, the president of ANDPO said that the supply and the demand for DPO was very misfit for the market and the overall society and companies weren't prepared enough for the application of the new regulation. The same source also said that the CNPD will probably need to expand their response capacity, in terms of human and material resources, to be able to answer all the solicitations that will came with the application of GDPR. This situation was also confirmed by Filipa Calvão (president of CNPD) later in the same year when she said that the human resources structure in CNPD didn't allowed the necessary supervision regarding the application and execution of the new rules of data protection.

However, the private institutions are the ones who do more studies regarding the web security, personal data and GDPR.

5.4. SPAIN

The Spanish Data Protection Agency (AEPD), with the support of the Small and Medium Enterprise Confederation (CEPYME) have launched a survey aimed at to obtain information related to the resources they manage to keep data protection and privacy levels requiered.

The purpose of this section is to determine, whether in the SMEs there is or there is not a knowledge about the Regulation and the new obligations concerning the privacy and security aerea.

In this sense, the extension of knowledge of current regulations is moderate.

- The knowledge of the Regulation (RGDP) reaches to a 63% of SMEs.
- The obligation to prepare the register of activities consists of 60%.
- The new obligations of the controller are known for 59% of SMEs

On the other hand, it is important to consider the extension of this knowledge to the main resources provided by the AEPD for the implementation of the new Regulation, The AEPD guides are known by 47% of SMEs.

In general, the perception of the data protection in SMEs, it's positive. The survey verifies that the impact produced by the regulations and, especially the recent changes, determine:

- About 8 out of 10 SMEs perceive the data protection regulations as positive.

- Almost 9 out of 10 consider that the Regulation is better that the previous regulation in data protection.

An overview about data and data protection implemented by SMEs, the survey shows:

- 90% of SMEs are confident that "data must be protected It's always something that affects us. " -
- 62% disagree with the sentence "personal data do not have any value to my business." - and
- 47% are also not of agreement with the proposal "data protection does not justify costs".

SMEs therefore share a positive view of the data protection. However, it is noteworthy that distance between the general consideration of data protection and tata as a valuable asset of a business, an aspect that is not detected by companies, and which does not reinforce the impulse of protection. Thus, SMEs attitude regarding data protection revolves arround 3 aspects:

- To hire an external advisory service, it show an 85% disposition of the companies.
- Be better informed about the new Regulation, with a 79% positive attitude.
- To manage the obligations of the regulations with own resources and the support of the AEPD. For this action they choose 60% of SMEs.

6. DO YOU CONSIDER THAT THE GOVERNMENT OF YOUR COUNTRY HAS CARRIED OUT ANY DISSEMINATION ACTIVITY WORTHY OF MENTION OR ANY ACTIVITY THAT YOU THINK MAY BE APPLIED IN OTHER COUNTRIES?

6.1. AUSTRIA

The data protection authority offers a quarterly newsletter, which is sent to those who have registered for it or can be downloaded from the website of the data protection authority.

The newsletter deals with a wide range of topics and perspectives on data protection as well as related topics and subject areas. In the last newsletter the following topics were dealt with:

- 100 days DSGVO (GDPR) from view of the data protection authority
- First experiences with Data Breach Notifications

- Selected decisions of the DSB (Datenschutzbehörde - Data Protection Authority)
  - Notification of affected persons in the course of a security breach
  - No right to delete contributions from discussion forums of an online newspaper article
  - No voluntary consent to the use of a "GPS tracker" in company vehicles
  - DSGVO-compliant, pre-formulated declarations of consent

- Selected decisions of the courts
  - Judgment of the ECJ of 10.07.2018, C-25/17, Jehovah's Witnesses

- Legal expertise - Opinion
- News

In this way, legal issues, innovations as well as the relation to the everyday life of the inhabitants of Austria are created and pointed out in the newsletter (Österreichische Datenschutzbehörde[4], 2019).

6.2. CZECH REPUBLIC

Czech Cyber Security Working Group was founded by AFCEA Czech chapter in 2018, officially started its activities in 2011. The mission of the working group is the identification and definition of joint, existing and developing open standards, rules, processes, principles, processes and techniques to achieve abilities for mutual cooperation of the public sector, business entities and the academia, in the area of cyber security and defence.

Objectives of the working group

- General awareness in the area of cyber security and defence.
- Mutual, broad cooperation among non-profit organizations, public sector, businesses and the academia.
- Broad cooperation with foreign entities active in the same area
- Enforcement of security standards and the standards of interoperability for the monitoring and communication systems (CSIRT).
- Enforcement and support of the legislative establishment of security standards.
- Definition of the security experts' profile to be requested from the universities and other educational institutions.

- Preparation of the scenarios of critical situations and provision of modelling and simulation systems.
- Regular organization of instructive seminars both for the lay as well as the expert community.
- Obtaining financial grants from the EU and NATO to support cyber security awareness, training, education and to support professional activities in cyber security area.

Basic tenets of the working group

- Terminology definition, definition of cyber security and cyber defence.
- Standardization and legislative support.
- Support of education.
- Training and simulation.
- General awareness.
- International cooperation.

6.3. PORTUGAL

Although there are some activities related to web security and data protection the Portuguese government don't have an active role when it comes to promote dissemination activities. If anyone as a problem related to data protection or web security they have to search for a solution online, contact a lawyer or a person that has more knowledge related to these subjects.

However, some activities are promoted by public and private institutions and can be applied in other European countries such as:

- **Consortium "Centro Internet mais segura em Portugal":** this initiative is a very good example that can be applied to other countries because people, in this case young people, adults, teachers and children, can find online or by telephone some answers and support to deal with some doubts and problems related to many subjects (online security, cyberbullying, bullying, child porn, violence and racism and unworthy exposure). It is also important to highlight that the support carried out by this center is confidential and anonymous.

- **Platform "SeguraNet - Navegar em segurança":** this imitative is also a good example that can be adapted to other countries because this is an online platform that uses attractive content to promote web safety for children, schools, young people, fathers and

teachers. The main content that exists in this platform include: animations; games; cartoons; applications; quizzes; and; YouTube videos. Nowadays almost everyone uses the internet in a daily basis and the existence of attractive content is crucial.

- **Program "Comunicar em Segurança":** this is a program that goes to elementary and middle schools to promote the correct utilization through games, a web series, videos and animations. This program also had a roadshow in many Portuguese schools.

- **Website "Ensina RTP":** this is an online website that has short videos and news for multiple themes such as internet security.

- **Project "Net Segura e Viva":** this project promotes a contest for young children to produce some videos that shows the importance of participating in social media with safety and with respect for privacy.

- **Project "Internet segura":** this project organizes lots of activities in physical events all over the country during one week regarding the celebration of "European Safe Internet Day".

To conclude, we suggest including more interactive, attractive and digital activities, particularly for younger generations. Also, all the information must be easy, simple and clear to all people because all the content available for web security and data protection are very often not accessible and sometimes confuse.

In this context, we recommend to use games, quizzes, animations, animated cartoons and short videos (with duration between 2-5 minutes).

We also think that is necessary that all private and public schools promotes in classes (for example once a week or once a month) the discussion of subjects related to web safety with some orientation by a experiment teacher for example.

6.4. SPAIN

THE CURRENT NATIONAL AND INTERNATIONAL SCENARIO IS DOMINATED BY DEVELOPMENTS IN INFORMATION AND COMMUNICATION TECHNOLOGIES (ICT) AND BY RISKS EMERGING FROM THEIR USE. THE ADMINISTRATION IS FULLY AWARE OF THIS SCENARIO AND IT IS NECESSARY FOR THIS BODY TO DEVELOP, ACQUIRE, CONSERVE AND SECURE USE OF ICTS TO GUARANTEE THAT ITS SERVICES RUN EFFECTIVELY FOR THE CITIZEN'S AND THE COUNTRY'S BEST INTERESTS

Effective cooperation between all three levels of the Spanish Government (local, regional and central) will make it possible to take action linked to business innovation that can be perceived by citizens and companies, such as a network where skills are enhanced. Cooperation agreements will be formalized with the main regional bodies devoted to innovation in order to promote the dissemination, valuation and transfer of technologies developed by the companies in each Spanish Region and to stimulate the participation of organizations in technological cooperation programs at both national and international level.

Spain has become the first country in the European Union to have a single framework for the notification and management of cyber-security incidents.

The Spanish National Cyber-security Incident Notification and Management Guide approved by the National Cyber-security Council is a technical document that creates a benchmark in terms of notifying and managing cyber-security incidents within Spanish territory. They are addressed both to the public and private sectors and they standardise the criteria in this field.

The Guide establishes a "one-stop" notification mechanism, that implies the incidents shall be reported only to the relevant institution (CSIRT): National Cryptologic Centre of the National Intelligence Centre (CCN-CERT) when it comes to the Public Sector and the National Cybersecurity Institute for the Private Sector (INCIBE-CERT).

The Guide comprises a classification system for the incidents, which are sorted into ten different categories: abusive content (e.g. Spam), harmful content (e.g. Malware), information gathering (e.g. Network traffic monitoring), intrusion attempt (e.g. Access to credentials), intrusion (e.g. Compromised applications), availability (e.g. DDoS), compromised information (e.g. lost data), fraud (e.g. Phishing), vulnerable (e.g. Weak cryptography) and other.

Each incident will be associated to a particular level of danger, which will be defined relying on the risk that the incident would involve for the affected organisations' systems if it was materialised. There are five levels of danger, namely: critical, very high, high, average and low. Additionally, the Guide sets up an impact indicator in order to assess the consequences post-incident for the organisation or company activities and systems. Depending on this indicator, the impact will be critical, very high, high, average, low. There is an extra category called "no impact", where no damage at all has been caused as a result of the incident.

As for the cyber-security incidents management, the Guide establishes a six-steps process to prevent these incidents and properly tackle them in case they take place. The phases are described as follows: preparation (e.g. updated policies), identification (e.g. network monitoring), containment (e.g. information assessment and classification), mitigation (e.g. recovery of the latest backup copy), recovery (e.g. restore the activities) and post-incident actions (identification and analysis of the origin of the incident and the costs).

Spanish approach to cybersecurity

Guaranteeing and implementing security in cyberspace, while respecting privacy and freedom, has become one of the strategic priorities of the most developed countries, due to its direct impact on national security, on the competitiveness of companies, and on the prosperity of society as a whole. The cyber world demands a constant commitment to technological evolution and the increasing sophistication of attacks.

Adapting to this scenario involves improving prevention and surveillance capabilities and designing increasingly effective responses to attacks. It also requires a greater degree of coordination and cooperation. On the one hand, at the national level, between all levels of the State Administration and private companies and entities; on the other, at the international level, with countries and multilateral organizations.

The National Cryptologic Center has made an approach to the development, implementation and improvement of a general scheme of National Cybersecurity, which will facilitate this task. Based on the development carried out in Spain in the last 20 years, and with the specific case of CCN-CERT, the aim is to provide a development model to face, at a national level, the different challenges arising from the protection of a country's network and, by extension, of its Administration, companies and citizens.

7. CONCLUSIONS

7.1. AUSTRIA

A critical analysis will be developed focusing on the following issues:

- To what extent have legislation systems been adapted to the changing needs of the web security?
- Barriers faced by each country in the field of legislation and web security
- Comparative analysis with partner countries.

As mentioned in the previous chapters, there are some complementary legal guidelines that complement the GDPR at the national level. 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.

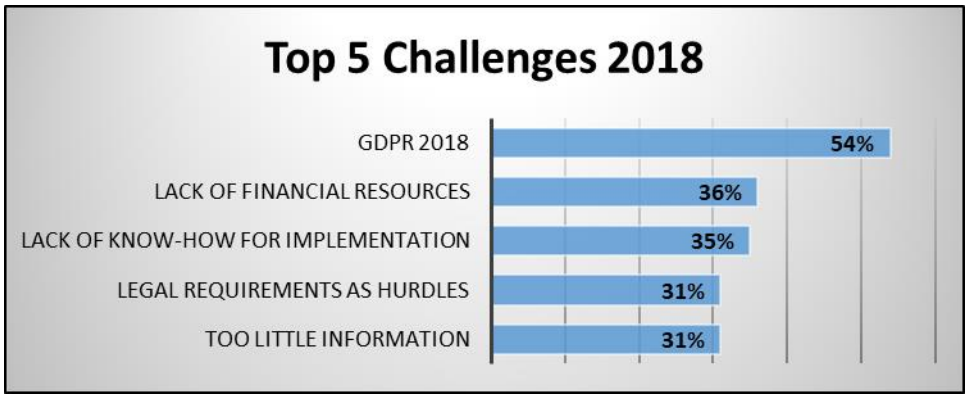
The digitalization study 2018 has captured digital development in SMEs and identified the key issues:

- 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

Figure 14. 5 Major Challenges of Digital Transformation 2017

Source: Little, 2018

Figure 15. 5 Major Challenges of Digital Transformation 2018



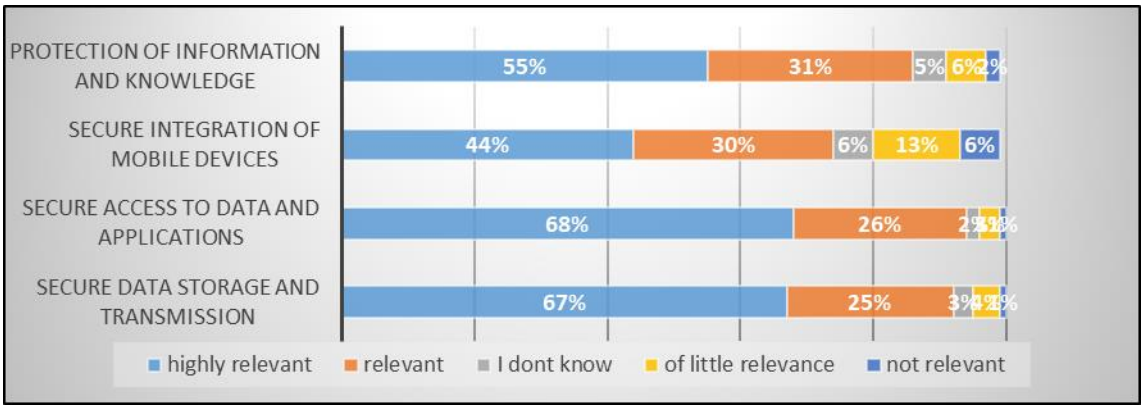
Source: Little, 2018

The issue of data protection has brought digitalization for SMEs into the focus of consideration and gives them increased cause for action.

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

3. New indices have identified industry dynamics, proactivity and financial resources as key drivers to meet these challenges.
4. The results of the 2018 Digitization Study show that SMEs actually need support: Funding for digital transformation and accompanying implementation consulting (Little, 2018).

Figure 16. Relevance to Information security and data protection



Source: Little, 2018

The outlook for 2019:

- The increasing change in internal processes in the course of digitization is creating a need for advice on implementation and financing among the SMEs surveyed.
- Statutory measures such as the GSPR are creating a desire among SMEs for a better legal framework.

On the basis of the information that was given in this report it can be recognized that there are many regulations in Austria beside the GDPR. 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.

7.2. CZECH REPUBLIC

A critical analysis will be developed focusing on the following issues:

- **To what extent have legislation systems been adapted to the changing needs of the web security?**

- **Barriers faced by each country in the field of legislation and web security**
- **Comparative analysis with partner countries.**

Current status:

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. It also supports the NSA CZ, which is a body responsible for the cybernetic security on the issues demanding co-operation with other state bodies and operators of critical information infrastructures.

Principles:

- Protection of fundamental human rights and freedoms and of the democratic rule of law principles.
- Comprehensive approach to cyber security based on principles of subsidiarity and cooperation.
- Trust building and co-operation among public and private sector, and civil society.
- Cyber security capacity building.

Main goals:

- Efficiency and enhancement of all relevant structures, processes, and of cooperation in ensuring cyber security.
- Active international cooperation.
- Protection of national CII and IIS.
- Cooperation with private sector.
- Research and development / Consumer trust.
- Education, awareness raising and information society development.
- Support to the Czech Police capabilities for cybercrime investigation and prosecution.
- Cyber security legislation (development of legislative framework). Participation in creation and implementation of European and international regulations.

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:

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

Generally we can say that the information about web security and their legislation are not well structured and are hardly available. In the Czech Republic this topic is considered as a very important and the several public and private institutions realized many activities, projects and surveys on that issue. 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.[1]

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

According to the study "Benchmarking of Safer Internet policies in Member States and policy indicators" we note 3 groups of countries:

- Group 1: high involvement of both the public and non-public sector (Austria, the Czech Republic, Finland, Luxembourg, Portugal, Slovenia, Sweden, and the UK);
- Group 2: Medium involvement of both the public and non-public sector (Bulgaria, Cyprus, Denmark, Estonia, Greece, Hungary, Iceland, Ireland, Latvia, the Netherlands, Norway, Spain, and Romania);
- There are also two countries that do not fit inside this correlation; Slovakia which sees high involvement of the non-public sector despite lower public sector involvement, and Italy, which sees very high public involvement but a lower nonpublic involvement by comparison.

7.3. PORTUGAL

- **To what extent have legislation systems been adapted to the changing needs of the web security?**
- **Comparative analysis with partner countries**

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.

[1] Benchmarking of Safer Internet policies in Member States and policy indicators

When in comes to companies, the information available confirms that Portuguese companies aren't still fully aware of what to do when it comes to the application of the GDPR. Even though, the 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.

As regards to web security the situation is similar. 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 same study reveals that Portugal is the third country in the EU that complains the most about this matter. 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.

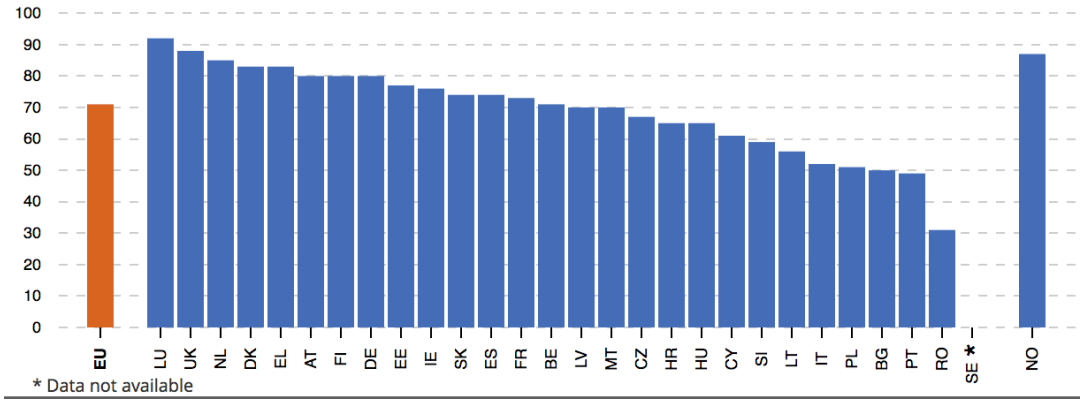
Another study carried out by "msn content portal" in 2012, indicates that 78% of Portuguese internet users surveyed have some basic online protection but they are poorly informed about what they should do to protect themselves against cybercrime threats based on fraud, such as phishing, identity theft 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.

Among people in the EU who has used the internet in the year priori to the 2016, 71% had provided some kind of personal information online. The most common types were contact details (61% of internet users) followed by personal details such as name, date of birth or identity card number (52%) and payment details, such as credit/debit card or bank account number (40%). About 22% had provided other personal information such as photos, their location or information related to their health, employment or income.

Disparities between the EU member states can also be observed in the way internet users managed access to their personal information in the internet in 2016. More than one quarter of EU-28 internet users didn't provide personal information over the internet, a share that ranged from just 8% in Luxembourg to half or more in Bulgaria, Portugal and Romania (see figure 17).

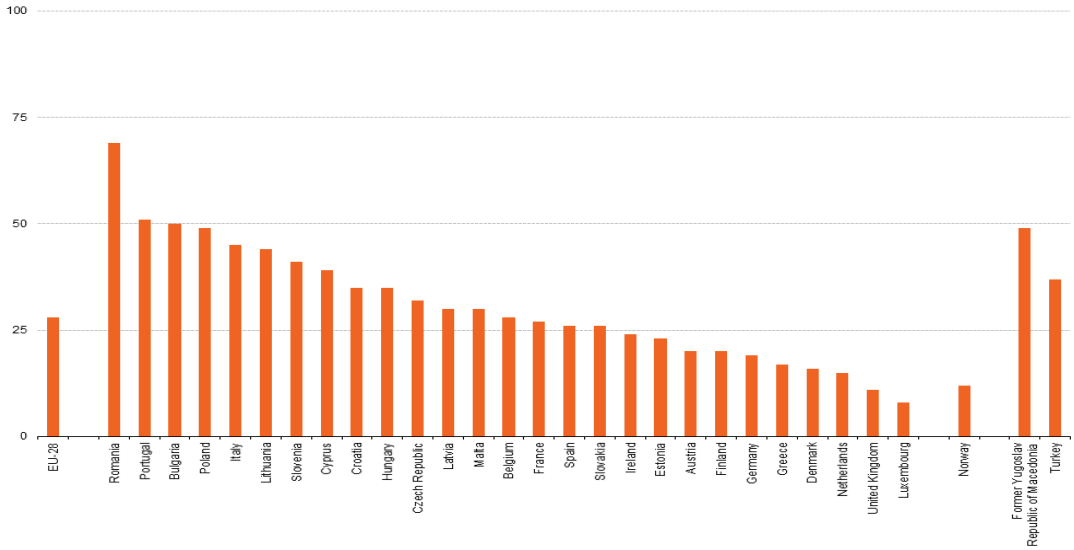
As you can see in figure 7, Portugal is one of the countries that shares less personal information over the internet. Younger generations seem to be more willing to provide personal information online (almost 80% of internet users aged 16 to 24 years had shared some kind of personal information online) compared with 57% of users aged 65 to 74 years.

Figure 17. People who provided any personal information online (2016)
(as % of internet users aged 16-74 years)



Source: Eurostat

Figure 11. Individuals who did not provide any personal information (2016)



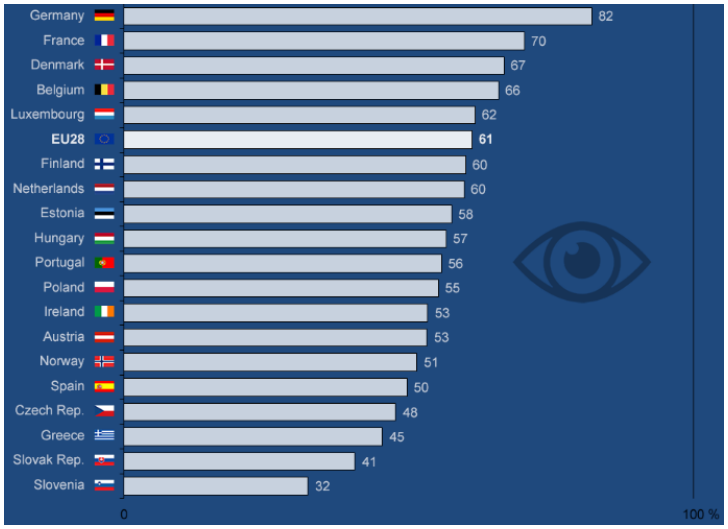
Source: Eurostat. Notes: Sweden not available

Also in figure 8, we can see that in the Portuguese case, a number of different actions are being applied by internet users, separately or together, to control access to personal information in the internet. The main actions undertaken by the Portuguese population to manage access to personal information demonstrate that 44% read privacy policy statements, 48% restricted access to geographical location, 57% limited access to profile/content on social networks and 52% refuse to allow the use of personal information for advertising.

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. In addition, although the majority of the Portuguese people are reluctant to give personal information, in a study developed by consultant Nielsen, in 2015, 44% of the Portuguese are

willing to give personal data to receive customized offers in their telephone when they are going shopping. This can also be confirmed in the next figure where we can see that Portuguese people don't have many concerns about online activities being recorded to provide tailored advertising.

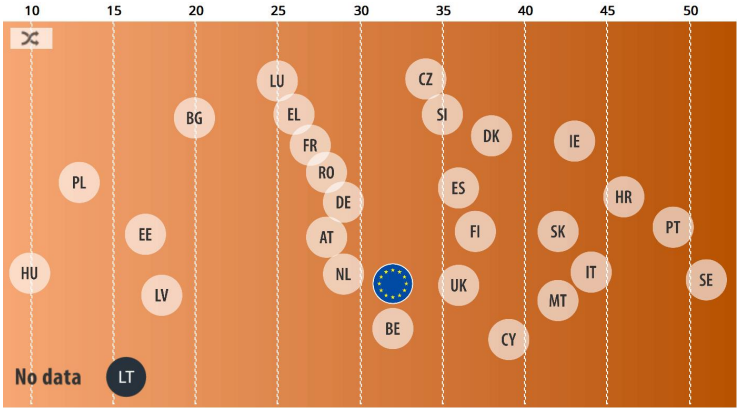
Figure 12. Concerns about online privacy



Source: Report "OECD Digital Economy Outlook 2017"

When it comes to enterprises, 3 in 10 SMEs in the EU have an ICT security policy and practically all businesses in the EU (98%) use computers and among those, only 32% have a formally defined ICT security policy. In Portugal, 49% of Portuguese companies have an ICT Information Management Policy (see figure 20).

Figure 20. Business with an ICT security policy (2015)
(as % of all businesses using a computer)



Source: Eurostat

The knowledge of cookies in Portugal is also a problem (see table 1). 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.

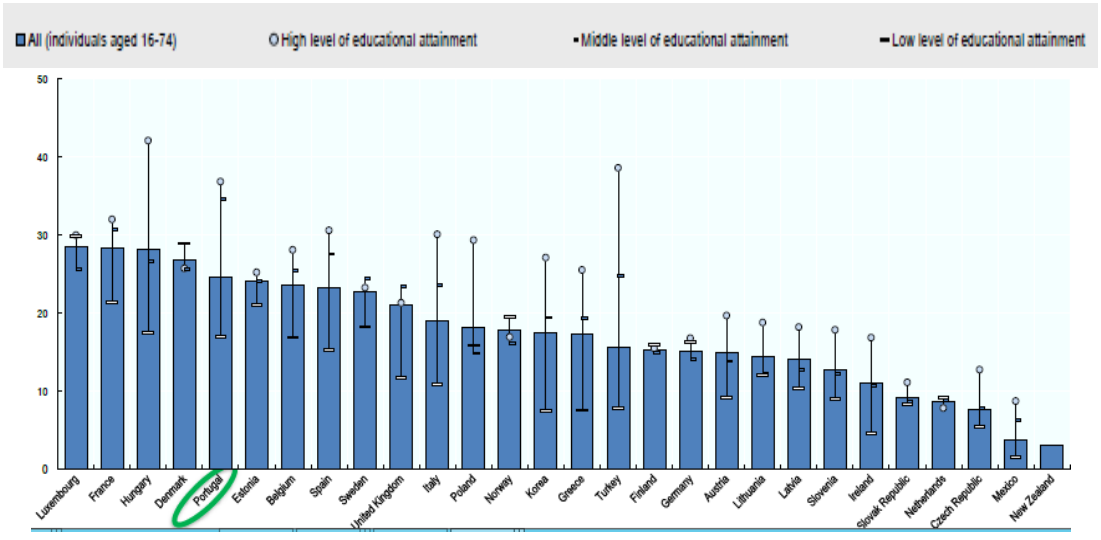
Table 1. Cookies in Portugal (2016)

	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 figure 11, we can see that Portugal is one of the countries that experienced more digital security incidents in 2015 or later. Receiving fraudulent emails to ask for money or personal data (including bank information) is the main cybercrime that the Portuguese complain about and 28% percent have received fraudulent emails (in the UE the percentage was 38%).

Figure 21. Digital security incidents by individuals (2015 or later)
(as a percentage of all individuals and by level of educational attainment)



Source: Report "OECD Digital Economy Outlook 2017"

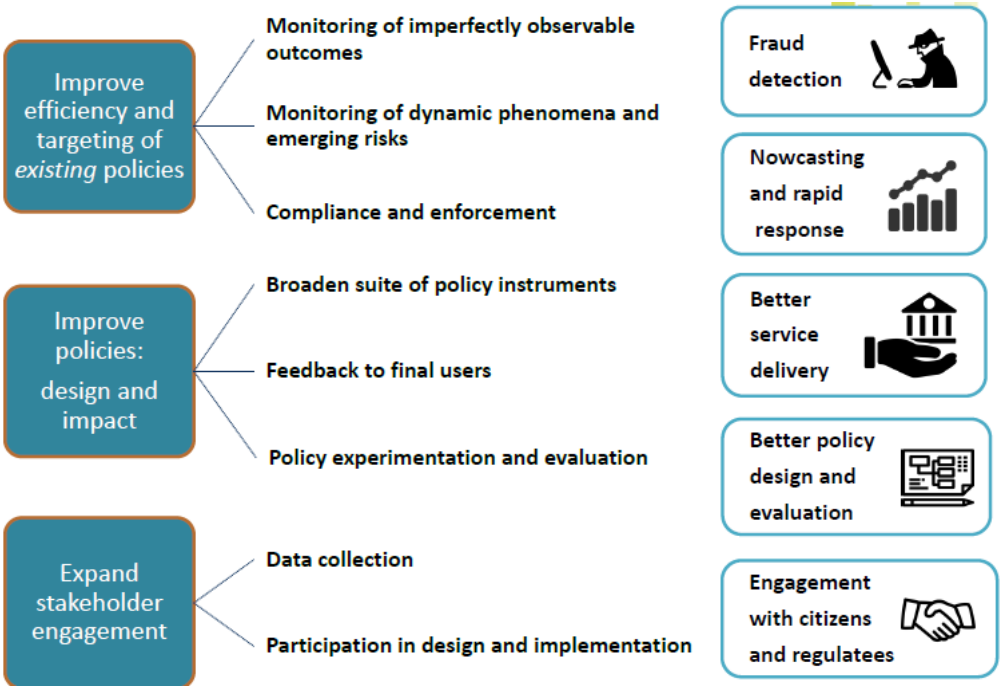
- **Barriers faced by each country in the field of legislation and web security**

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, the main barriers faced by Portugal in the field of legislation and web security are:

- The existence of divergences regarding the information, the measures and the procedures necessary to a proper implementation of the RGDP because lots of companies still don't know exactly what to do;
- A lot of people and companies complain about the excess of information that is also not clear or simple regarding the new RGDP because lots of institutions, media and people give to much information that sometimes is very contradictory;
- The CNPD said that they don't have means to do their job properly because there are too many solicitations from companies;
- A lot of companies still recognize the need to reinforce the information and training for the workers regarding RGDP;
- The lack of knowledge and skills regarding the penalties associated to RGDP;
- The lack of definition that still exists in some aspects related to the regulation and its supervision that also limit the growth of the size of the company;
- The majority of the companies need a first assessment related to the level of the conformity and the adequacy of current policies and processes for a correct identification of possible changes;
- The actual challenges related to the modernization, globalization, technology and digitalization implies a revision of the RGDP process that already exists continuously.

In this context, there are some things that can and must be done in order to improve digital transformation (see figure 22).

Figure 22. How to improve digital transformation



Source: "Trend and Key Policy Issues for Digital Transformation" by OECD (2017)

7.4. SPAIN

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

This code references the following laws, among others:

- National Security Regulations:
  - Law 36/2015, of September 28 on National Security, which regulates the key principles and agencies, as well as the functions they must perform, for the defense of the National Security.
  - Order TIN/3016/2011, of October 28, which established the Security on Information and Communication Technologies Committee of the Ministry of Labor and Immigration.
  - Security regulations:
  - Organic Law 4/2015, of March 30, on the protection of public safety.
  - Law 5/2014, of April 4, on Private Security.

- In relation to security incidents, there is a whole network related to the Armed Forces, but there is also a partial inclusion in the Law 34/2002, of July 1, on services to the society of information and electronic commerce.
- Regarding telecommunications, the following rules exist:
  - Law 34/2002, of July 11, on services to the information society and e-commerce (cited above).
  - Royal Decree 381/2015, of May 14, which establishes measures against illegal or irregular traffic which has fraudulent purposes in electronic communications.
  - Law 50/2003, of December 19, on the electronic signature.
  - Law 9/2014, of May 9, general telecommunications.
  - Law 25/2007, of October 18, on the retention of data related to electronic communications and public communication networks.

- Related to cybercrime, we find partial inclusions in the Criminal Code, the Organic Law 5/2000, of January 12, which regulates the criminal responsibility of minors; or in the Royal Decree approving the Criminal Procedure Law.
- Also applicable is the regulation on the protection of data, developed by the Organic Law 15/1999, of December 13 and its regulations, approved by the Royal Decree 1720/2007 of December 21.

The Spanish approach to cybersecurity includes the following ten sections:

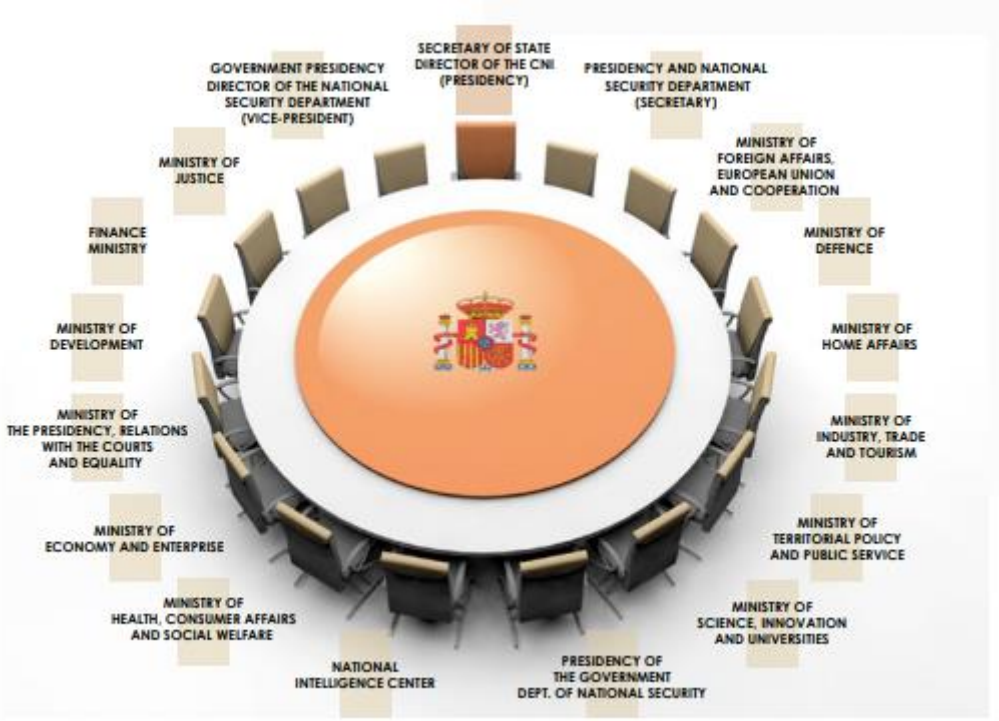
1. Establishment of the vision, scope, objectives and priorities: Cybersecurity Strategy.
2. Establishing a clear governance structure that identifies and engages stakeholders: Governance.
3. Take stock of existing policies, regulations and capacities: Enabling regulatory development. Support in an operational and effective legal framework.
4. Increased capacity for prevention, detection and response to cyberthreats, creating reference and sector CSIRT.
5. Development and implementation of Early Warning Systems. Detection capacity and establishment of incident notification mechanisms.
6. Increased surveillance, with a continuous assessment and cybervigilance service based on Cybersecurity Operations Centers (SOC), that allow knowing at any time the surface area of exposure to a potential threat and thus allocating resources in an optimal and prioritized manner.
7. Promotion, development and maintenance of qualified professional profiles at all levels (management, administration, implementation and users) to protect against cyberthreats. Talent search has become a critical element.
8. Actions to strengthen public-private partnerships and the security and robustness of ICT networks, products and services used by the industrial sector will be promoted and led. Institutionalize cooperation between public agencies and private enterprise as a key to building community.
9. Implementation of reliable mechanisms for the exchange of information between public and private organizations, both for the cyberthreats analysis and for the cyberincidents' notification, in order to build trust.
10. Communication and promotion, aimed at achieving strategic objectives. All of this, aware of the need to make themselves known, to disseminate services and to achieve the recognition and trust of the entire community, becoming a reference point in cybersecurity matters.

Action lines:

1. Cyberthreat: prevention, detection, response and recovery capabilities.
2. Ensure: implementation of the National Security Framework, strengthen capacities.
3. Information: Systems and Telecommunications Security that support the Critical Infrastructures.
4. Capacity to investigate and prosecute cyberterrorism and cybercrime.
5. Enhance the security and resilience of infrastructures, networks, products and services using public-private cooperation instruments

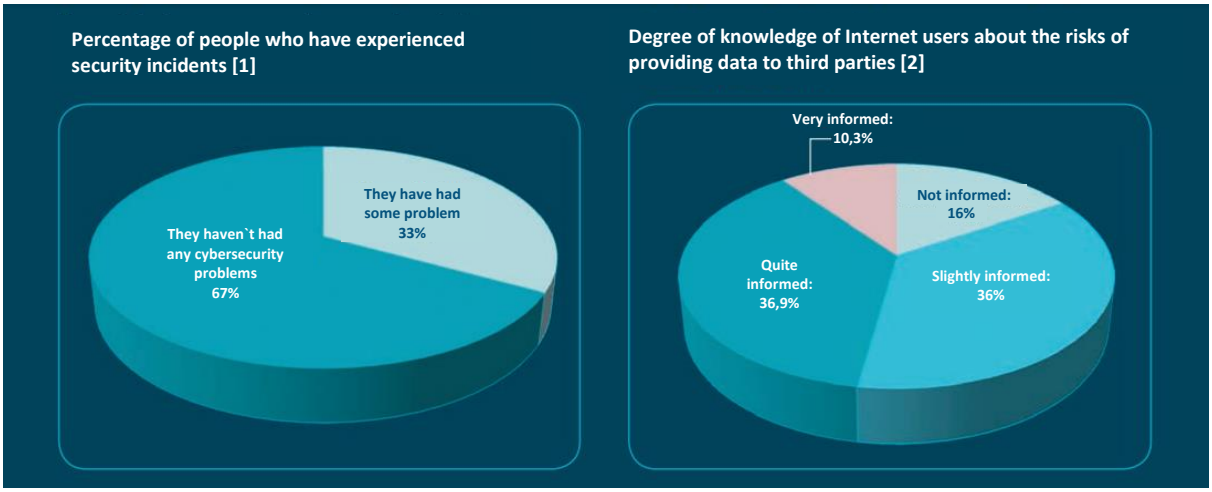
6. Promote professionals' training, boost industrial development and strengthen the R&D system in the area of cybersecurity
7. Raise awareness among citizens, professionals and businesses of the importance of cybersecurity and the responsible use of new technologies
8. Promoting a safe and reliable international cyberspace in support of national interests

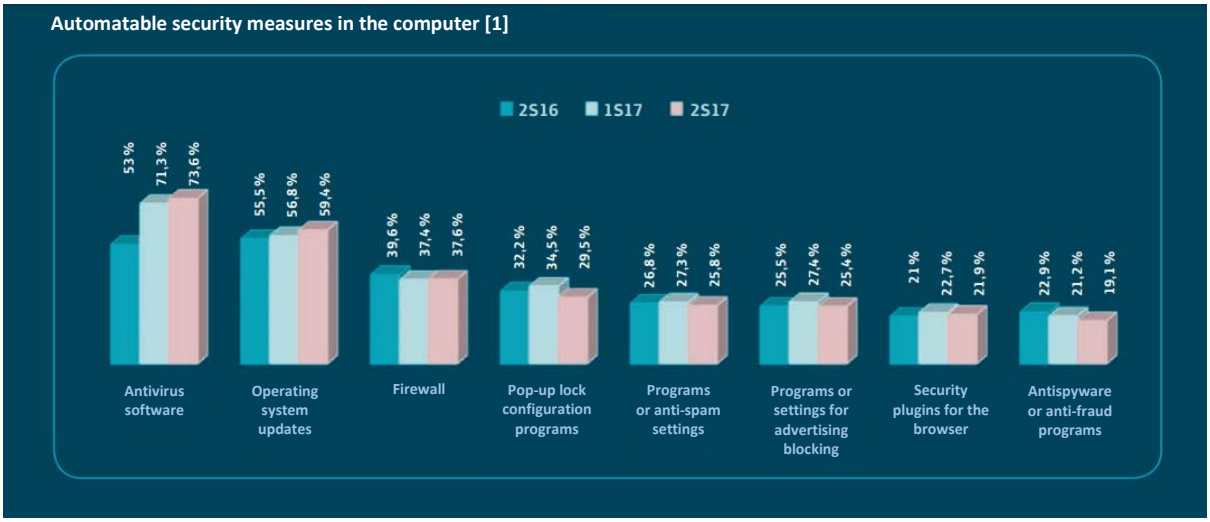
Figura 23. Authorities

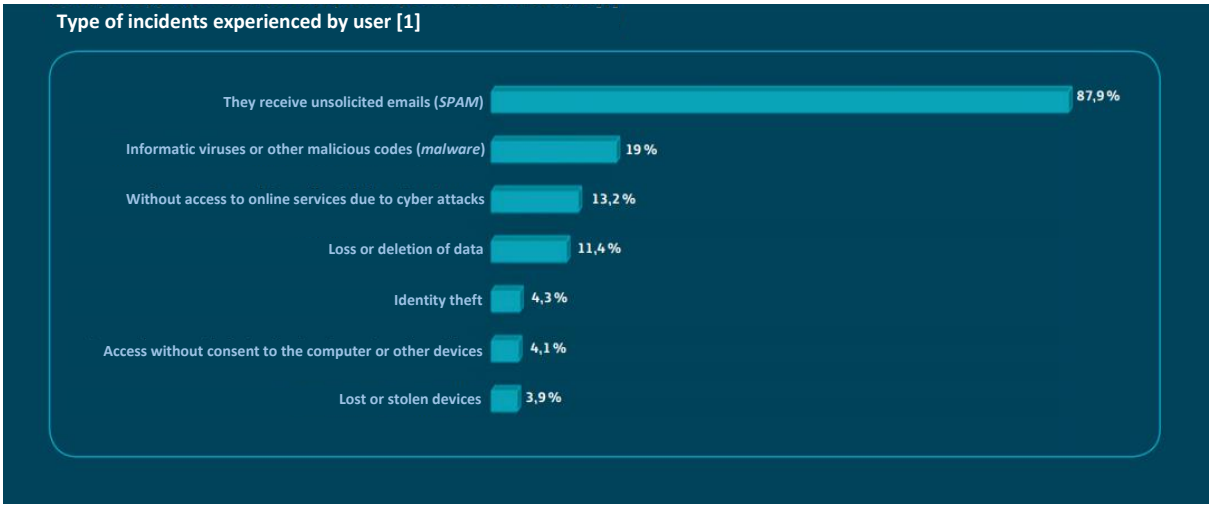


Source: CNN

Figura 24. Users cybersecurity knowledge







Source: Red.es

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. In December 2018, Spain approved a controversial data protection law (LOPD) to facilitate compliance with Spanish law to the EU General Data Protection Regulation. The Official Gazette of Spain published the Organic Law 3/2018, of December 5, on the Protection of Personal Data and the Guarantee of Digital Rights.This law adapts the General Data Protection Regulation, applicable from 25 May 2018, to the Spanish legal system, and introduces and guarantees a new set of digital rights to the public, in accordance with the mandate contained in the Spanish Constitution. 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. For this reason, those businesses, associations, administrations or the self-employed that deal with personal data on a daily basis must consider the following questions to determine if they are complying with the LOPD.

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.

Compliance with the new standards becomes necessary, not only because it imposes important sanctions of up to 4% of the annual global turnover or 20 million euros for the breach of the established obligations, but also because for the first time many digital advertising businesses will have to necessary comply with data protection standards.

Some of the more noteworthy aspects regulated by this act are the followings:

- It regulates the processing of deceased persons' data in a specific and separate way.
- It makes use of the leeway granted under the GDPR, establishing the minimum age of consent for minors at 14.
- It limits the consent granted regarding special categories of personal data, in such a way that it will be insufficient to process certain types of personal data (ideology, union membership, religion, sexual orientation, race, creed, or ethnicity).
- It specifies those cases wherein the processing of data of a criminal nature is permitted.
- It recognizes the double layer mechanism and the minimum content of basic information to comply with the duty of information for data subjects regarding the processing of their personal data.
- It develops the regulation applicable to the exercise of the rights of data subjects, adding the concept of "data blocking," when the data subjects request the amendment or deletion of their personal data.
- It specifically regulates certain personal data processing, which it considers lawful based on legitimate interest or public interest (processing of contact data; credit information systems; commercial transactions; video surveillance; advertising exclusion systems; internal whistleblower information systems).
- It includes a catalogue of situations that must be taken into account when determining the application of technical and organizational measures.
- It clarifies the distinction between the data controller and the data processor, as well as their duties.

- It includes a full catalogue of entities that must appoint a data protection officer, including new categories in addition to those initially envisioned, and it imposes the obligation to report the appointment to the Spanish Data Protection Agency within a maximum period of 10 days.
- It details the cases where an international data transfer is permitted.
- It specifies how to initiate the sanctioning process and its duration, differentiating between cases that concern the (i) failure to address a request for the exercise of rights; (ii) determination of the existence of a possible infringement; and (iii) processing of the procedure as a result of notification of a claim filed with another national control authority. Likewise, it includes an open catalogue of infringements, divided into three categories (minor, severe, and very severe).
- It recognizes and guarantees a new catalogue of digital rights, which includes net neutrality, universal internet access, digital security, digital literacy, the online protection of minors, the amendment or updating of information online, the right to be forgotten on search engines and social networks, and the regulation of the right to a digital last will and testament.
- It strengthens the privacy of employees and their right to digital disconnection and privacy vis-à-vis the use of digital devices, video surveillance, and geolocation in the workplace, and it permits collective agreements that ensure greater protection.
- It extends the validity of data processing agreements signed prior to the application of the GDPR until their expiration date or, for indefinite contracts, until May 25, 2022.

In conclusion, the LOPDGDD has gone a step further and has not limited itself to specifying or restricting the provisions of the GDPR (as regulated in recital 8) but has incorporated a series of digital rights to citizens, which a priori covers the needs favoured by the rapid evolution of new technologies, but on which it will be necessary to analyse whether its practical application reflects the reality and needs of the public in relation to said matters, and the impact that they might have on information society and internet services providers, as these are also the main parties affected by the introduction of these new rights.

BIBLIOGRAPHY

Bundesministerium für Digitalisierung und Wirtschaftsstandort1 (2019). Bundesrecht konsolidiert. Retrieved from https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR12017706.

Bundesministerium für Digitalisierung und Wirtschaftsstandort2 (2019). Bundesrecht konsolidiert. Retrieved from https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR40045309.

Bundesministerium für Digitalisierung und Wirtschaftsstandort3 (2019). Bundesrecht konsolidiert. Retrieved from https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR12108893.

Bundesministerium für Digitalisierung und Wirtschaftsstandort4 (2019). Bundesrecht konsolidiert. Retrieved from https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR12097063.

Bundesministerium für Digitalisierung und Wirtschaftsstandort5 (2019). Bundesrecht konsolidiert. Retrieved from https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR40123095.

Bundesministerium für Digitalisierung und Wirtschaftsstandort6 (2019). Bundesrecht konsolidiert. Retrieved from https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR12097069.

Bundesministerium für Digitalisierung und Wirtschaftsstandort7 (2019). Bundesrecht konsolidiert. Retrieved from https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR12057374.

Bundesministerium für Digitalisierung und Wirtschaftsstandort8 (2019). Art. 8 Federal Constitutional Law Bundes-Verfassungsgesetz (BVG). Retrieved from https://www.dsb.gv.at/documents/22758/116802/Art_8_Bundes-Verfassungsgesetz_(B-VG)_auf_Deutsch_und_Englisch.pdf/02e7057d-a82c-415f-bff0-15f8423a7487.

Bundesministerium für Digitalisierung und Wirtschaftsstandort9 (2019). Bundesrecht konsolidiert. Retrieved from https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR40025801.

Bundesministerium für Digitalisierung und Wirtschaftsstandort10 (2019). Bundesrecht konsolidiert. Retrieved from https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR40025802.

Bundesministerium für Digitalisierung und Wirtschaftsstandort11 (2019). Bundesrecht konsolidiert. Retrieved from https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR40025803.

Bundesministerium für Digitalisierung und Wirtschaftsstandort12 (2019). Bundesrecht konsolidiert. Retrieved from https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR40025804.

Bundesministerium für Digitalisierung und Wirtschaftsstandort13 (2019). Auszug aus dem Gentechnikgesetz, BGBl. Nr. 510/1994. Retrieved from https://www.dsb.gv.at/documents/22758/116802/§_67_Gentechnikgesetz_auf_Deutsch_und_Englisch.pdf/4acf9864-b2f1-4eed-98f8-b9a5bfbbac5a.

Bundesministerium für Digitalisierung und Wirtschaftsstandort14 (2019). Bundesrecht konsolidiert. Retrieved from https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR40032660.

Bundesministerium für Digitalisierung und Wirtschaftsstandort15 (2019). Bundesrecht konsolidiert. Retrieved from https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR40050278.

Bundesministerium für Digitalisierung und Wirtschaftsstandort16 (2019). Bundesrecht konsolidiert. Retrieved from https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR40138785.

Bundesministerium für Digitalisierung und Wirtschaftsstandort17 (2019). Bundesrecht konsolidiert. Retrieved from https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR40155546.

Bundesministerium für Digitalisierung und Wirtschaftsstandort18 (2019). Bundesrecht konsolidiert. Retrieved from https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR40136946.

Bundesministerium für Digitalisierung und Wirtschaftsstandort19 (2019). Bundesrecht konsolidiert. Retrieved from https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR40154248.

Bundesministerium für Digitalisierung und Wirtschaftsstandort20 (2019). Bundesrecht konsolidiert. Retrieved from https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR40154231.

Bundesministerium für Digitalisierung und Wirtschaftsstandort21 (2019). Bundesrecht konsolidiert. Retrieved from https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR40154252.

Bundesministerium für Digitalisierung und Wirtschaftsstandort22 (2019). Bundesrecht konsolidiert. Retrieved from https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR40153731.

Bundesministerium für Digitalisierung und Wirtschaftsstandort23 (2019). Bundesrecht konsolidiert. Retrieved from https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR40150504.

Bundesministerium für Digitalisierung und Wirtschaftsstandort23 (2019). Bundesrecht konsolidiert. Retrieved from https://www.ris.bka.gv.at/.Dokument.wxe?Abfrage=Bundesnormen&DokumentnummDo=NOR40138453

IPSA (2019): Über IPSA. Retrieved from https://www.ispa.at/ueber-ispa/ueber-ispa.html.

Little, A.D. (2018). Digitale Transformation von KMU in Österreich 2018. Retrieved from https://news.wko.at/news/ wien/KMU-Digitalisierungsstudie-2018_Final.pdf.

Österreichische Datenschutzbehörde1 (2019). Datenschutzrecht in Österreich. Retrieved from https://www.dsb.gv.at/ gesetze-in-osterreich [16.04.2019].

Österreichische Datenschutzbehörde2 (2019). Willkommen auf der Website der Datenschutzbehörde. Retrieved from https://www.dsb.gv.at/.

Österreichische Datenschutzbehörde3 (2019). Impressum & Offenlegung gemäß § 25 des Mediengesetzes. Retrieved from https://www.dsb.gv.at/impressum-copyright.

Österreichische Datenschutzbehörde4 (2019). Newsletter. Retrieved from https://www.dsb.gv.at/newsletter.

Österreichische Forschungsförderungsgesellschaft mbH1 (2019). Digitalisierungsagentur. Retrieved from https://www.ffg.at/dia.

Österreichische Forschungsförderungsgesellschaft mbH2 (2019). Andreas Tschas wird Leiter der Digitalisierungsagentur DIA Retrieved from https://www.ffg.at/digitalisierungsagentur.

Saferinternet.at1 (2019). Die Initiative. Retrieved from https://www.saferinternet.at/ueber-saferinternetat/die-initiative/.

Saferinternet.at2 (2019). Unser Team. Retrieved from https://www.saferinternet.at/ueber-saferinternetat/unser-team/.