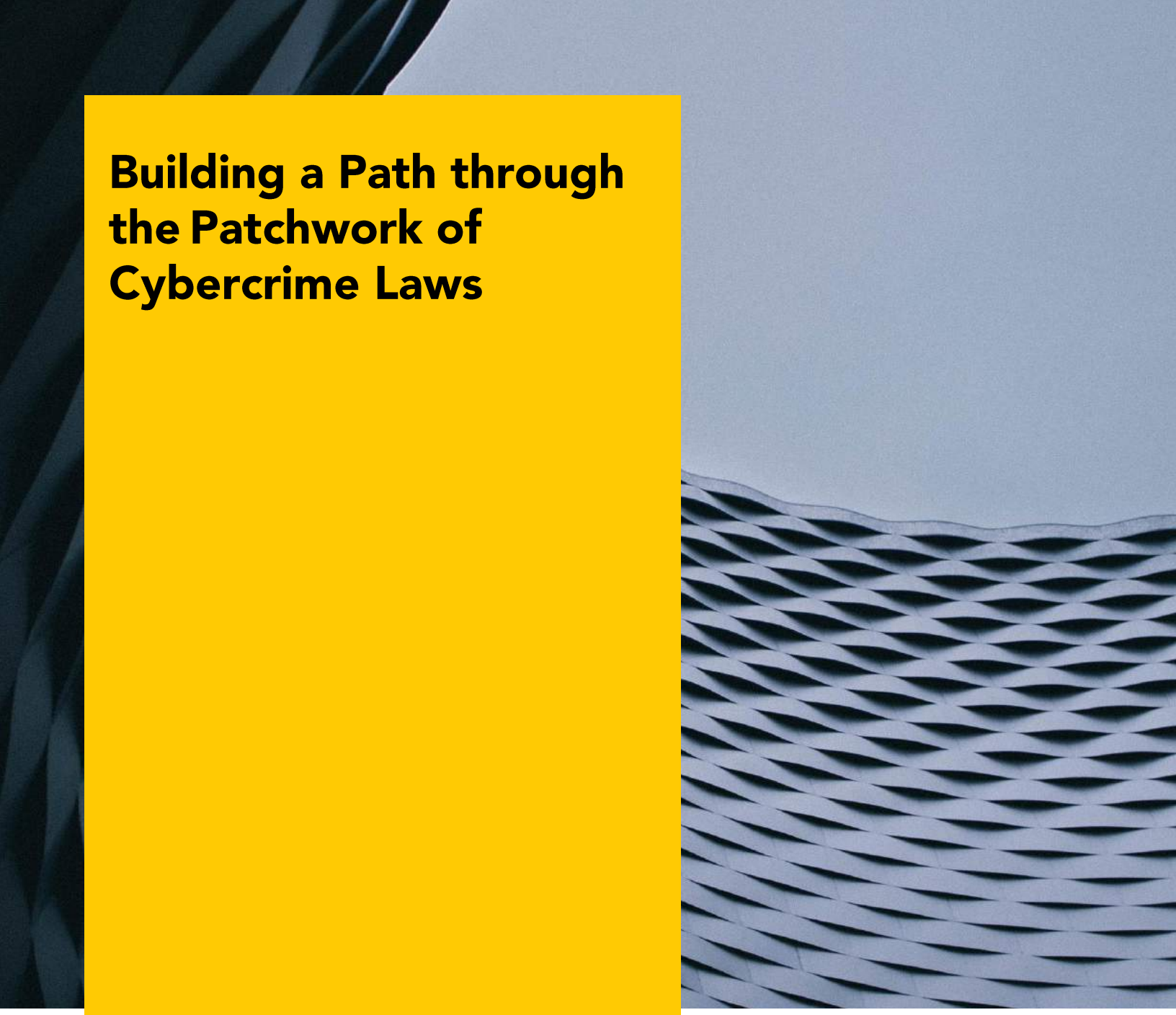


Building a Path through the Patchwork of Cybercrime Laws

OCTOBER 2019

Malta IT Law Association

MALTA IT LAW ASSOCIATION

Malta Information Technology Law Association (MITLA)

www.mitla.org.mt

info@mitla.org.mt

TABLE OF CONTENTS

CONTENTS

1 | ACRONYMS

CoE – Council of Europe

EU – European Union

EU MS – EU Member States

MITLA – Maltese Information Technology Law Association

SME – Small and Medium Size Enterprise

UM – University of Malta

VO – Voluntary Organization

2 | EXECUTIVE SUMMARY

Executive Summary

After first outlining the methodology followed, including the working definition of cybercrime deployed, this report carries out an outline review of national, European and international legislation which may be relevant to the subject.

A key finding of the report is that international, European and national legal frameworks do not include special provisions for SMEs and/or VOs.

As the international, European and national legal frameworks do not include special provisions for SMEs and/or VOs, the only recommendations identified in this report refer not to legal provisions but to methods of implementation and accessibility of legal information which may be organised as follows.

a. Methods of implementation

The GDPR requires all organizations to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. However, what constitutes appropriate security measures varies from country to country.

Emerging Practice 1:

Supporting VOs and SMEs in better understanding and implementing appropriate measures.

This can be achieved in several ways:

a) **By making reference to specific ISO standards (though it is not mandatory to follow this standards) – e.g. Germany**
b) **By developing certification programmes for basic technical controls. These help organisations protect themselves against common online security threats. – e.g. UK Cyber Essentials scheme**

b. Accessibility of legal information

Because of the complexity and diversity of legislation related to cybercrime it can be very difficult for VOs and SMEs to find the right legal information applicable to their individual circumstances.

Emerging Practice 2:

Setting up a one-stop shop for cyber security information

This can be achieved in several ways:

a) **Building a public information platform (or alternatively including such resources on the website of national authorities in the field of cyber security) – UK and Spain (https://www.incibe.es)**
b) **Grouping all relevant legal provisions dealing with cybercrime in one Code – e.g. Codigo de Derecho Ciberseguridad in Spain.**

While the legal framework does not include special provisions for SMEs and/or VOs, European and national cyber-strategies do make specific references to such organizations. The following are some of the key ideas associated with these two categories of actors which we recommend may be considered as options for further action in a Maltese context:

1. SMEs and VOs need special focus and additional support/No "one size fits all" policy

    - Providing funding and know-how for SMEs and VOs to enable them to meet cybersecurity standards;
    - Providing adequate and easily accessible informational resources regarding their rights and obligations in the area of cybersecurity;
    - Setting-up certification mechanisms, which would ensure they meet the required cybersecurity standards.

2. Importance of knowledge transfer between government, academia and private entities and importance of public-private partnerships

    - Fostering exchange of information between government, the private sector, academia and civil society;
    - Create platforms where different actors can collaborate on issues related to cybersecurity.

3. More supply-chain transparency

    - Ensuring that SMEs which are part of the supply-chain of critical infrastructure operators follow the same security procedures;

4. Fostering research & innovation in the area of cyber security
    - Supporting start-ups developing innovative cyber security solutions;

5. Developing skills of SME and VO personnel in the area of cybersecurity

- Organizing training programmes for SMEs and VOs;
- Organizing cybersecurity exercises, which include different societal actors.

Raising awareness of cybersecurity issues (e.g. safe behaviour online).

3 | INTRODUCTION

The Malta IT Law Association (MITLA) embarked on a project - Raising Awareness on Cyber Security (RACS) - funded through the Voluntary Organisations Project Scheme managed by the Malta Council for the Voluntary Sector on behalf of Parliamentary Secretary for Youth, Sports and Voluntary Organisations within the Ministry for Education and Employment".

Malta is increasingly dependent upon the use of Information and Communications Technology (ICT), to the extent that its disruption may affect service, business and potentially, everyday life.

Malta Cyber security Strategy 2016.

The Raising Awareness on Cyber Security (RACS) project seeks to determine where SMEs and Voluntary Organisations (VOs) in Malta stand on cyber security and cyber threats.

More specifically, the study comprises three (3) phases, that may be broadly segmented as follows:

- Phase 1 - Discovery Phase;
- Phase 2 - Research Phase; and
- Phase 3 - Dissemination

Such study was deemed of essence in view of the growing risk of cyberattacks, with European studies evidencing that most European companies are still unprepared and unaware of the risk. Furthermore, a recent study commissioned by the European Economic and Social Committee1 highlighted how small and medium-sized companies (SMEs) are the most exposed, often in view of their budget constraints that limited their investment in cyber security. Furthermore, almost 70% of European companies do not understand the extent of their exposure to cyber risks.

This study is part of WP 1 - Discovery Phase, which aims to study the Maltese cyber security legal framework, to determine laws regulating cyber security and any legal developments in the field, if any, which apply to VOs and local businesses to protect them against cyber threats.

The study will consider local, EU and international legal instruments which regulate online security, including privacy and data protection laws, criminal laws, intellectual property laws, electronic communications laws, laws on electronic commerce, and other instruments regulating confidentiality. This analysis will assist in identifying and researching technical permutations of local VOs and businesses, which are directly dependent on legal obligations related to cybersecurity.

The number of cybercrimes in the world is increasing exponentially each year with global cybercrime damages predicted to cost $6 trillion annually by 2021. While a lot of the cybercrime has been directed against governments and larger business actors, there is quite a number of attacks, which have targeted VOs and SMEs. A FSB statistic released in 2016 showed that 66% of small businesses in the UK had been victims of cyber crime[1] while a Deloitte report from 2017 indicated that cyber crime costs the Dutch SME Sector €1 billion each year[2].

[1] UK National Federation of Self Employed & Small Businesses Limited (FSB), *Cyber Resilience: How to Protect Small Firms in the Digital Economy*, June 2016, available at https://www.fsb.org.uk/docs/default-source/fsb-org-uk/FSB-Cyber-Resilience-report-2016.pdf?sfvrsn=0.
[2] The Hague Security Delta, Cyber Security Week, *Cyber Crime Costs Dutch SME Sector €1 Billion Each Year*, 25 September 2017, available at https://www.cybersecurityweek.nl/news/46-cyber-crime-costs-dutch-sme-sector-1-billion-each-year.

4 | METHODOLOGY

Methodology

This analysis seeks to carry out a comparative analysis of legal provisions and strategies at international, European and EU MS level related to cybercrime and extract those, which are applicable to VOs and SMEs.

It will also try to identify any promising practices in this area and explore ways in which they could be applied to the Maltese context, through integration with the Maltese National Cyber Security Strategy and harmonization with existing legislation in this area.

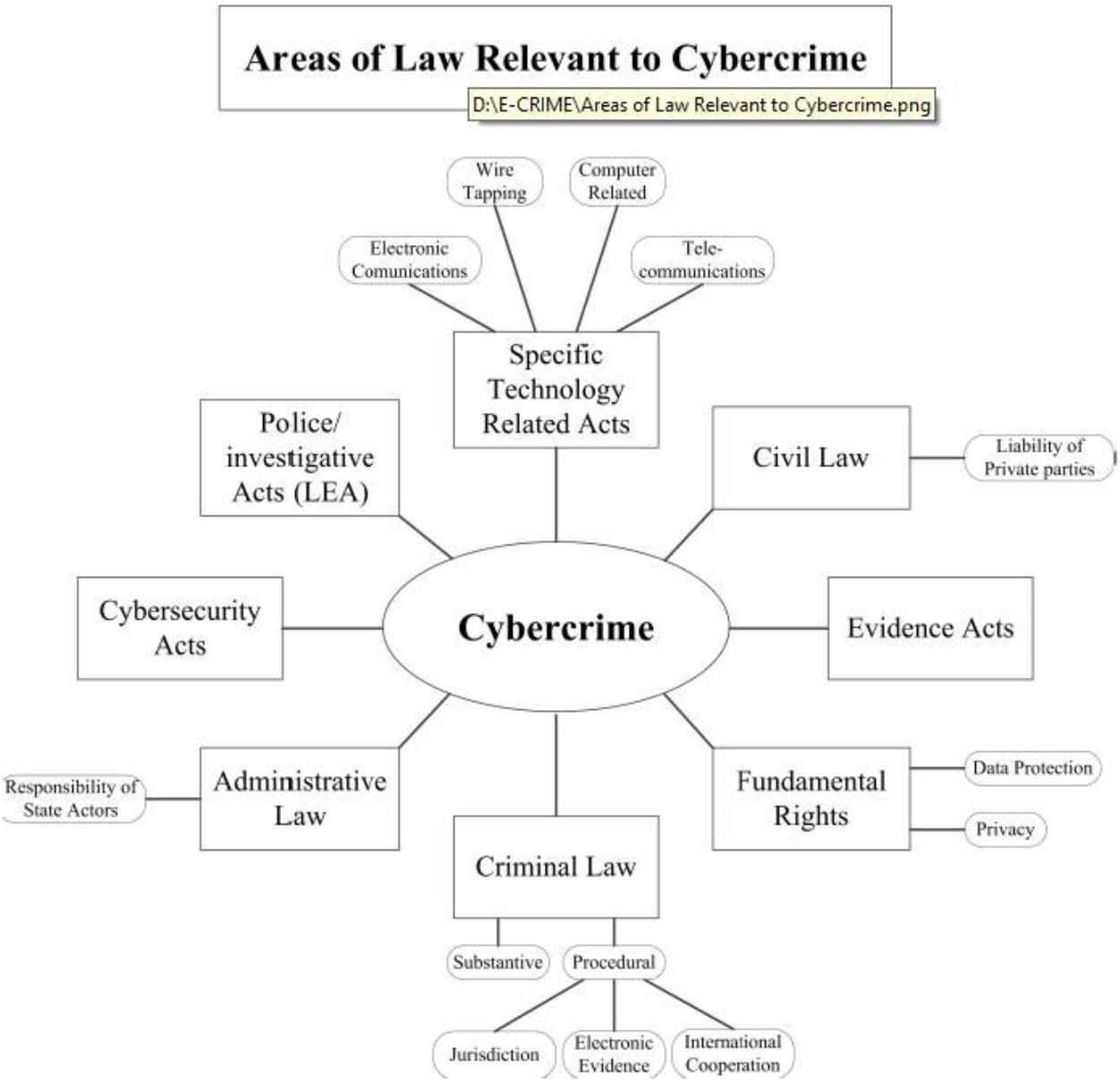
To achieve this, the study uses the comparative legal research methodology. The main criticism brought to this method is the difficulties inherent to cutting across "legal families". This is especially relevant when trying to identify "best practices" that can then be used to improve one's own legal system.

Acknowledging this limitation, the authors of this study have sought to contextualize the analyses being carried out by focusing on three levels: international, European and national and thus providing a wider context for national developments in the different EU Member States. Moreover, we have opted to use the term "promising practices" instead of "best practices" to, further, emphasize the fact that importing rules and solutions from abroad may not work because of a different in national context.

It is important to note here, that in Europe, the adoption of cybercrime legislation at national level was often fostered and influenced by international and/or European developments in the field such as be CoE guidelines published in 1989 or Convention 185 on Cybercrime of the Council of Europe adopted in Budapest on 23rd November 2001. These were later followed by several European Directives and Regulations, the most recent being the General Data Protection Regulation, which entered into force in May 2018.

Furthermore, given that cyber security legislation is often not one single body of laws, but multiple areas of laws are involved, which are directly or indirectly affected by cybercrime. The figure developed as part of the E-Crime project below shows which areas of law are relevant to cybercrime issues.

Fig. 1 – Areas of Law Relevant to Cybercrime[3]



[3] Deliverable 3.2 of the E-CRIME project (Grant Agreement Number 607775): *Final report on countermeasure including policy and enforcement responses*, March 2015.

As it may be seen from the figure above, while both substantive and procedural criminal law is an area directly relevant to cybercrime, there are other areas of law, such as civil and administrative law, specific technology related acts and fundamental rights, which should also be given due consideration. Especially when it comes to the responsibility and liability of state actors or private actors, such as corporations and service providers, civil and administrative law aspects can be very important in preventing or deterring cybercrime. Civil and administrative regulations might also come into play when certain computer related acts are minor infringements that do not need to be covered by criminal law, when criminal law uses underlying civil and administrative standards or when provisions of all these areas of law are combined, for example, in order to create liability[4].

Definition of Cybercrime

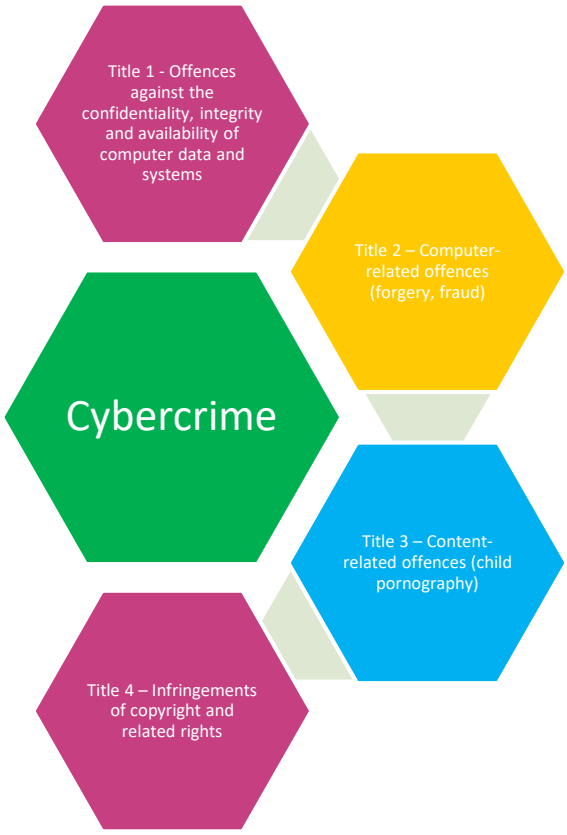
It is important to explain our use of the term 'cybercrime' in this report. Cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content related offences (e.g. online distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware).10

In this report we follow a simple definition and classification of cybercrime. In simple terms, we use the term 'cybercrime' to refer to any cyber activity/activities that meet the characteristics identified by law to be classified as a crime(s). In this simple definition, only cyber activities that fit the description of the law are cybercrimes.

Convention 185 of the Council of Europe (as described later) has four broad categories of activities that can be categorised as cybercrimes:

[4] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, draft February 2013, p. 52.

Fig. 2 – Definition of cybercrime according to Convention 185



Definition and typology of VOs

For the purpose of this study, it is important to first define what voluntary organizations are. This study employs the term voluntary organization (VO) as it is defined in the Maltese Voluntary Organizations Act (Chapter 492 of the Laws of Malta) from 2007. According to this document, VOs are organizations which are created or established for:

- Any lawful purpose;
- As non-profit making;
- Voluntary;

In other European countries, the term "voluntary organization" is replaced by "non-governmental organization" (NGO).

According to their types VOs can be grouped in:

- Foundations;
- Associations; and
- Trusts.

An important consideration to be made regards the legal status of voluntary organizations. While these have the option to register as legal persons, in most countries they do not have the obligation to do so. Which is why in the comparative legal research carried out in this study, we have decided to include both provisions related to individuals (e.g. Criminal Code provisions) and provisions related to legal persons.

Definition and Typology of SMEs

- According to the EU recommendation 2003/361, small and medium-sized enterprises (SMEs) are defined as all entities engaged in an economic activity, irrespective of their legal form with fewer than 250 employees and which are independent from larger companies. This includes, in particular, self-employed persons and family businesses engaged in craft or other activities, and partnerships or associations regularly engaged in an economic activity[5].

There are three types of SME:

- Microenterprises are defined as enterprises which employ fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million.
- Small enterprises have between 10 and 49 employees and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million.
- Medium-sized enterprises have between 50 and 249 employees which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43m

[5] European Commission, *User Guide to the SME Definition*, Ref. Ares(2016)956541, European Union, 2015.

Limitations of the research

When trying to identify promising practices in cyber security legislation applicable to VOs and SMEs, one main limitation is the fact that in most cases, the law only makes a distinction between government and private actors, without including special provisions for different types of private entities[6], such as VOs and SMEs. Therefore, most of the provisions identified in this study are applicable to all private entities and were not designed specifically for either VOs or SMEs. Distinct references to SMEs and occasionally VOs can only be found in national cyber security strategies, and these have been addressed in a special focus of this analysis.

While VOs and SMEs are not identified separately in cyber security legislation, there are cases when, especially the latter category, is actually targeted by special provisions such as the ones dealing with operators of critical infrastructure. When SMEs are part of the supply-chain for critical infrastructure operators, they may have similar legal obligations. However, given the fact that this is a special case and due to time and space limitations, this particular situation will not be addressed in this study.

Another limitation of the research has been the accessibility of national legislation to the research team. While in most cases the research team has tried to use the original version of the legal documents analysed or an official translation, there have been some cases, where the research team lacked the necessary knowledge to be able to use the original version of the law and no official translations were available. In these cases, informal and/or secondary analyses were employed to extract the relevant information.

[6] An exception are provisions dealing with a special category of private actors, namely the operators of critical infrastructure, which are often identified as a separate category in legislation dealing with cybercrime and cyber security.

5 | LEGISLATION

National, European and International Legislation

Not only is cybercrime addressed by different areas of law, but it is also addressed at different levels. According to the EU's Cybersecurity strategy, it is predominantly the task of Member States to deal with security challenges in cyberspace. However, cybercrime by its very nature requires to be addressed internationally, as it is not restricted by geographical limitations or national boundaries[7]

This section examines the existing framework of legislation and policies covering cybercrime, the emphasis will be on the international and European framework. Some examples of national laws and policies will also be mentioned in order to illustrate how the international framework influences national laws.

International Legal Instruments

When it comes to cybercrime the most important piece of international legislation is by far the Convention 185 of the Council of Europe adopted on 23rd November 2001. The Convention entered into force on the first of July 2004 and currently has 61 ratifications and 4 signatures not yet followed by ratification (including a number of EU Member States). The Convention includes a number of ratifications and signatories, which are non-members of the Council of Europe, such as the United States of America, Japan and Australia.

The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography, hate crimes, and violations of network security.

The aim of the Convention is to:

- Harmonise domestic criminal substantive law elements of offences and connected provisions in the area of cybercrime;
- Provide for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form;
- Set up a fast and effective regime of international cooperation.[8]

[7] Council of Europe, *Explanatory report to the Convention of Cybercrime* (ETS No 185), p. 1 – 2.
[8] Council of Europe, *Explanatory report to the Convention of Cybercrime* (ETS No 185), p. 4.

The convention consists of four chapters:

- Use of terms;
- Measures to be taken at domestic level – substantive law and procedural law;
- International cooperation;
- Final clauses.

In chapter 1 (Use of terms) of the Convention, which consists only of 1 article, the Convention provides for a number of definitions – including 'computer system', 'computer data', 'service provider' and 'traffic data' – to be used for the purpose of the Convention.

Chapter 2, 'Measures to be taken at the national level', of the Convention consists of three sections: substantive criminal law, procedural law and jurisdiction.

Chapter 3 of the Convention on international cooperation consists of a section on general principles and a section on specific provisions.

The final chapter of the Convention, chapter 4 consists of the final provisions determining the signature and entry into force of the Convention, accession details, the territorial application and the effects of the Convention, declarations, reservations and amendments to the Convention and the settlement of disputes relating to the interpretation or application of the Convention. A number of elements of the Convention mentioned before will be discussed in more detail.

6 | CRIMINAL LAW

Substantive Criminal Law

The substantive criminal law part of the Convention is directed at States Parties to the Convention in order to harmonise 4 categories of offences:

a) Offences against the confidentiality, integrity and availability of computer data and systems;

b) Computer related offences;

c) Content related offences;

d) Offences related to infringements of copyright and related rights.

The substantive criminal law part furthermore provides for ancillary liability and sanctions.

Category 1:- Offences against the confidentiality, integrity and availability of computer data and systems.

This category of crime includes:

- illegal access (Art. 2)
- illegal interception (Art. 3)
- data interference (Art. 4)
- system interference (Art. 5); and
- misuse of devices (Art. 6).

These offences may include: building a botnet, ransomware, malware, etc.

Illegal access (Art. 2)

Illegal access refers to acts where part of or the entire computer system is entered without any authorisation or justification. For example, circumventing a firewall and entering the computer system of a bank . According to the Council of Europe, illegal access covers the basic offence of dangerous threats to and attacks against the security (i.e. the confidentiality, integrity and availability) of computer systems and data .

Based on Art. 2 of the Convention illegal access requires the intentionally committed act of accessing the whole or any part of a computer system without right. Without right, meaning that there is no criminalisation of the access authorised by the owner or other right holder of the system or of access to open sources.

This is a very broad approach of criminalisation, which has led to a range of countries introducing a narrower approach requiring additional qualifying circumstance .

The Convention furthermore stipulates in the second sentence of article 2 that States Parties to the Convention may require within their national laws that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system. May require, meaning that this provision is optional.

States Parties to the Convention may attach any or all of the qualifying elements listed in the second sentence: infringing security measures, special intent to obtain computer data, other dishonest intent that justifies criminal culpability, or the requirement that the offence is committed in relation to a computer system that is connected remotely to another computer system.

This article protects the interests of organisations and individuals in managing, operating and controlling their systems in an undisturbed and uninhibited manner as illegal access may cause alteration or destruction with high costs for reconstruction. In the explanatory report to the Convention, the Council emphasises that the most effective means of preventing unauthorised access is to introduce effective security.

Illegal interception (Art. 3)

Illegal interception refers to acts involving obtaining data during a transmission process that is not intended to be public, as well as obtaining computer data (such as by copying data) without authorisation. For example, illegally accessing a computer database and recording transmissions without right within a wireless network.

The main aim of this article is thus to protect the right of privacy of data communication enshrined in article 8 of the European Convention on Human Rights (ECHR)[9].

Based on Art. 3 of the Convention, illegal interception requires intentional interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. For criminal liability, the illegal interception must thus be committed intentionally and without right, meaning that the act is justified, for example, if the intercepting person has the right to do so, if he acts on the instructions or by authorisation of the participants of the transmission (including authorised testing or protection activities agreed to by the participants), or if surveillance is lawfully authorised in the interests of national security or the detection of offences by investigating authorities.

States Parties to the Convention may furthermore require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system. The "may" in this sentence suggests that this part of the provision is optional.

[9] Convention for the Protection of Human Rights and Fundamental Freedoms [1950] as amended by Protocols No. 11 and No. 14 [2010] CETS No. 194.

Data interference (Art. 4)

Data interference refers to acts involving damage, deletion, deterioration, alteration or suppression of computer data without authorisation or justification. For example, deleting computer program files necessary for the functioning of an internet server or altering records in a computer database. Hacking into computer systems associated with critical infrastructures such as water or electricity supply systems may result in illegal data interference or system damage.

Based on article 4 of the Convention, data interference requires intentionally, damaging, deleting, deteriorating, altering or suppressing of computer data without right. These acts are thus only punishable if committed intentionally and without right. This provision aims to protect computer data and computer programs.

Article 4 furthermore stipulates that States Parties to the Convention may reserve the right to require that this conduct results in serious harm. This allows Parties to enter a reservation concerning the offence in that they may require that the conduct result in serious harm under national law.

System interference (Art. 5)

System interference refers to acts hindering the functioning of a computer system without authorisation or justification. For example, submitting so many requests to a computer system that it can no longer respond to legitimate requests, denial-of-service attacks.

Based on article 5 of the Convention, system interference entails the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data. These acts are only punishable if committed intentionally, without right and if the hindering is serious, meaning that States Parties to the Convention may require a minimum amount of damage to be caused in order for the hindering to be considered serious. This provision

aims at criminalising the intentional hindering of the lawful use of computer systems including telecommunications facilities by using or influencing computer data.

Misuse of devices (Art. 6)

Misuse of devices refers to acts involving the development or distribution of hardware or software solutions that can be used to carry out computer or internet related offences. For example, develops tools to automate denial-of-service attacks.

Based on article 6 of the Convention misuse of devices entails:

- The production, sale, procurement for use, import, distribution or otherwise making available of a device, including a computer programme, designed or adapted primarily for the purpose of committing any of the offences established in Art. 2 – 5 of the Convention described above;

- The production, sale, procurement for use, import, distribution or otherwise making available of a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed;

- Possession of any of these items. With regard to possession, States Parties to the Convention may require by law that a number of such items be possessed. The number of items possessed goes directly to proving criminal intent. It is up to each Party to decide the number of items required before criminal liability attaches.

The offence furthermore requires that it be committed intentionally and without right. Production and putting on the market devices for legitimate purposes, e.g. to counter attacks against computer systems as well as tools created for the authorised testing or the protection of a computer system are not criminalised. Apart from the general intent requirement, there must be the specific direct intent that the device is used for the purpose of committing any of the offences established in articles 2 – 5 of the Convention

Category 2 – Computer-related offences

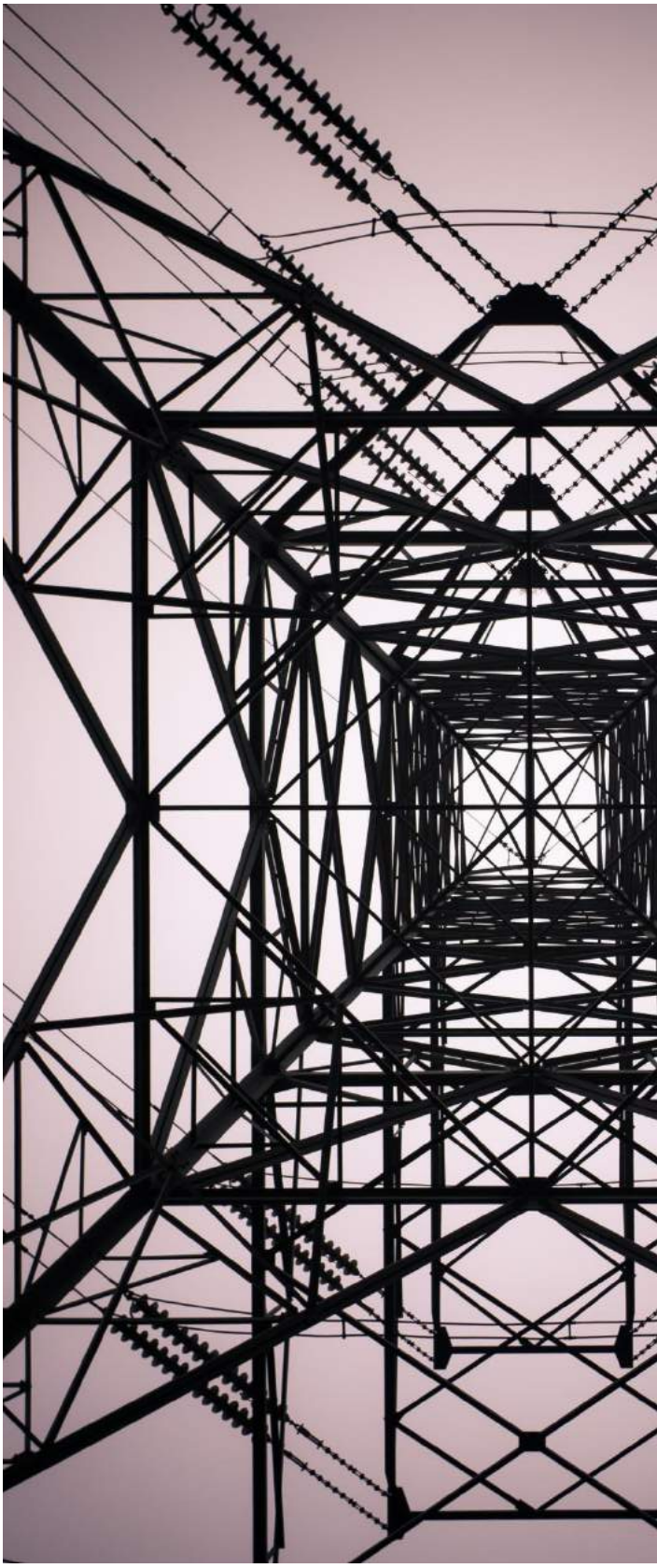
Computer related offences include forgery (Art. 7) and fraud (Art. 8). Click fraud for example may fall within these types of offences. These may be ordinary crimes that are frequently committed through the use of a computer system.

Computer-related forgery (Art. 7)

Computer related forgery refers to acts involving interference with or illegal accesses to a computer system or data with the intent of deceitfully or dishonestly obtaining money, other economic benefit or evading a liability, as well as to acts involving interference with a computer system or data in way that results in the creation of inauthentic computer data. For example, modifying software used by a bank to redirect money transfer processes.

Based on Art. 7 of the Convention, computer related forgery entails intentionally and without right inputting, altering, deleting, or suppressing computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may furthermore require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Computer related forgery involves unauthorised creating or altering stored data so that they acquire a different value in the course of transactions. National concepts of forgery vary greatly. Forgery within the spirit of this article requires that the deception as to authenticity refers at minimum to the issuer of the data, regardless of the correctness or veracity of the contents of the data[10].



[10] Council of Europe, *Explanatory report to the Convention of Cybercrime* (ETS No 185), paras. 81 – 85.

Computer-related fraud refers to acts involving interference with or illegal accesses to a computer system or data with the intent of deceitfully, dishonestly obtaining money, other economic benefit, or evading a liability, as well as to acts involving interference with a computer system or data in way that results in the creation of inauthentic computer data. For example, modifying an authentic email from a financial institution with an underlying intent to defraud, for example phishing.

Computer-related fraud (Art. 8)

Based on article 8 of the Convention, computer related fraud entails intentionally and without right, causing of a loss of property to another person by any input, alteration, deletion or suppression of computer data or by any interference with the functioning of a computer system with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Computer related fraud consists mainly of input manipulations, where incorrect data is fed into the computer, or by programme manipulations and other interferences with the course of data processing. Article 8 criminalises any undue manipulation in the course of data processing with the intention to effect an illegal transfer of property. The computer fraud is thus criminalised if direct economic or possessory loss of another person's property is produced and the perpetrator acted with the intent of procuring an unlawful economic gain for himself or for another person[11].

[11] Council of Europe, *Explanatory report to the Convention of Cybercrime* (ETS No 185), paras. 86 – 90

Category 3 – Content-related offences

Content related offences (Art. 9) are offences related to child pornography. This area has been further regulated in various international instruments[12].

Category 4 – Offences related to infringements of copyright and related rights

The final category are offences related to infringements of copyright and related rights (Art. 10), such as espionage. Infringements of intellectual property rights, in particular of copyright, are among the most commonly committed offences on the Internet. The reproduction and dissemination on the internet of protected works, without the approval of the copyright holder, are extremely frequent[13].

Offences related to infringements of copyright and related rights (Art. 10)

Offences related to infringements of copyright and related rights refers to acts involving the copying of material stored in computer data or generates computer data in violation of copyright or trademark protections. For example, distributing a song protected by copyright through a file sharing system without the license of the copyright owner[14].

Based on Art. 10 of the Convention, the infringement of copyrights and related rights, as defined under national law, where such acts are committed wilfully, on a commercial scale and by means of a computer system is criminalised. States Parties to the Convention are required to criminalise those infringements. The precise manner in which such infringements are defined under national law and may thus vary per country. However, criminalisation obligations under the Convention do not cover intellectual property

[12] Such as Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse [2007] CETS No. 201; Optional Protocol to the UN Convention on the rights of the child, on the sale of children, child prostitution and child pornography; o Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA [2012] OJ L 26.
[13] Council of Europe, *Explanatory report to the Convention of Cybercrime* (ETS No 185), para. 107.
[14] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, draft February 2013, Annex one, p. 257-258.

infringements other that those explicitly addressed in article 10 and thus exclude patent or trademark-related violations[15].

This provision is in line with various international trade instruments and therefore provides for criminal sanctions against infringements on a commercial scale and by means of a computer system[16].

Category 5 – Ancillary liability and sanctions

The substantive criminal law part of the Convention furthermore criminalises attempt and aiding or abetting (Art. 11), sets rules for corporate liability (Art. 12) and requires States Parties to the Convention to adopt sanctions and measures (Art. 13) in accordance with which the offences listed before (Art. 2 – Art. 11) are punishable by effective, proportionate and dissuasive sanctions, including deprivation of liberty. Art. 13 does however not indicate minimum penalties or guidelines meaning that sanctions and measures may vary significantly among the States Parties.

Corporate liability

Legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

- a power of representation of the legal person;
- an authority to take decisions on behalf of the legal person;
- an authority to exercise control within the legal person.

[15] Council of Europe, *Explanatory report to the Convention of Cybercrime* (ETS No 185), para. 109.
[16] Council of Europe, *Explanatory report to the Convention of Cybercrime* (ETS No 185), paras. 107 – 117.

Transposition of the Convention on cybercrime into the national legislation of EU Member States.

Austria

Austria has ratified the Convention in 2012 and has implemented its provisions in the Austrian Penal Code.

The Penal Code includes the following crimes as defined by Articles 2-12 of the Cybercrime Convention:

- Article 2 (illegal access) is implemented by § 118a StGB;
- Article 3 (unlawful interception) is implemented by § 119a StGB (and possibly also by § 119 StGB (violation of secrecy of telecommunications;
- Article 4 (data manipulation) is implemented by 126a StGB;
- Article 5 (system interference) is implemented by § 126b;
- Article 6 (misuse of devices) is envisaged by § 126c StGB;
- Article 7 (computer-related forgery) is implemented by § 225a StGB;
- Article 8 (computer-related fraud) is implemented by § 148a StGB;
- Article 9 (child abuse images) is implemented by § 207a StGB
- Article 10 (copyright and related rights) is criminalized by § 91 juncto 86 para 1, 90b, 90c para 1, 90d para 1 UrhG.
- Article 11 (aiding, abetting, attempt) can be found in §§ 12 and 15 that find general application.
- Article 12 (corporate liability) is represented by § 3 Federal Statute on Liability of Entities (Verbandsverantwortlichkeitzgezetz)[17].

[17] More information on this is available in the section on Transposition of Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems.

Belgium

Belgium signed Convention 185 in 2003, but had not yet ratified it. However, Belgium now has in place Law of 28 November 2000 on computer crime. Prior to the Law of 28 November 2000 on computer crime, Belgium did not have any specific legislation for the criminalization of computer offenses.

Bulgaria

Criminal code Bulgaria:

- Article 212a:

  (1) (Amended, SG No. 38/2007) Where an individual, in view of providing a benefit to him-/herself or another, brings or maintains misleading representations in someone through introducing, modifying, deleting, or erasing computerized data or through the use of an electronic signature of another causes him/her or another harm, shall be punished for computer fraud by imprisonment from one to six years and a fine from up to BGN 6,000.

  (2) (Amended, SG No. 38/2007) The same form and amount of punishment shall be imposed to the individual who, without being entitled thereto, introduces, modifies, or erases computerized data in order to unduly obtain something, that should not go to him.

- Article 216 Section VII Destruction and Endamagement

  (3) (New, SG No. 92/2002) Where an individual, through acquiring illegal access to a computer relevant to an enterprise, establishment, legal entity or individual, destroys or causes harm to the property of another, shall be punished by imprisonment from one to six years and a fine of up to BGN 10,000

- Article 319a Chapter Nine "A" (New, SG No. 92/2002) Cybercrime

  (1) (Amended, SG No. 38/2007) Anyone who copies, uses or obtains access to computer data in a computer system without permission, where such is required, shall be punished by a fine from up to BGN 3,000.

  (2) Where the act under Paragraph 1 has been committed by two or more people, who have previously agreed so to do, the punishment shall be imprisonment of up to one year or a fine from up to BGN 3,000.

  (3) (Supplemented, SG No. 38/2007) Where the act under Paragraph 1 is repeated or is with regard to data for creation of an electronic signature, the punishment shall be imprisonment of up three years or a fine of up to BGN 5,000.

  (4) (Amended, SG No. 26/2004, supplemented, SG No. 38/2007) Where acts under paragraphs 1 - 3 have been committed with regard to information that qualifies as a secret of the State or to another information protected by the law, the punishment shall

be imprisonment from one to three years, unless severer punishment has been envisaged.

(5) Where grave consequences have occurred as a result of the acts under Paragraph 4, punishment shall be of one to eight years.

- Articles 319b, c, d, e

Croatia

Croatia ratified the Convention in 2002.

It entered into force in 2004 through the following amendments to the Criminal Code OG (125/11, 144/12, 56/15, 61/15):

- Article 266 – Unauthorized Access;
- Article 269 - Unauthorised Interception of Computer Data;
- Article 273 - Serious Criminal Offences Against Computer Systems, Programmes and Data;
- Article 268 - Damage to Computer Data;
- Article 273 - Serious Criminal Offences Against Computer Systems, Programmes and Data;
- Article 267 - Computer System Interference;
- Article 273 - Serious Criminal Offences Against Computer Systems, Programmes and Data;
- Article 272 - Misuse of Devices;
- Article 270 - Computer Forgery;
- Article 273 - Serious Criminal Offences Against Computer Systems, Programmes and Data;
- Article 271 Computer Fraud;
- Article 284 - Infringement of the Personal Rights of an Author or Artist Performer;
- Article 285 Unauthorised Use of a Copyright Work or Performance by an Artist Performer;
- Article 286 - Infringement of Other Rights Related to Copyright;
- Article 27 Punishability for Acting Intentionally and Negligently;
- Article 28 – Intent;

- Article 34 – Attempt;
- Article 36 – Perpetratorship;
- Article 37 – Incitement;
- Article 38 – Aiding;
- Article 39 - Punishment of Accomplice and Participant.

Corporate liability is addressed by the Act on the responsibility of the legal persons for the criminal offences (OG 151/2003, 110/7, 45/11, 143/12):

- Article 1 - General provisions;
- Article 3 - The basis of responsibility of legal persons;
- Article 4 - The Responsibile person;
- Article 5 - The imputation of guilt of the responsible person to the legal person and in the Criminal Code by Article 20 - Manner of Committing a Criminal Offence.

Cyprus

Ratified Convention 185 in 2005

The relevant ratification laws are: Ratification Law No.26 (III)/2004, Ratification Law No.22 (III)/2004

Note: NGOs and SMEs do not have any obligation. They are covered (as any other legal person) when they involve in cybercrime activities

Czech Republic

Ratified Convention 185 in 2013

Czech Republic does not have comprehensive cyber-specific legal framework. Instead Cybercrime acts and procedures related to Convention 185 can be found in different piece of legislation such as the criminal code, the criminal procedure code, the Act on Criminal Liability of Legal Persons and Proceedings against Them, the Electronic Communications Act, the Act on the Police of the Czech Republic, Act on protection of classified information and security eligibility.

Note: Neither Convention 185 nor the implementing national legislations explicitly address NGOs and SMEs

Denmark

Denmark ratified the Convention in 2005, same year it entered into force.

Illegal access to information systems is criminalized in the following sections of the Criminal Code:

- Section 263(2) regarding wrongfully (unjustifiable) gaining of access to any data or programs of another person intended for use in an information system;
- Section 263a regarding wrongfully selling of or distribution to a wide group for commercial gain of a code or other means access to a non-public information system protected by a code or other special access protection and disclosure of a larger number of such codes or access means(concerns non-commercial systems);
- Section 301a regarding wrongfully (unjustifiable) obtaining or disclosure of codes or other means of access to information systems where access is reserved for paying members and protected by a code or other special access restriction (concerns commercial systems).

Illegal interception of computer data is criminalized in the Criminal Code Section 263(2) regarding wrongfully (unjustifiable) gaining of access to any data or programs of another person intended for use in an information system. Reference is made to the comments about Section 263(2) under illegal access to information (see under article 5).

Reference is made to the comments regarding article 5, since deletion, damaging, , etc., of computer data is criminalized by the same Sections of the Criminal Code as the Sections mentioned regarding article 5 and illegal system interference.

Illegal system interference is criminalized in the following sections of the Criminal Code:

- Section 193(1) regarding the causing of comprehensive interference with the operation of any public transport means, public postal service, telegraph or telephone service, radio or television broadcasting system, information system or service providing public utility supplies of water, gas, electricity or heating;
- Section 291(1) regarding destroying, damaging or removal of any property belonging to another person;[18]
- Section 293(2) regarding wrongfully preventing another person from disposing of an item in full or in part.

Production, distribution, procurement for use, import or otherwise making available or possession of computer misuse tools is not criminalized per se. However, the production, procurement etc. of devices or tools with features that can be misused for the use in criminal offences is punishable as incitement or

[18] Deleting, damaging, deteriorating, altering or suppressing computer data is covered by Section 291 of the Criminal Code. Denial of service attacks that prevents the normal use of or access to data systems by overload or by causing a break down is criminalized under Section 293(2).

aiding and abetting to an offence (Section 23) or attempting to commit an offence (Section 21). Hence, planning to design a program with the intention to use it in a cyber attack is punishable as an attempt to commit, inter alia, illegal interference according to section 293(2).

Computer-related forgery is criminalized in Section 171 regarding fraud. The section applies to forgery of electronic data. Hence, the offence covers every electronic data that form a verification, including e-mails, voice-mails etc.

Section 299 b of the Criminal Code deals with offences related to infringements of copyright and related rights, while sections 21 and 23 of the Criminal Code deal with attempt and aiding or abetting.

Estonia

Specific legislation on cybercrime has been enacted through the following instrument: Penal code. A number of paragraphs describe framework dealing with cybercrime:

Subdivision 2 Damage to Property

- § 206. Interference with computer data (Page 57 Penal Code)

  (6) Illegal alteration, deletion, damaging or blocking of data in computer systems is punishable by a pecuniary punishment or up to three years' imprisonment. [RT I, 12.07.2014, 1 - entry into force 01.01.2015]

- § 206(1). Unlawful removal and alteration of means of identification of terminal equipment (Page 57 Penal Code)

  (1) Unlawful removal or alteration, for commercial purposes, of the means of identification of terminal equipment used in an electronic communication network is punishable by a pecuniary punishment or up to three years' imprisonment.

  (2) The same act, if committed by a legal person, is punishable by a pecuniary punishment. [RT I 2007, 13, 69 - entry into force 15.03.2007]

- § 207. Hindering of functioning of computer systems (Page 57 Penal Code)

  (1) Illegal interference with or hindering of the functioning of computer systems by way of uploading, transmitting, deleting, damaging, altering or blocking of data is punishable by a pecuniary punishment or up to three years' imprisonment.

Division 2: Offences against all types of property:

- § 213. Computer-related fraud (Page 58 Penal Code)

  (1) Causing of proprietary damage to another person through unlawful entry, alteration, deletion, damaging or blocking of computer programs or data or other unlawful

interference with data processing operation for the purpose of proprietary benefit is punishable by a pecuniary punishment or up to three years' imprisonment.

Subdivision 3: Unlawful Use

- § 216. Preparation of computer-related crime (Page 60 Penal Code)

  (1) Supply, production, possession, distribution or making otherwise available of a device or computer program which is created or adjusted in particular for the commission of the criminal offences provided for in §§ 206, 207, 213 or 217 of this Code, or of the means of protection which allow to get access to a computer system with the intention of committing himself or herself or enabling a third person to commit the crimes provided for in §§ 206, 207, 213 or 217 of this Code is punishable by a pecuniary punishment or up to two years' imprisonment.

- § 217. Illegal obtaining of access to computer systems (Page 60 Penal Code)

  (1) Illegal obtaining of access to computer systems by elimination or avoidance of means of protection is punishable by a pecuniary punishment or up to three years' imprisonment.

  (2) The same act:

  i. if it causes significant damage; or

  ii. if access was obtained to a computer system containing a state secret, classified foreign information or information prescribed for official use only; or

  iii. if access was obtained to a computer system of a vital sector, is punishable by a pecuniary punishment or up to five years' imprisonment.

Finland

Specific legislation on cybercrime has been enacted through the following instrument:

The criminal code Finland: (Page 139): Chapter 34 - Endangerment (578/1995):

- Section 9(a) – Endangerment of data processing (368/2015)

A person who, in order to impede or damage data processing or the functioning or security of an information system or telecommunications system,

(a) a device or computer program or set of programming instructions designed or altered to endanger or damage data processing or the functioning of an information system or telecommunications system or to break or disable the technical security of electronic communications or the security of an information system, or

(b) an information system password, access code or other corresponding information belonging to another, or

(2) disseminates or makes available instructions for the production of a computer program or set of programming instructions referred to in paragraph (1) shall be sentenced, unless an equally severe or more severe penalty for the act is provided elsewhere in the law, for endangerment of data processing to a fine or to imprisonment for at most two years.

- Section 9(b) – Possession of a data system offence device (540/2007)

A person who in order to cause impediment or damage to data processing or to the operation or security of a data or communications system has possession of a device, computer program or set of programming instructions referred to in section 9(a), paragraph 1(a) or a password, access code or other corresponding information referred to in subparagraph b, shall be sentenced for possession of a data system offence device to a fine or to imprisonment for at most six months.

Chapter 35 - Criminal damage (769/1990) (Page 146):

- Section 3(a) – Damage to data (368/2015)

(1) A person who, in order to cause damage to another, unlawfully destroys, demolishes, hides, damages, alters, renders unusable or conceals data recorded on an information device or another recording or data in an information system, shall be sentenced for petty criminal damage to a fine.

(2) An attempt is punishable.

- Section 3(b) – Aggravated damage to data (368/2015)

- Section 3(c) - Petty damage to data (368/2015)

If the damage to data, when assessed as a whole, with due consideration to the minor significance of the damage or the other circumstances connected with the offence, is to be deemed petty, the offender shall be sentenced for petty damage to data to a fine.

Chapter 38 - Data and communications offences (578/1995) (Page 154)

- Section 8 - Computer break-in (368/2015) (Page 157-159)

France

Decree no 2006-580, 23 May 2006, publishing the Convention on cybercrime, adopted in Budapest on 23 November 2001.

Law no 2005-493, 19 May 2005, authorizing the approval of the Convention on cybercrime and its additional Protocol concerning the incriminations of acts of a racist and xenophobic nature committed through computer systems.

France has enacted laws regarding a wide range of cybercrime-related offences since 1988 which are regularly updated. As such, wilful and unauthorised access to an automated data processing system is considered an offence. Further, additional investigatory powers and tools have been provided to the

police to deal efficiently with cybercrime activities and a specialised court has been established. Finally, the cybercrime legislation sanction also involves several personal data-related offences, such as unauthorised alteration or processing.

Law No. 2018-133 of February 26, 2018 "On Various Provisions for Adaptation to European Union Law in the Field of Security" was adopted on February 15, 2018 and promulgated on February 26, 2018 (hereinafter "Network and information systems security law").

This law transposes the Directive (EU) 2016/1148 of 6 July 2016, known by the acronym "NIS" (National Information Security) and on measures to ensure a common high level of security of networks and information systems in the European Union. This Directive is largely based on the French legislation on information systems of vital importance and in particular the law n ° 2013-1168 of December 18, 2013 (called "law of military programming") which allows the security of the Operators of Vital Importance (OIV), that is to say operators of systems for which the breach of security or operation could significantly reduce the war or economic potential, the security or the capacity of survival of the Nation.

The transposition law on the security of networks and information systems thus makes it possible to extend to other categories of operators other than the simple OIVs a number of obligations with regard to the security of networks and information systems. . As such, the law recalls that the security of networks and information systems "consists in their ability to withstand, at a given level of confidence, actions that compromise availability, authenticity, integrity or confidentiality. data stored, transmitted or processed and the related services that such networks and information systems provide or make available. "

Thus, the network and information systems security law creates two new categories of actors namely on the one hand the Operators of Essential Services (OSE) and the Digital Service Providers (DSF).

Germany

Mostly within the frame of the international Budapest Convention on Cybercrime signed in 2001, the German legislator implemented more specific regulations to criminalise hacking, including the production, sale, and distribution of hacking tools. These regulations include:

- Section 202a of the German Criminal Code (Strafgesetzbuch) (StGB) (Data espionage / unauthorised obtaining of data).
- Section 202b of the StGB (Interception of data).
- Section 202c of the StGB (Preparing unauthorised obtaining or interception of data).
- Section 206 of the StGB (Violation of the postal and telecommunications secret).
- Section 303a of the StGB (Data tampering).
- Section 303b of the StGB (Computer sabotage).
- Section 44 of the BDSG (Violation of the Federal Data Protection Act with the intention to enrichment or to harm someone).

Greece

Ratified Convention 185 in 2017

The Greek Penal Code covers cybercrimes related to Convention 185

Note: NGOs and SMEs do not have any obligation. They are covered (as any other legal person) when they involve in cybercrime activities.

Hungary

Ratified Convention 185 in 2004

Cybercrime is covered by the criminal code (Act C of 2012).

Note: NGOs and SMEs do not have any obligation. They are covered (as any other legal person) when they involve in cybercrime activities.

Ireland

Cybercrime Bill – This Bill will give effect to those provisions of the Convention on Cybercrime 2001 not already provided for in national law. The legislation programme notes that preparatory work is underway, but there is no indication as to when the Bill will be published. Criminal Justice (Offences Relating to Information Systems) Act 2017 which creates a number of cybercrime offences including: accessing or interfering with the functioning of an information system without lawful authority (e.g. hacking); interfering with data without lawful authority intercepting the transmission of data without lawful authority; and using a computer programme, password, code or data for the commission of any of the above offences.

Italy

Italy has ratified the Convention in 2008. The Italian Criminal code and the special laws indicated below (on copyright and the protection of credit cards) cover all the offences under Articles 2-10 of the Convention. Under Articles 24 and 24bis of Legislative Decree no. 231 of 8 June 2001 provision has also been made for the liability of legal persons in case of commission of some cybercrimes when these have been committed for their benefit.

The Italian legal framework on cybercrime includes the following special laws:

a. Law on copyright (Law of 22 April 1941, no. 633) that also lays down criminal sanctions in relation to alleged violations on the Internet (Article 171 et seq.);
b. Criminal-law protection of credit cards under Article 55 of Legislative Decree of 21 November 2007 no. 231;
c. Italian Personal Data Protection Code – Legislative Decree no.196 of 30 June 2003, also laying down provisions on data retention (Article 132) including provisions on the requests from foreign investigative authorities (Article 132, paragraph 4-ter);
d. Electronic Communications Code (Legislative Decree 1 August 2003, no. 259) including the related obligations for Italian telecommunications companies pursuant to Article 96 (so-called mandatory assistance for purposes of justice).

Latvia

Latvia has ratified the Convention in 2007. Specific legislation on cybercrime has been enacted through the Electronic Communications Law (definitions) and Criminal Law:

- Illegal access – Article 144, Article 1931, Article 241, Article 243, Article 244, Article 2441, Article 245;
- Illegal interception – Article 144, Article 1931, Article 241, Article 243, Article 2441, article 245
- Data interference – Article 144, Article 1931, Article 241, Article 243, Article 244, Article 2441, Article 245 ;
- System interference – Article 144, Article 1931, Article 241, Article 243, Article 244, Article 2441, Article 245 ;
- Misuse of devices – Article 144, Article 1931, Article 241, Article 243, Article 2441, Article 245 ;
- Computer-related offences – Article 145, Article 1771;
- Computer-related fraud – Article 145, Article 1771,
- Offences related to infringements of copyright and related rights – Article 148;
- Section 70.1 of Criminal Law.

Lithuania

Ratified the Convention in 2004.

Specific legislation on cybercrime has been enacted through the following instrument: the Criminal Code of the Republic of Lithuania (chapter on crimes against security of electronic Data and Information Systems).

Only public administration bodies must report cybercrime threats, attacks and breaches to the relevant authorities. There is no such requirement for other (ie, private) entities.

Note: NGOs and SMEs do not have any obligation. They are covered (as any other legal person) when they involve in cybercrime activities.

According to the Code on Administrative Offences, failure to follow the Cybersecurity Law may result in administrative liability. However, if the term 'cybercrime' is interpreted in a broader sense, it could be considered a crime "against security of electronic data and information systems", as set out in the Criminal Code.

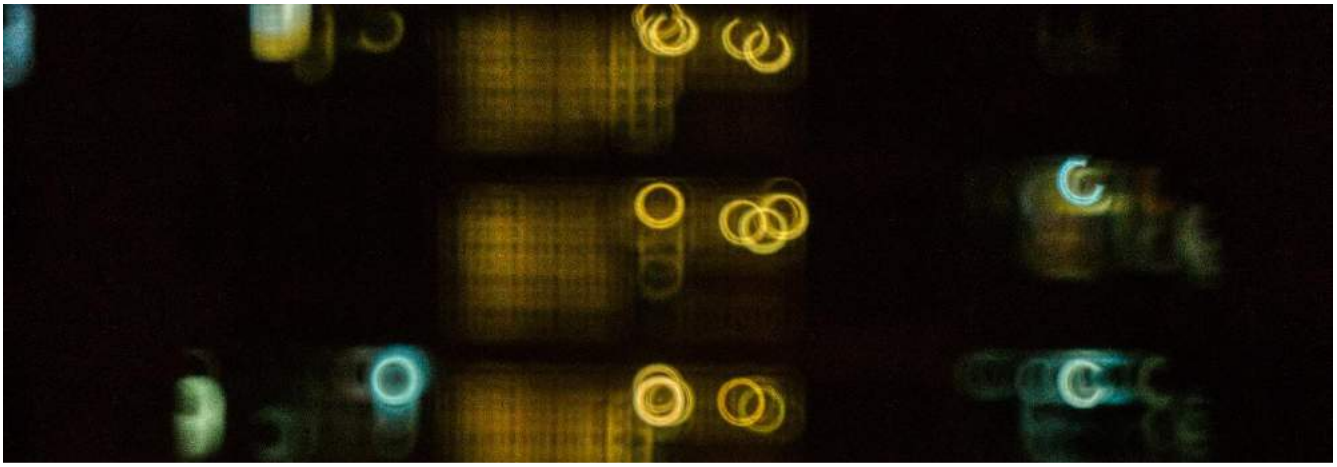
Luxembourg

On 18 July 2014, the Grand Duchy of Luxembourg ratified and implemented the Council of Europe Convention on Cybercrime, opened for signature in Budapest on 23 November 2001, and its additional protocol on Xenophobia and Racism signed in Strasbourg.

The Law also adapts the national substantive and procedural criminal law by amending the existing provisions of the Criminal Code and adding new offences (interception of computer data, misuse of devices, misuse of electronic signature).

Regulations in the Criminal Procedure Code on the prompt preservation of stored computer data and traffic data are also amended.

Act of 18 July 2014 concerning the approval of the Convention on Cybercrime of the Council of Europe, opened for signature in Budapest on 23 November 2001.



Malta

Maltese laws dealing with various aspects of cybersecurity include:

- the Criminal Code, which deals with cybercrime in the chapter entitled 'Of Computer Misuse';
- the Processing of Personal Data (Electronic Communications Sector) Regulations (Subsidiary Legislation 586.01);
- the Measures for High Common Level of Security of Network and Information Systems Order (Subsidiary Legislation 460.35); and
- the Electronic Communications Networks and Services (General) Regulations (Subsidiary Legislation 399.28).

Malta has also been a signatory to the Council of Europe Cybercrime Convention since 2001, which was ratified in April 2012.

The Malta Critical Infrastructure Directorate (CPID), which operates within the portfolio of the Ministry of Home Affairs and National Security (MHAS), issued a draft legal notice for public consultation regarding Malta's transposition of the EU Network and Information Security Directive (2016/1148/EC). This directive represents the first EU-wide rules on cybersecurity. Interested parties and stakeholders were invited to review the draft legal notice and provide their feedback and proposals by April 11th 2018. The directive was finally transposed into Maltese law through the Measures for High Common Level of Security of Network and Information Systems Order (Subsidiary Legislation 460.35) on the 6th of July 2018.

Netherlands

The Netherlands ratified the Convention in 2006, and it entered into force in 2007. Previous to the coming into force of the Cybercrime Convention the Netherlands already adopted Cybercrime Law in 1993, containing provisions of substantive and procedural law as well on international co-operation (CC-I). In order to be able to ratify the Cybercrime Convention 2001 the Computercrime Law (CC-II) was adopted in 2006 [1] Under preparation is a third law concerning substantive and procedural provisions (CC-III), to be sent to Parliament soon. In the meantime a number of subsequent amendments concerning cybercrime provisions were adopted.

Poland

Ratified the Convention in 2015

Specific legislation on cybercrime has been enacted through the Penal Code (Art 267; Art.268; Art.269)

The Penal Code:

- Article 267.

  § 1. Whoever, without being authorised to do so, aquires information not destined for him, by opening a sealed letter, or connecting to a wire that transmits information or by breaching electronic, magnetic or other special protection for that information shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years.

  § 2. The same punishment shall be imposed on anyone, who, in order to aquire information to which he is not authorised to access, installs or uses tapping, visual detection or other special equipment.

  § 3. The same punishment shall be imposed on anyone, who imparts to another person the information obtained in the manner specified in § 1 or 2 discloses to another person.

  § 4. The prosecution of the offence specified in §1 - 3 shall occur on a motion of the injured person.

- Article 268.

  § 1. Whoever, not being himself authorised to do so, destroys, damages, deletes or alters a record of essential information or otherwise prevents or makes it significantly difficult for an authorised person to obtain knowledge of that information, shall be subject to a fine, the penalty of liberty or the penalty of deprivation of liberty for up to 2 years.

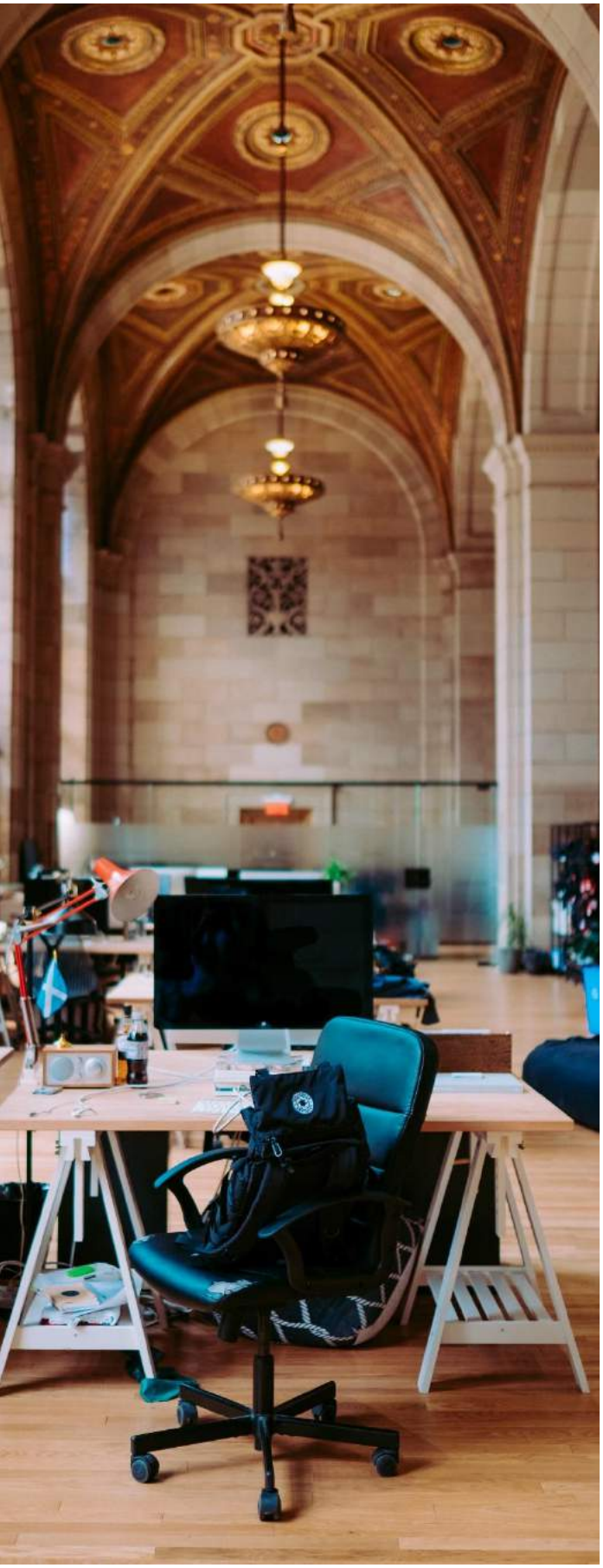
  § 2. If the act specified in § 1 concerns the record on an electronic information carrier, the perpetrator shall be subject to the penalty of deprivation of liberty for up to 3 years.

  § 3. Whoever, by committing an act specified in § 1 or 2, causes a significant loss of property shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years.

  § 4. The prosecution of the offence specified in § 1-3 shall occur on a motion of the injured person.

- Article 269.

  §1. Whoever destroys, deletes or changes a record on an electronic information carrier, having a particular significance for national defense, transport safety, local



government, or interferes with or prevents automatic collection and transmission of such information, shall be subject to the penalty of deprivation of liberty for a term of between 6 months and 8 years.

§ 2. The same punishment shall be imposed on anyone, who commits the act specified in §1 by damaging a device used for the automatic processing, collection or transmission of information.

Portugal

Cybercrime Convention - AR Resolution 88/2009 of 15 September;

Additional Protocol to the Cybercrime Convention - Resolution No. 91/2009 of 15 September;

Cybercrime Law - Law No. 109/2009 of 15 September.

Romania

In 2004 Romania ratified the Convention on Cybercrime (Law no 64/2004).

Law No. 161/2003 (Title III - Prevention and combating cybercrime) implemented accurately the Budapest Convention in Romanian legislation.

Romania is one of the few states which does not yet have a law on cyber security. A draft law on cybersecurity is currently under debate in Romania.

Slovakia

Ratified the Convention in 2008; it also entered into force in 2008 through the Criminal Code Act no 300/2005 Coll. and Code of Criminal Procedure Act no 301/2005 Coll.

Slovenia

Criminal code Slovenia:

- Abuse of Personal Data Article 143 (Page 60):

  (1) Whoever breaks into a computer database in order to acquire personal data for his or a third person's use shall be punished in accordance with the preceding paragraph.

  (2) Whoever publishes on the World Wide Web or enables another person to publish personal data of victims of criminal offences, victims of violation of rights and liberties, protected witnesses, which are contained in judicial records of court proceedings, in which the presence of the public or witness identification or protected witnesses and personal records thereof related to the court proceeding was not allowed according to the law or court decision, on the basis of which these persons may be identified or are identifiable, shall be sentenced to imprisonment for not more than three years.

- Violation of Material Copyright Article 148 (Page 62):

  (1) Whoever uses with the purpose to sell and without authorisation one or more copyrighted works or copies thereof of a high total market value shall be given a prison sentence of up to three years.

  (2) If the market value of copyrighted works from the preceding paragraph is very high, the perpetrator shall be given a prison sentence of up to five years

- Attack on Information Systems Article 221 (Page 91):

  (1) Whoever breaks into an information system, or illegally intercepts data during a non-public transmission into or from the information system, shall be sentenced to imprisonment for not more than one year.

  (2) Whoever makes an illegal use of data in an information system, or changes, copies, transmits, destroys, or illegally imports data in an information system, or obstructs data transmission or information system operation, shall be sentenced to imprisonment for not more than two years.

- Breaking into Business Information Systems Article 237 (Page 97):

  (1) Whoever, in the performance of business operations, without authority inserts, alters, hides, deletes or destroys any data or computer program, or otherwise breaks into a computer system in order either to procure an unlawful property benefit for himself or a third person or to cause damage to the property of another, shall be sentenced to imprisonment for not more than three years.

  (2) If the offence under the above paragraph has resulted in a large property benefit or a large loss of property and if the perpetrator intended to cause such loss of property or

to gain such property benefit, he shall be sentenced to imprisonment for not more than five years.

Spain

Section 42 Criminal Code (pg. 798 of the Cybersecurity Law Code).

Sweden

Sweden penal code:

- Section 8

A person who unlawfully obtains access to a communication which a postal or telecommunications firm delivers or transmits in the form of mail or as a telecommunication, shall be sentenced for breach of postal or telecommunication secrecy to a fine or imprisonment for at most two years

- Section 9

A person who, in a case not covered by Section 8, unlawfully opens a letter or a telegram or otherwise obtains access to something kept under seal or lock or otherwise enclosed, shall be sentenced for intrusion into a safe depository to a fine or imprisonment for at most two years.

- Section 9a

A person who, in a case other than as stated in Section 8, unlawfully and secretly listens to or records by technical means for

sound reproduction, speech in a room, a conversation between others or discussions at a conference or other meeting to which the public is not admitted and in which he himself does not participate, or to which he has improperly obtained access, shall be sentenced for eavesdropping to a fine or imprisonment for at most two years. (Law 1975:239)

- Section 9b

A person who employs technical means with the intention of committing a breach of telecommunication secrecy in the manner stated in Section 8 or to commit a crime as defined in Section 9a, shall be sentenced for preparation of such a crime to a fine or imprisonment for at most two years if he is not responsible for a completed crime. (Law 1975:239)

- Section 9c

A person who, in cases other than those defined in Sections 8 and 9, unlawfully obtains access to a recording for automatic data processing or unlawfully alters or erases or inserts such a recording in a register, shall be sentenced for breach of data secrecy to a fine or imprisonment for at most two years.

United Kingdom

- Computer Misuse Act 1990;
- Police & Justice Act 2006;
- Serious Crime Act 2015;
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Offences under the Fraud Act 2006 are applicable to a wide range of cyber-frauds by focussing on the underlying dishonesty and deception.

The nature of the offending will dictate the appropriate charges, and prosecutors may also consider offences under the Theft Act 1968, Theft Act 1978, Computer Misuse Act 1990, Forgery and Counterfeiting Act 1981 and Proceeds of Crime Act 2002.

NGOs and SMEs do not have any special obligations. They are subject to individual and corporate liabilities, as all other individual and legal persons when they involve in cybercrime activities.

EU Legislation

At a European Union (EU) level, cybercrime is a borderless problem, which consists of criminal acts that are committed online by using electronic communications networks and information systems and can be classified in three broad definitions:

1. Crimes specific to the Internet, such as attacks against information systems or phishing;
2. Online fraud and forgery. Large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code;
3. Illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia[19].

As pointed out in a joint communication of the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, in order to tackle cybercrime the EU and the Member States need strong and effective legislation to tackle cybercrime.

Moreover, they consider the Council of Europe Convention a binding international treaty that provides an effective framework for the adoption of national legislation and a basis for international cooperation

[19] European Commission, EU Legal and Policy Framework, *Organised Crime Dimension of Trafficking in Human Beings*, available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-humantrafficking/cybercrime/ index_en.htm.

in this field. In several pieces of EU legislation and policy documents it is the Convention is referred to as a legal benchmark for combating cybercrime, including attacks against information systems.[20]

The EU does therefore not call for the creation of new international legal instruments for cyber issues. However, because of the complex and global nature of cybercrime and the diversity of actors involved, the EU's involvement is necessary in order to have more coordinated regulation, coherent strategies and standards and effective cooperation and information sharing between all the actors involved.[21] EU legislation and policies therefore build on the Convention. For this purpose and in order to combat cybercrime the EU adopted several pieces of legislation and policies:

- Adopted:
  - ✓ Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L 218;
  - ✓ Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency [2004] OJ L 77.
- Indirectly related to cybercrime:
  - ✓ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L 201 as amended by Directive 2009/136/EC [2009] OJ L 77;
  - ✓ Council Framework Decision 2001/413/JHA of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment [2001] L 149/1.
- Proposed:
  - ✓ Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union COM(2013) 48 final;

[20] Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [2013] JOIN(2013) 1 final, p. 9, 15; See also Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L 218, Recital 15.

[21] Fostering cooperation, exchanging best practices and sharing of information is reiterated in almost all pieces of EU legislation and policy documents and therefore the key to cybersecurity according to the EU. Other suggestions made are providing adequate training (raising awareness about different national legal systems, possible legal and technical challenges of criminal investigations, distribution of competences between the relevant national authorities, etc.) to the relevant authorities in order to raise understanding of cybercrime and its impact. See for example Directive 2013/40/EU, Recital 28.

- Reports, communications, strategies, studies, resolutions:

  - ✓ Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems COM(2008) 448 final;
  - ✓ Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [2013] JOIN(2013) 1 final;
  - ✓ Communication from the Commission to the Council and the European Parliament on Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre [2012] COM(2012) 140 final;
  - ✓ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security' [2011] COM(2011) 163 final;
  - ✓ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" [2009] COM(2009) 149 final;
  - ✓ Communication from the Commission to the European Parliament, the Council and the Committee of the Regions - Towards a general policy on the fight against cyber crime [2007] COM(2007) 267 final;
  - ✓ Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - Creating a Safer Information Society by improving the Security of Information Infrastructures and Combating Computer-related Crime [2000] COM(2000) 890 final;
  - ✓ European Commission, Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft, 11 December 2012;
  - ✓ RAND Europe, Feasibility study for a European Cybercrime Centre, February 2012;
  - ✓ RAND Europe, Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime: Final Report, June 2011;
  - ✓ European Parliament Resolution on supporting consumer rights in the digital single market (2014/2973(RSP));
  - ✓ European Parliament Resolution on a Cybersecurity Strategy of the European Union: an open, safe and secure cyberspace (2013/2606(RSP));
  - ✓ European Parliament Resolution on the suspension of the TFTP agreement as a result of US National Security Agency surveillance (2013/2831(RSP));
  - ✓ European Parliament Resolution on the second report on the implementation of the EU Internal Security Strategy (2013/2636(RSP));
  - ✓ European Parliament Resolution on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy (2013/2682(RSP));
  - ✓ European Parliament document on Cyber security and defence (2012/2096(INI));
  - ✓ Information society, eEurope 2002: security of infrastructures, combating computer-related crime (2001/2070(COS)).

- Data protection framework

  - ✓ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
  - ✓ General Data Protection Regulation

- Outside the scope of this report:

  - ✓ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
  - ✓ Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA [2012] OJ L 26.

A close look at the documents mentioned above may lead to the conclusion that there is no comprehensive legal framework governing cybercrime at EU level, only a patchwork. The fragmentation mentioned before is visible also at EU level, which is not entirely surprising as the aim of the EU is not to create a new legal framework relating to cybercrime, but build on the Convention.

Like the Convention, EU legislation is binding to its Member States.

Unlike the Convention however, apart from combating cybercrime, EU legislation in the area of cybercrime generally has another mayor goal, namely contributing to the smooth functioning of the EU's internal market. EU policy documents including reports, communications, strategies and studies are intended to clarify the EU's vision, roles, responsibilities and actions in the area of cybercrime and are generally not legally binding.

As may be seen in the list above, certain pieces of EU legislation and policy documents are specifically on cybercrime while others contribute to the fight against cybercrime.[22]

[22] The list mentioned above is non-exclusive, there are several EU legislative acts which might also contribute to the fight against cybercrime. For example, Council Framework Decision 2008/841/JHA is on the fight against organised crime, cybercrime can also be organised crime and if that is the case, according to Directive 2013/40/EU penalties should be more severe where an attack against an information system is committed by a criminal organisation. See Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L 218, Recital 13.

7 | ADOPTED LEGISLATION

Adopted legislation

a. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L 218;

b. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency [2004] OJ L 77.

Directive on attacks against information systems

Gaps and differences in Member States' legislation and procedures hinder the fight against cybercrime and complicate effective police and judicial cooperation in this area. The objective of the Directive on attacks against information systems[23] is to harmonise criminal law of the Member States in the area of attacks against information systems by subjecting attacks against information systems in the EU to effective, proportionate and dissuasive criminal penalties and to improve and encourage cooperation between competent authorities (Art. 13 and 14).

According to the text of this Directive, attacks against information systems are increasingly dangerous and recurrent and are accompanied by the development of increasingly sophisticated methods. These attacks can be critical to Member States or to particular functions in the public or private sector. For these reasons, measures against cyber attacks should be complemented by stringent criminal penalties reflecting the gravity of such attacks.

The Directive criminalises illegal access to information systems (Art. 3), illegal system interference (Art. 4), illegal data interference (Art. 5), illegal interception (Art. 6) and making available of tools for committing offences (Art. 7)62 as well as aiding and abetting and the incitement and attempt to commit an offence (Art. 8) and provides that these offences are punishable by criminal penalties (Art. 9)

Transposition of EU legal instruments into national legislation

Austria

Framework Decision 2005/222/JHA on attacks against information systems has been incorporated into Austrian law via Criminal Law Amendment Act 2008, Federal Law Gazette I No 109/2007. The provisions of the Criminal Law Amendment Act 2015 that entered into force on 1 January 2016 transpose Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

Legal persons may be held criminally liable for offences committed by individuals in management positions (decision makers) or by individuals under their authority (employees). However, in the latter case, they may be held liable only if they failed to provide sufficient supervision or control. In order for a legal person to be held liable for a criminal offence, the offence must have been committed for its benefit or in breach of its duties. If the constituent elements described are present, it is therefore also

[23] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L 218.

possible for legal persons to be held criminally liable for cybercrime. The penalty imposed generally takes the form of a fine, which is calculated by multiplying the number of daily rates imposed (from 40 to 180) by the amount of the applicable daily rate (calculated on the basis of revenue).

The law is also intended to penalise new manifestations of computer crime hitherto not fully covered by criminal law (e.g. payment card fraud involving 'phishing' and 'skimming' - Section 241h Criminal Code).

The framework of cybersecurity is dependent on the adoption into domestic law of the NIS Directive, which was planned for May, 2018 but is still delayed. Since the NIS Directive has not been implemented, there is not officially designated "national CSIRT". However, the CERT.at body does exist, and represents Austria at FIRST, so it can be considered to meet basic requirements of the NIS Directive (unofficially). See here: https://www.cert.at/services/blog/20180731155524-2252_en.html (summary at end).

Belgium

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Electronic Communications Act
- Law on Electronic Signatures and certification services
- Law on Certain legal aspects of the Information Society
- Law on the protection of private life with regard to the processing of personal data.

Belgian ePrivacy laws are contained in the Code of Economic Law (the "CEL") and the Royal Decree of 4 April 2003 on the sending of advertising by e-mail (the "RD"), with regard to e-mails, all of which implemented Article 13 of the Privacy and Electronic Communications Directive.

Belgian law has been amended to implement some, but not all, the amendments to the Privacy and Electronic Communications Directive.

The cookie requirements in the Privacy and Electronic Communications Directive have been implemented into Belgian law. It is only possible to use cookies if:

(i) clear and specific information has been provided to the individual regarding the purposes of the data processing and their rights, all in accordance with the general requirements of the DPA; and
(ii) the individual provides consent after receiving this information. These restrictions do not apply to cookies that are strictly necessary for a service requested by an individual. Last, users must be allowed to withdraw their consent free of charge.

As in most other Member States, the law does not specify how consent from users should be obtained. This matter has to be clarified through regulatory guidance. The Commission reviewing the draft bill opined that consent may not be obtained through current browser settings.

It also released a recommendation in February 2015 which provides detailed guidance regarding the use of cookies, including the way to obtain valid consent. This requires an affirmative action by the user

who must have a chance to review the cookie policy beforehand. This policy must detail each category of cookies with their purposes, the categories of information stored, the retention period, how to delete them and any disclosures of information to third parties.

- Law of 30 June 1994 on copyright

- Law of 15 May 2007 on the punishment of counterfeiting and piracy of intellectual property rights (updated February 25, 2011)

- The law of 28 November 2000 on computer crime includes a series of provisions designed to fight against computer crime. The Penal Code introduces four new offenses: forgery in the computer field (Article 210 bis), computer fraud (Article 504 ter.), data manipulation (Article 550 bis.) and piracy (article 550 ter.). These are in addition to previously identified offenses, including child pornography and paedophilia (art. 383 bis), racism and holocaust denial (art. 444), spamming (art. 496), and certain violations of intellectual property rights. Articles 550bis and 550ter of the Penal Code also covers the use of cyberspace for terrorist purposes.

Bulgaria

The Council of the European Union's Bulgarian presidency has released a progress report on the draft ePrivacy Regulation ahead of a council meeting June 8. The report offers several updates to the ePR, including its scope and link to the EU General Data Protection Regulation, the processing of electronic communications content and metadata, the protection of terminal equipment information, privacy settings, data retention, and direct marketing communications, among others. The processing of metadata and corresponding balance between privacy and innovation "has been one of the main concerns of the Member States," and, the report notes, the "topic remains one of the most sensitive issues." The presidency also "introduced significant changes to Article 10 on privacy settings," most notably that providers of software will be "only obliged ... to inform end-users about these settings" rather than required. The regulation seems to be not published yet.

- Electronic Commerce Act: Commercial Communication Article 5:

    (1) Commercial communication within the meaning of this Act is advertising or any other communication, designed to promote, directly or indirectly, the goods, services or reputation of the person, performing a commercial or craft activity or exercising a regulated profession.

    (2) The independent usage of the following does not constitute commercial communication within the meaning of Article 1:

        i. information, assuring direct access to the person's activities, like the name of its domain or e-mail address;

        ii. messages for the goods, services or for the reputation of the person, the information for which has been collected in an independent manner with no payment made for this.

(3) The commercial communication that is a part of or constitutes an information society service must meet the following requirements:

i. to be easily identifiable as commercial ones;

ii. to enable clear identification of the natural or legal persons on whose behalf it has been made;

iii. to define clearly and unambiguously the conditions for participation in promotional offers such as discounts, premiums and gifts, if such are included;

(4) to assure easy access to clear and unambiguous conditions for participation in competitions and games with declared prizes, if they contain such information;

(5) to contain any other information, stipulated in other statutory instruments.

- Unwanted commercial communication - Article 6.:

(1) A service provider who sends unwanted commercial communication via e-mail without addressee's preliminary consent shall be under the obligation to provide clear and unambiguous identification of the commercial communication as an unwanted one yet on the entrance with the receiver.

Croatia

The Police Directive has not yet been transposed into law, although new draft law has been submitted.

The Electronic Communications Act, 2008 sets up the laws to be followed by communications service providers.

The Information Security Act, passed in 2007, empowered the creation of the Information Systems Security Bureau (ZSIS). It operates under the Office for National Security.

The Act applies to legal and natural persons who gain access to or handle classified and unclassified data" (Article 1(3)).

In the case of an SME/NGO having an "information system" that uses classified data of "of CONFIDENTIAL, SECRET and TOP SECRET level", a security accreditation process is mandated by law. (See Article 12 of the Information Security Act). In the case of usage of classified information, the Regulation on Information Security Measures must also be followed.

The CERT.ah was established through the Information Security Act, 2007. (See Article 20). This is also per the NIS Directive, which has been transposed into the Croatian National Cyber Security Strategy (2015).

Cyprus

Electronic Commerce Law (156(I)/2004) - regulates the following online activities: online information services; online advertising and marketing; online selling of products and services; and online entertainment services

- the Law for the Protection of Confidentiality of Private Communications (92(I)/1996) the Law Regulating Electronic Communications and Postal Services 112(I)/2004, last amended by Law No. 76(I)/2017 prohibits the unauthorized interception of any private communication, subject to certain exceptions.

- the Legal Framework for Electronic Signatures and for Relevant Matters Law 188(I)/2004 effectively establishes the legal framework governing electronic signatures and certain certification services for the purpose of facilitating the use of electronic signatures and their legal recognition

- Cyprus published a new data protection law on July 21, 2018 to implement the GDPR (note- the law is available only in Greek), but there is no indication of transposing the E-privacy Directive.

The NIS Directive has been implemented in Cyprus on 5 April 2018: implementing act is 'Network and Information Security Law of 2018 (Law 17(I)/2018. Operators must notify the competent authority without undue delay of any incident having a substantial impact on the provision of the services. This could apply to SMEs when they involve in critical service offering.

Czech Republic

- Act on Cyber Security No. 181, 2014:

This Act regulates rights and obligations of natural and legal persons and competence and power of public authorities in the field of cyber security.

It covers cybersecurity issues not related to convention 185

This Act could apply to NGOs and SMEs only if they involve in providing critical services

Established two CERTs: 1) a Government Computer Energency Response Team (GovCERT.ZE) and 2) a national Computer Security Incident Response Team (CSIRT.CZ)

CERT & CSIRT Capacity Building Strategy defined in the Action Plan 2015-2020

Most of the Czech businesses, including SMEs deal with the National CSIRT Team

- National Cyber Security Strategy (2015-2020)

Recognized the need for cooperation among CERT and CSIRT teams at national and international level

Note: Even though SMEs can be required to report cybersecurity incidents to CERT (as indicated below), there is no indication of how CERT & NGOs interact

Electronic Communications Act 2015 transposes the ePrivacy Directive into Czech law. For instance, paragraph 3 of Article 89 of the Electronic Communications Act is a direct copy of the ePrivacy Directive's Article 5 (3)

The Electronic Communications Act 2005 covers issues beyond the Convention 185. It transposes Directive 2002/19/EC of the European Parliament and of the Council on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive). This Act regulates the market in the electronic communications area.

Czech NIS Directive amended the Act on Cyber Security No. 181, 2014 by Act No. 205/2017 Coll. to implement NIS Directive. The Act applies to SMEs providing essential services. In this case, SMEs have the obligation to take preventive cybersecurity measures and to report incidents to the national CERT or the National Cyber and Information Security Agency.

Denmark

The NIS Directive has been transposed into the Danish Cyber and Information Security Strategy 2018-2021

The E-Commerce Act was passed in 2004. The law requires providers of services in the information society to clearly provide information about themselves and their contractual obligations.

Estonia

Estonia has an officially recognized national CERT known as CERT-EE. The Estonian Information System Authority has developed as a result of the reorganisation and merger of several institutions.

Over the years, the Estonian Informatics Fund, established in 1990 in the jurisdiction of the Government Office, has become a governmental authority in the jurisdiction of the Ministry of Economic Affairs and Communications. --> established by means of law

Information regarding the IP laws was found in the Penal Code:

Chapter 14: Intellectual Property:

- § 222(1). Infringement of copyright in computer system (Page 61 Penal Code)

(1) Knowing infringement of proprietary rights of a holder of copyright or related rights by means of a computer system in professional or economic activities, if the amount of gains or damage caused by the infringement exceeds the amount of twenty minimum daily rates and it does not contain the necessary elements provided for in § 222, is punishable by a pecuniary punishment or up to one year of imprisonment.

- § 223. Unlawful direction of works and objects of related rights towards public (Page 62 Penal Code)

(1) Unlawful public performance, showing, transmission, re-transmission or making available to the public of works or objects of related rights in professional or economic activities, if the amount of gains or damage caused by the infringement exceeds the amount of twenty minimum daily rates, is punishable by a pecuniary punishment or up to one year of imprisonment.

- § 225. Removal of technical protective measures and information (Page 62 Penal Code)

(1) Unlawful alteration or removal of technical protective measures preventing the infringement of copyright or related rights or electronic information on the exercise thereof, or manufacture, use, making available as a service or distribution of means or devices used solely or mainly for removal of the protective measures, if the act was committed outside personal use in order to receive benefits, is punishable by a fine of up to 100 fine units.

Payment Institutions and E-money Institutions Act (seems to be the closest to electronic commerce law) In this act cybersecurity is not mentioned specifically. However, it is mentioned the conditions which apply to the institutions to be able to issue e-money (§ 2- 10)

Finland

Act on Electronic Signatures: Section 19 (Page 7): A certification-service-provider providing certificates to the public may collect personal data necessary for the issuing and maintenance of the certificate only directly from the signatory. With regard to a certification-service-provider providing qualified certificates to the public, further provisions on the issuing of a qualified certificate, the registers to be maintained and the information to be maintained are contained in chapter 2 of this Act. When verifying the identity of a person applying for a certificate, the certification service- provider may require him to provide his personal identity number.

Act on the Protection of Privacy in Electronic Communications: Chapter 2 - Protection of privacy and confidentiality of messages (Page 5), Section 6 - Protecting messages and identification data, Section 13f (125/2009) - Special restrictions to the right to process data in cases of misuse (Page 14), Section 19 - Obligation to maintain information security (Page 22)

France

The EU Directive on the Security of Network and Information Systems (NIS) came into force in France on 25 May 2018. The directive aims to raise levels of the overall security and resilience of network and information systems across the European Union.

Aside from the violation of automated data processing systems, numerous cyber activities are criminal offences, including:

- internet protocol spoofing;
- identity theft;
- hacking;
- child soliciting; or
- any act inciting terrorism.

Many companies obtain insurance for security breaches. This generally involves an inspection and upgrade of the company's cybersecurity measures, along with an employee training session. Insurance both protects against potential damages resulting from cyberattacks and breaches and provides strategic support when under direct cyberthreat or cyberattack.

Such insurance is common only for companies that are likely to be subject to cyberattacks or which business is directly dependent on data security.

Companies are required to keep records of security breaches that involve personal data theft or corruption.

Art. 323-1 à 323-7 Penal Code defines as crimes all offences against the confidentiality, integrity and availability of computer data and systems, including illegal access (art. 323-1 al. 1), data interference (art. 323-1 al.2 and 323-3), system interference (art. 323-2), as well as misuse of devices (art. 323-3-1 CP).

The "Trust in the Digital Economy Act" (the "Act") implemented Article 13 of the Privacy and Electronic Communications Directive on 21 June 2004. The Act is now codified under Article L. 34-5 of the Postal and Electronic Communications Code and is mentioned in Articles L. 222-16 and 223-7 of the Consumer Code.

The Ordinance no. 2011-1012 of 24 August 2011 (the "Ordinance"). The Ordinance implements the amendments to the Privacy and Electronic Communications Directive.

The current French Data Protection Act, as amended by the Ordinance, requires data controllers to obtain prior consent from users to store or access cookies after having provided the user with information about the purposes for which cookies are used and about the means to prevent such storage or access

The Ordinance explicitly recognises that such consent may result from appropriate settings on a user's connection device (such as an internet browser) or from any other applications placed under a user's control, and the CNIL's guidance provides that an implied consent to cookies is sufficient, provided that such consent is informed and prior (CNIL, 5 December 2013, no. 2013-378).

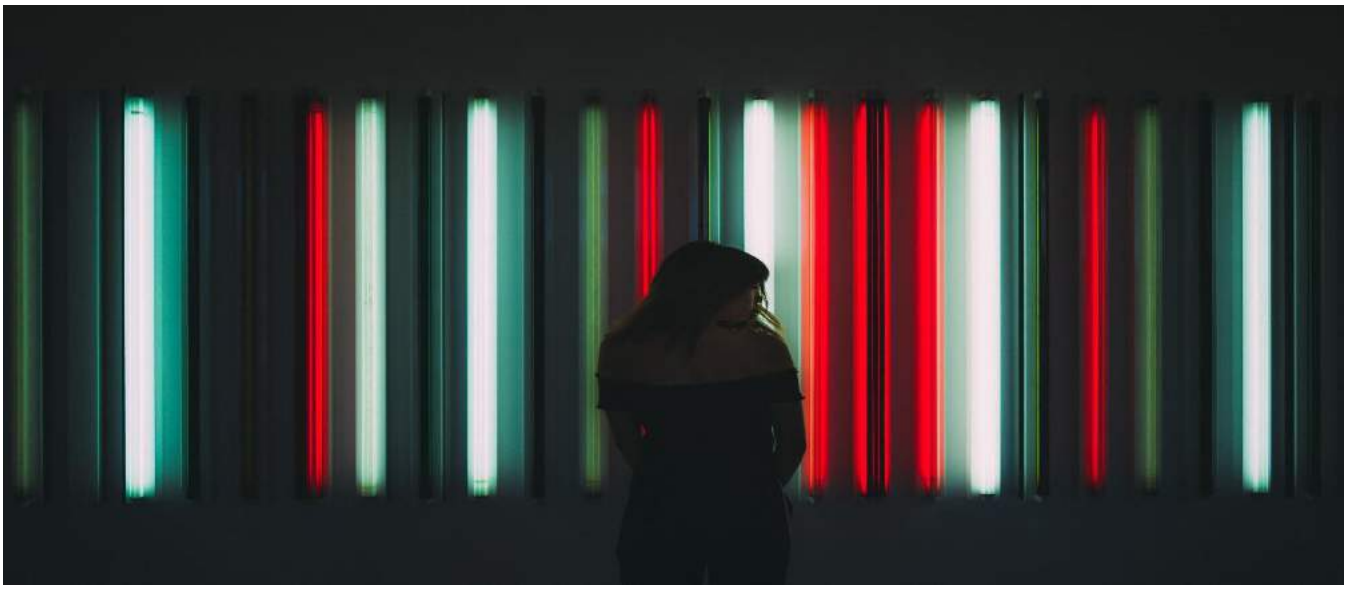
Prior information and consent requirements do not apply where the cookie's sole purpose is to enable or facilitate the communication (i.e. technical cookies) or where the cookie is strictly necessary to provide an online communication service requested by the user (e.g. cookies concerning language preferences).

The CNIL considers that the use by employees of personal devices at work presents a risk of breach of privacy for the employee and the security of his or her data. The relevant data controller must take technical and practical measures to ensure the protection of employees' privacy and data.

The CNIL published Resolution No. 2017-012 of 19 January 2017 amended by Resolution No. 2017-190 of 22 June 2017 adopting a recommendation on passwords.

The requirements of the CNIL are related to password authentication, authentication security, password storage and password renewal or recovery.

Decree No. 2017-428 of 28 March 2017 concerns individuals and companies providing private electronic correspondence services, and it imposes a time limit of a year for the periodicity of the collection of the express consent of the user.



Germany

- Article 13(7) of the Telemedia Act (Telemediengesetz) (TMG), each telemedia provider (for example, each provider of a website, a web-application and smartphone app) must ensure through appropriate, economically proportional arrangements that unauthorised access is not possible. The requirements regarding the IT security measures that a company must implement are not detailed. In most cases, the legislator requires that the undertakings comply with or at least consider the art of IT security. This is assessed on a case-by-case basis and is explained in more detail below.

- Section 25a of the Banking Act (Kreditwesengesetz) (KWG), each bank licence holder must implement an appropriate risk management. According to administrative instructions of the Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) which are laid down in the Minimum Requirements For Risk Management (Mindestanforderungen an das Risikomanagement (MARisk), this risk management must also take into account requirements regarding IT security.

- Section 33 of the Securities Trading Act (Wertpapierhandelsgesetz) (WpHG), a securities service companies must fulfil the same requirements as a bank with respect to section 25a of the KWG (see above).

- Minimum requirements for the security of internal network payments (Mindestanforderungen an die Sicherheit von Internetzahlungen) (MaSI) are specified by the BaFin and the European Banking Authority (EBA).

- Section 109 of the Telecomunication Act (Telekommunikationsgesetz) (TKG), each provider of a public telecommunications network and/or a telecommunication service must implement adequate technical measures to prevent hacking or other disturbances, appoint a security officer and adopt a IT-security concept. The security concept must be revealed to the Federal Network Agency (Bundesnetzagentur) (BNetzA). In all of these regulations the requirements regarding the IT security measures that a company must implement are not detailed. In most cases, the legislator requires that the undertakings comply with or at least consider the art of IT security. This is assessed on a case-by-case basis. 5. German IT Security Act (IT-Sicherheitsgesetz) of 25 July 2015 has amended a number of laws, in particular the German Telemdia Act, the German Telecommunications Act, the German Gederal Data Protection Act and the Act on the Federal Office for Information Security (Gesetz uber das Bundesamt fur Sicherheit in der Informationstechnik)

CERT-Bund <www.cert-bund.de> was established in 2012 and is responsible for warning systems and coordinating incident response measures for German federal government authorities. It works closely with German CERT alliances and state-level CERTs to provide wider coverage.

The German legislator did not implement the provisions of the ePrivacy Directive but instead relied upon its existing rules in the Telecommunications Act (Telemediengesetz, TMG). Cookies fall within the scope of §§ 12, 13 II and 15 III TMG, which operate on the lex generalis and lex specialis principles. The general rule of §§ 12 and 13 II TMG stipulates that personal data may be collected and processed if the user has given his or her consent. The specific rule of § 15 TMG is a derogation from the general rule

and concerns 'utilization data', which is defined as characteristics which identify the user, details on the start and end of usage, and importantly, details on the content and/or services that are used by the user. When a profile of this data is made and this profile undergoes pseudonymisation, §15 III TMG provides that informing the user and giving him or her the possibility to opt-out is sufficient to safeguard the user's privacy.

Trade secrets. German law requires that information not be easily accessible to receive trade secret protection (Bundesgerichtshof (BGH) Federal Court of Justice Feb. 26, 2009, no. I ZR 28/06, recital 13). To ensure trade secret protection, organizations should: take sufficient organizational and technological measures to protect their information, although no particular data security measures are required; and prevent unauthorized third party access to their trade secrets.

Companies that have implemented a works council, typically German workplaces with more than five employees, must consider co-determination rights when developing information security policies and controls. Specifically, the Works Constitution

Act (Betriebsverfassungsgesetz) (BetrVG) provides workers with co-determination rights regarding employers' use of technologies that monitor employee behavior or performance. These obligations likely affect technical controls that scan communications or network traffic, including anti-virus software, firewalls, intrusion detection and prevention programs, and data loss prevention tools.

Other German laws may affect typical information security policy areas, including: „ Employee monitoring and personal use. Employers in Germany are free to choose whether they allow or prohibit personal use of an organization's email, telephone, internet access, or other communications facilities. However, employers who permit personal use may be subject to communications secrecy laws. In both cases, the BDSG likely limits any monitoring without consent, and data protection authorities generally question consent as a legal basis in the employment context. „ Bring your own device to work. Organizations with a works council that support bring your own device to work (BYOD) must establish a works council agreement for related policies and procedures. Organizations should also consider BDSG obligations to protect personal data when: z establishing BYOD policies; z entering into BYOD agreements with individuals; and z selecting BYOD technical controls such as data segmentation, encryption, and remote wiping capabilities.

There is no case law or a regulatory statement specifying a preferred standard. The standards only specify what could be considered as the state of art in IT security. As the law does not oblige [companies] to comply with the state of the art of IT security but only obliges to consider it (see, for example, section 13(7) of the TMG), the company can choose which parts of the standard it wants to implement. German IT Security Law - changes to the Telemedia Act - Website operators and other service providers must make sure that no one can access the IT systems they use without authorization and that their systems are secured against unauthorized access to personal (customer) data and against disruptions caused by external attacks. To this end they must implement the relevant state-of-the art technical and organizational measures, which include using secure encryption procedures. However, a service provider will only be required to implement the corresponding measures insofar as this is "technically possible and can be reasonably expected" of the provider.

The statutory regulation has been intentionally designed to be flexible, which makes it difficult to assess specifically which measures are expected from which providers. Hence, some votes have considered the regulation as unconstitutional on the grounds of its indeterminate obligations. Here it is particularly important to keep an eye on further development, especially on how responsible state authorities will be in terms of implementing the Act in practice. It is also not yet clear whether this new statutory regulation is intended to regulate market conduct, in other words it is as yet not known whether warnings can be issued to competitors and/or consumer protection associations for violating the law.

Greece

- Regulation for the Assurance of Confidentiality in Electronic Communications No. 165/2011: the law obliges all organizations involved in providing electronic communications networks and/or services to have and to implement a Security Policy for the Assurance of Communications Confidentiality. The law could be applicable to SMEs which involve in the provision of electronic communications networks and/or services as defined in the law.

- LAW 3471 Protection of personal data and privacy in the electronic communications sector transposes E-privacy Directive into Greek law

1. Presidential Decree131/2003, adopted to implement the E-commerce Directive (Directive 2000/31)

2. Consumer Code of Ethics for E-Commerce

According to this code of conduct, E-Commerce companies (including SMEs) must:

- Make every effort to use the appropriate tools and measures according to their category and type of business and the type of data they use and apply all appropriate measures to provide the legally envisaged security of electronic transactions

- Use appropriate technical and organizational measures to ensure the confidentiality of the data they collect and process to the extent reasonably foreseen and according to the nature of the products and services they provide

- NIS Directive has not been implemented yet
- The National Strategy aims to harmonize NIS but not transposed into law

Hungary

Act No C/2003 on Electronic Communications:

- Covers natural persons, legal entities or other organisations without legal entity and their leading officers performing activities or providing services of electronic communications activities.
- SMEs who involve in these services may have cybersecurity-related obligations such as to take the necessary technical and organisational measures Article 155.

Act No C/2003 on Electronic Communications. SMEs who involve in these services may have certain cybersecurity-related obligations

Act CVIII of 2001 on certain issues of electronic commerce services and information society services states that holders of a right protected by the Copyright Act--- which has been infringed by the information made accessible by the service provider may request the removal of the information infringing. Article 13 (1)5

Act CVIII of 2001 on certain issues of electronic commerce services and information society services

- The Act covers SMEs which involve in delivery of 'Information society service'
- From cybersecurity perspective, SMEs which involve in delivery of 'Information society service' have the obligation give general information about the level of security of the systems applied for information processing, the risk factors to the recipient of the service and the protection measures to be taken by the recipient of the service.

NIS Directive implemented by:

- Act 134 of 2017 on modifying certain interior related tasks and corresponding laws, and
- Government Decree 394/2017 (XII.13) (note: law not available in English)
- Service Providers must immediately report significant incidents in relation to network and information systems that have significant effects on their services. This obligation could be applied to SMEs, who engage in critical service provision.

Ireland

Data-Sharing and Governance Bill – This Bill provides a legal mechanism to facilitate lawful data-sharing and data–linking for public bodies, and define standards for data governance and security to be followed in any data sharing or data-linking activities.

Cyber Security Bill – This Bill will provide general powers to the Minister in respect of Cyber Security to transpose the Network and Information Security (NIS) Directive, which is the first piece of EU-wide legislation on cybersecurity. Preliminary work is underway in the drafting of this Bill. Member States are required to transpose the NIS Directive by 9 May 2018.

Italy

Italy has implemented EU Directive 2013/40/EC on attacks against information systems, which approximates its member states' criminal law regarding:

- illegal access to information systems;
- illegal system interference;
- illegal data interference;
- illegal interception, incitement, aiding and abetting; and
- attempts to commit one of the aforementioned offences.

Italian law establishes that providers of electronic communication services (eg, telecoms service, Voice over Internet Protocol and email service providers) must retain telephone and electronic communication traffic data, but not the content of communications, for 72 months from the date of the communication for the purpose of detecting and suppressing criminal offences.

Ratified the Convention in 2008.

The Italian Criminal code and the special laws indicated below (on copyright and the protection of credit cards) cover all the offences under Articles 2-10 of the Budapest Convention.

Note: NGOs and SMEs do not have any obligation. They are covered (as any other legal person) when they involve in cybercrime activities.

Under Articles 24 and 24bis of Legislative Decree no. 231 of 8 June 2001 provision has also been made for the liability of legal persons in case of commission of some cybercrimes when these have been committed for their benefit.

The legal framework on cybercrime includes the following special laws:

- Law on copyright (Law of 22 April 1941, no. 633) that also lays down criminal sanctions in relation to alleged violations on the Internet (Article 171 et seq.);

- Criminal-law protection of credit cards under Article 55 of Legislative Decree of 21 November 2007 no. 231;

- Italian Personal Data Protection Code – Legislative Decree no.196 of 30 June 2003, also laying down provisions on data retention (Article 132) including provisions on the requests from foreign investigative authorities (Article 132, paragraph 4-ter);

- Electronic Communications Code (Legislative Decree 1 August 2003, no. 259) including the related obligations for Italian telecommunications companies pursuant to Article 96 (so-called mandatory assistance for purposes of justice).

The NIS Directive has been transposed through Legislative Decree 65/2018) on May 16th, 2018.

The Ministry of Economic Development has been mandated by the Legislative Decree n.70, May 28th 2012, which transposes the 2009/140/EC Directive, to implement the national CERT (CERT-PA) https://www.cert-pa.it/

On 4 September, the Legislative Decree no. 101 of 10 August 2018 (the "Decree") for the national implementation of General Data Protection Regulation (EU) 2016/679 (the "GDPR") has been published in the Official Journal. The approach of the legislator was to maintain the structure of former Legislative Decree 196/2003 (the "Privacy Code") which, however, has been extensively amended and integrated, and now contains only some residual provisions in addition to those of the GDPR which are directly applicable. The Decree will enter into force on 19 September 2018.

Law no. 124 of 3 August 2007 on "Information System for the security of the Republic and new rules on State secrets" (Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto), Art 31-34.

Data Protection Code, Art. 160 (4). --> the DPA is responsible for providing ongoing and ex post oversight on the services. It has the right to initiate inspections and to access classified materials. (FRA Report 2017)

Legislative Decree No. 7 of 18 February 2015 converted, with amendments by law of 17 April 2015, No. 43, Art. 8.gives AISE authority to perform its tasks also by electronic means (assetti di ricerca elettronica). The law does not provide more details about these surveillance means; it only states that it should be exclusively directed abroad.

Code of criminal procedure (Codice di procedura penale), Art. 266 and following and Italy, Implementing norms (norme di attuazione), Art. 226. --> In Italy, requests for targeted interception measures need to be authorised by the Prosecutor General of Rome.

Latvia

- ''Law on the Security of Information Technologies'' (2011) applies
- Latvia follows EU policy in the field of cybersecurity. No specific international standards have been adopted;
- Electronic communications merchants must report personal data threats, attacks or breaches to the Data State Inspectorate;
- There is no general obligation to report cybercrime threats, attacks or breaches to the relevant authorities;
- Latvia has an officially recognized national CIRT known as CERT.LV.
- Authorities responsible for enforcing cybersecurity rules: The Information Technologies Security Incidents Response Institution (known as 'cert.lv') promotes the security of information technology. Certain functions are delegated to the Institute of Mathematics and the Computer Science of the University of Latvia.
- Cert.lv can request and receive from state and local government authorities and other legal persons technical information regarding an IT security incident (eg, information on the scope of the incident, malicious software files that have caused the incident, a description of vulnerabilities, technical measures performed for the prevention of the incident, information regarding activities performed by persons doing harm or other technical information, including IP addresses), as well as obtaining, by mutual agreement, online data flow.

Lithuania

Law on Cybersecurity (2015). Authorities responsible for enforcing cybersecurity rules: The National Cybersecurity Council and the Communications Regulatory Authority.

Lithuania has an officially recognized national CIRT (CERT-LT) established within the Communications Regulatory Authority dealing with network and information security incidents in Lithuanian public electronic communications networks.

Concerning sector-specific CERT; LITNET CERT is the Computer Emergency Response Team of the Lithuanian academic and research network LITNET. SVDPT-CERT is a computer emergency response team of Secure State Dat Communication Network of the Lithuanian state institutions and municipalities and LTU MOD CIRT is a computer incident response team of the Lithuanian Ministry of Defence.

Luxembourg

Act of 1 August 2018 on the processing of passenger name record data in the context of the prevention and repression of terrorism and serious crime and amending the Act of 5 July 2016 on the reorganisation of the State Intelligence Service.

Act about the ratification of the treaty between Belgium, Germany, Spain, Netherlands, France, Austria and Luxembourg about the cross-border cooperation, especially in terms of anti-terror fight, the cross-border crime scene and illegal immigration, as well as the common declaration, signed in Prüm (Germany) on 27th May 2005 / Amendement of the Act of 21 December 2004 concerning the cross-border police assignment, signed in Luxembourg on 8th July 2004 / Amendement of the Act of 25 August 2006 concerning the genetic finger print within penal cases / Amendemend of the Act of 7 March 1980 about the organisation of judiciary agencies.

The law of 30 May 2005 relating to specific provisions concerning the processing of personal data and the protection of privacy in the electronic communications sector, modifying provisions 88-2 and 88-4 of the Criminal Instruction Code and modifying the DPA (the "ECA"), has implemented Article 13 of the Privacy and Electronic Communications Directive.

The ECA was amended on 28 July 2011 to implement the amendments to the Privacy and Electronic Communications Directive.

Act of 27 February 2011 (networks and electronic communications services)

The objectives of the Act of 27 February 2011 are:

- the creation of a competitive environment for the electronic communications sector and the free exercise of these activities in compliance with legal provisions;
- the regulation of access to electronic communications networks and associated ressources, as well as their interconnexion for the purpose of creating competition and ensure the interoperability of electronic communications services while providing advantages to consumers;
- the establishement of consumer and user rights and corresponding obligations of companies providing networks and electronic communication services available to the public;
- the definition of a universal service in electronic communications;
- the separation of the regulatory function from the operation of the networks and the provision of electronic communication services.

Articles 45 et 46 address the safety and integrity of networks and services.

The Act of 30 May 2005 on the networks and electronic communications services is repealed.

Consent is needed for the use of cookies unless the cookie is strictly necessary for the provision of a service to that subscriber or user. The ECA expressly refers to the use of browser settings as a means to obtain consent. There is an express requirement for consent to be "prior" to the use of a cookie.

The CNPD has not yet provided any guidance on the use of cookies.

In Luxembourg, the CNPD has approved binding corporate rules from eBay and ArcelorMittal.

Amended Act of 14 August 2000 on e-commerce. This Act is part of a consolidated text on the subject produced in 2004.

Malta

Maltese Subsidiary Legislation 586.10 regulates the processing of data concerning health for insurance purposes. Among other things, these regulations stipulate that the processing of data concerning health shall be lawful where such processing is necessary and proportionate for the purposes of a policy in the business of insurance, where the data controller cannot reasonably be expected to obtain the consent of the data subject, and where the data controller is not aware that the data subject is withholding consent.

The amendments to the Privacy and Electronic Communications Directive have been implemented into Maltese law through Subsidiary Legislation 586.01, now entitled Processing of Personal Data (Electronic Communications Sector) Regulations (the "Implementing Legislation").

Under the Implementing Legislation, consent is needed for the use of cookies unless the cookie is strictly necessary for the provision of a service to that subscriber or user. The Implementing Legislation does not expressly refer to the use of browser settings as a means to obtain consent. It remains to be seen whether the proposed E-Privacy Regulation will have any effect on the current local position.

No regulatory guidance has to date been published.

The Implementing Legislation provides that direct marketing e-mails cannot be sent without prior explicit consent of the subscriber in writing.

The Criminal Code criminalises unlawful access to, or use of, information, particularly through the use of computers or other devices. The following actions may result in a criminal offence:

- the unlawful use of a computer or other device or equipment to access any data;
- unauthorised activities that hinder access to any data;
- unlawful disclosure of data or passwords; and
- the misuse of hardware.

Netherlands

Since the adoption of the NIS Directive is still in progress (The Cybersecurity Act stems from the EU Directive on Security of Network and Information Systems (NIS Directive) and was submitted to the House of Representatives in February 2018), there is no official CERT as yet.

The Police Directive has not yet been transposed, but the draft bill has been submitted.

"Besides an extensive legal framework on technical aspects - regulated by means of statutory instruments – other important acts to be mentioned are:

Telecommunications Act - Law of October 19, 1998, Stb. 1998, 310, latest amendment Stb. 2014, 247. Access to national infrastructures: Telecommunications Agency of Ministry of Economic Affairs.

Under the Telecommunications Law:

Chapter 13 Telecommunications Act: Authorised Surveillance.

This chapter obliges service providers of public telecommunication networks and public communication services to provide for the capacity to intercept and shall cooperate with LEA or Intelligence Services when legally ordered.

Service providers shall retain traffic data for a period of two years. They shall provide subscriber data when so ordered.

Centraal Informatiepunt Onderzoek Telecommunicatie CIOT (Central Information Point Investigation Telecommunications).

Chapter 11 Protection of personal data in telecommunications.

Notification of security breaches; unsolicited advertisement (spam); cookies, law enforcement by ACM by means of non-criminal but administrative sanctions

Electronic commerce law is covered by the Civil Code in the Netherlands, specifically Civil Code (Burgerlijk Wetboek), Book 3 and 6.

Romania

Romania is one of the few states which does not yet have a law on cyber security. A draft law on cybersecurity is currently under debate in Romania.

Law no. 506/2004 of 17 November 2004 regarding the processing of personal data and the protection of privacy in the electronic communications sector (the "PECR"), published in the Official Gazette No. 1101 of 25 November 2004 implemented Article 13 of the Privacy and Electronic Communications Directive. The PECR came into force on 28 November 2004 and has been amended in 2012 in order to implement the amendments to the Privacy and Electronic Communications Directive.

Under the PECR, storing cookies or gaining access to such data is permitted subject to obtaining the prior consent of the data subject that has been informed of the processing activity and of its purpose in a complete, accessible and clear manner. In case of third party access to cookies, additional information

obligations have to be observed prior to obtaining the consent, such as informing the data subject of: (i) the general purpose of the processing activities performed by third parties; and (ii) the possibility of using internet browser settings or other similar technologies to erase the stored personal data or to refuse third party access to the above information.

An internet browser setting or other similar technology made by the data subject to give consent to a controller for using cookies is sufficient. A controller is exempted from the obligation to obtain prior consent for using cookies when the processing: (i) is exclusively for the purpose of transmitting a communication through an electronic communication network; and (ii) is strictly necessary for providing an information society service expressly requested by the respective data subject.

There is no regulatory guidance for the use of cookies.

Poland

On 5 July 2018, the Polish Parliament passed the Act on the

National Cybersecurity System which transposes the NIS Directive

Specific legislation and regulation related to cybersecurity has been enacted through the following acts:

- Act on Electronic Signature - Act on Electronic Payment Instruments

- The Act on the Protection of Personal Data - Act on Providing Services by Electronic Means

- The Act on the Computerisation of the Operations of Entities Performing Public Tasks.

Poland has an officially recognized national CIRT called CERT.GOV.PL. The first CERT created in Poland was the CERT

Polska followed by the PIONIERCERT and the TP CERT. CERT Polska is a member of CSIRT network (set up within NIS Directive).

Portugal

In the past couple of years, the CNPD has issued several opinions that received wide media attention.

In 2015, the CNPD conducted an audit of the Portuguese Tax and Customs Authority (the Tax Authority) following the creation of a 'VIP list' (a list concerning a special group of taxpayers composed of public figures linked to politics and sports). The CNPD concluded that no adequate security measures had been adopted and, therefore, confidentiality was compromised. Also in 2015, the CNPD issued several opinions, including Opinion 1704/2015 on the processing of personal data within clinical investigations; Opinion 1450/2015 on access to data from the electoral registration database; and Opinion 1770/2015 on the intra-group agreements review procedure for transfers of data outside the EU. In 2016, the CNPD issued Opinion 923/2016 on the access of executive officers and solicitors to the personal data included in employees' payslips in the course of executive processes, and an Opinion7 on a legislative proposal to provide the Tax Authority with access to bank account data. In July 2017, the CNPD approved Opinion 1039/2017 on the Principles Applicable to the Recording of Phone Calls, revising Opinion

629/2010. In this document, the CNPD defines new time limits for the retention of call recordings for the purpose of proving commercial transactions and any other communications regarding the contractual relationship.

Decree-Law No. 69/2014, of May 9th (although broader and known as the National Cybersecurity Center), came into operation only on October 7th, 2014.

Portugal has approved Law 46/2012 of 29 August (the ePrivacy Act) concerning the processing of personal data and the protection of privacy.

Slovakia

These laws deal mostly with national security and handling of confidential/classified information, as well as the setup of the SK-CERT:

- Decree of the National Security Authority No. 166/2018 Coll. on details of the technical and technological equipment and staffing of the CSIRT Unit
- Decree of the National Security Authority No. 165/2018 Coll. that determines identification criteria for respective categories of serious cybersecurity incidents and details of cybersecurity incidents reporting
- Decree of the National Security Authority No. 164/2018 Coll. that determines identification criteria of the operated service (criteria of the essential service)
- Decree of the Ministry of Finance of the Slovak Republic No. 55/2014 Coll. on Standards for Information Systems in Public Administration as amended
- Act No. 45/2011 Coll. on Critical Infrastructure as amended
- Act No. 275/2006 Coll. on Information Systems in Public Administration as amended
- Act No. 215/2004 Coll. on Protection of Classified Information and on Amendment and Supplementing of Certain Acts as amended
- Act No. 319/2002 Coll. on Defence of the Slovak Republic as amended

SK-CERT (Slovak Computer Emergency Response Team) exists as the National Authority for Cyber Security since January 1, 2016. Provision for it was made under the national strategy 2015-2020, as a transposition of the NIS Directive.

Act No. 351/2011 Coll. on Electronic Communications has been passed, but is only available in Slovak.

Slovenia

ZVOP-1 (Personal data protection, does not include the GDPR yet, Page 15)):

- Security of Personal Data, Article 24

(1) Security of personal data comprises organisational, technical and logical-technical procedures and measures to protect personal data, and to prevent accidental or deliberate unauthorised destruction, modification or loss of data, and unauthorised processing of such data:

i. by protecting premises, equipment and systems software, including input-output units;
ii. by protecting software applications used to process personal data;
iii. by preventing unauthorised access to personal data during transmission thereof, including transmission via telecommunications means and networks;
iv. by ensuring effective methods of blocking, destruction, deletion or anonymisation of personal data;
v. by enabling subsequent determination of when individual personal data were entered into a filing system, used or otherwise processed, and who did so, for the period covered by statutory protection of the rights of an individual due to unauthorised supply or processing of personal data.

(2) In cases of processing of personal data accessible over telecommunications means or network, the hardware, systems software and software applications must ensure that the processing of personal data in filing systems is within the limits of authorisations of the data recipient.

Currently, the operational capacities to respond to cyber threats are distributed among SI-CERT as the national response centre for network incidents, the Information Security Sector within the IT Directorate at the Ministry of Public Administration

Slovenian ePrivacy laws are mainly contained in: (i) the ZVOP-1 (soon to be repealed by the ZVOP-2) together with GDPR. Now ZVOP-2 is not yet adopted.

Legislation on the IP Law is reflected in the criminal code and penal code of Slovenia.

From the Penal Code of Slovenia: Breaking into the Information System, Article 242 (Page 91)

(1) Whoever, in the course of business operations and without authorisation, uses, changes, copies, transfers or destroys data held in an information system, or enters their own data, obstructs the transfer of data or the operation of the information system, or breaks into the information system in any other way in order to obtain an unlawful property benefit for themselves or another, or to cause pecuniary damage to another, shall be sentenced to imprisonment of not more than three years.

(2) If the offence under the above paragraph has resulted in a large loss of property or a large property benefit and if the perpetrator intended to cause such loss of property or to gain such property benefit, he shall be sentenced to imprisonment of not more than five years.

- Abuse of inside information Article 243

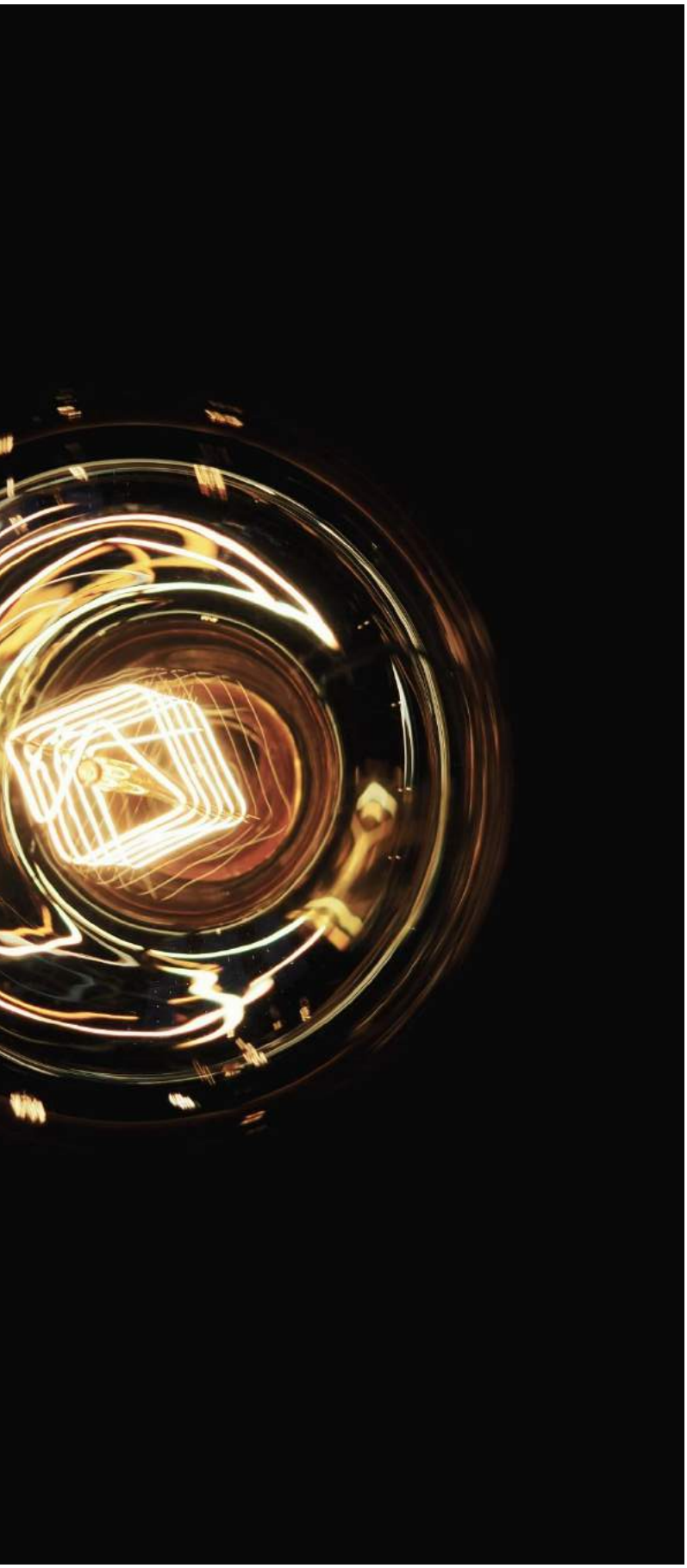
(1) Whoever, on account of their position with an issuer of securities, their ownership share in the capital of an issuer of securities or their employment, or in the course of performing their activities, obtains inside information that could have an important effect on the price of a security or executive financial instrument listed on the organised market in the Republic of Slovenia or in one of the member states of the European Union, or for which a proposal for listing on this market has been submitted (regardless of whether they are engaged in trading them on this market), and exploits that position through the purchase or sale of this security or executive financial instrument for their own or for another's benefit, indirectly or directly, shall be sentenced to imprisonment of not more than three years.

Electronic commerce and e-signatures Act (Page 5): The Act is entirely adjusted with the provisions United Nations– Commission or the International Trade Law–s (UNCITRAL) Model Law of the electronic commerce and with the provisions of the primary European legislation. It assumes also all the provisions of the Directive 1999/93/EC of the European parliament and EU Council from 13. December 1999 concerning common framework of the Community framework for electronic signatures.

- Section 2 # Electronic data, Article 12 (Page 11)

(1) Where the law or any other provision requires that certain documents, records or data be retained, that requirement is met by retaining electronic data, provided that the following requirements are met:

i. if the information, contained in an electronic document or record is accessible so as to be usable for subsequent reference; and
ii. if the information is retained on the format, in which it was generated, sent or received, or in a format which represents accurately the information generated, sent or received; and
iii. if such information is retained as to enable the identification of the origin and destination of an electronic message and the place and time when it was sent or received; and
iv. if such technology and procedures are used as to prevent in a sufficient manner any change or deletion of data, which would not be easily ascertained, or to reliably assure the inalterability of the message.



Spain

Royal Decree-Law 12/2018, of September 7, on the security of networks and information systems. Its provisions are NOT applicable to SMEs.

Good example of online resources for SMEs:

incibe.es/protege-tu-pany/tool/politics and grouping of relevant legislation in the Code of Cybersecurity Law.

Sweden

Electronic Communications Act. This Act implements Directive 2002/58/EC on the protection of privacy in the electronic communications sector (E-Privacy Directive). The Electronic Communications Act also contains provisions on the retention of data generated or processed in connection with the provision of electronic communications networks and services.

These provisions were introduced to implement Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (Data Retention Directive), which was declared invalid by the Court of Justice of the European Union (CJEU) in 2014 (Digital Rights Ireland (Joined Cases C-293/12 and C-594/12)).

However, the national provisions still apply, as the E-Privacy Directive allows EU member states to introduce national rules to that effect provided that certain requirements are met. Whether Swedish legislation fulfils those requirements was contested by providers of electronic networks and services.

United Kingdom

CERT-UK is the Computer Emergency Response Team.

The UK's Privacy and Electronic Communications (EC Directive) Regulations 2003/2426 (which implement the e-Privacy Directive (2002/58/EC) . These Regulations make amendments to the Communications Act 2003 and the Wireless Telegraphy Act 2006 (along with other primary and secondary legislation) to implement the Citizens' Rights and Better Regulation Directives, which amend the European Framework on Electronic Communications ("European Framework" – see paragraph 4.1 for the Directives in the Framework). Amendments to the "E-Privacy" Directive are being implemented by separate regulations.

Cyber piracy of music/films/e-books and other items is copyright infringement and is an offence under the Copyright Designs and Patents Act 1988. Counterfeiting goods is a trade mark infringement and is an offence under the Trade Marks Act 1994.

When considering cases involving intellectual property crime prosecutors should also consider the Counterfeiting and Forgery Act 1981, Video Recordings Act 2010, the Registered Designs Act 1949.

As well the predicate intellectual property offences governed by the relevant legislation, general statutory offences under the Fraud Act 2006 and money laundering offences under the Proceeds of Crime Act 2002 should also be considered.

For instance, if an individual offers a fake item for sale online, which they falsely represent to be a genuine article, prosecution under the Forgery and Counterfeiting Act 1981 should be considered, alongside offences under the Fraud Act 2006 and Proceeds of Crime Act 2002.

In instances where an individual offers fake identity documents online, prosecution should also be considered under the Identity Documents Act 2010, where the document is one prescribed under section 7.

The National Cyber Security Centre (NCSC) launched on 1 October 2016. The NCSC provides a unique opportunity to build effective cyber security partnerships between government, industry and the public to ensure that the UK is safer online. It will provide cyber incident response and be the UK's authoritative voice on cyber security. For the first time, key sectors will be able to engage directly with NCSC staff to get the best possible advice and support on securing networks and systems from cyber threats. The NCSC provides:

- a unified source of advice for the Government's cyber security threat intelligence and information assurance;
- the strong public face of the Government's action against cyber threats – working hand in hand with industry, academia and international partners to keep the UK protected against cyber attack; and
- a public-facing organisation with reach back into GCHQ to draw on necessarily secret intelligence and world-class technical expertise. Providing communications on how organisations in the public and private sector can deal with cyber security issues, facilitating the sharing of cyber threat information;

The Government worked with the Information Assurance for Small and Medium Enterprises (IASME) consortium and the Information Security Forum (ISF) to develop Cyber Essentials, a set of basic technical controls to help organisations protect themselves against common online security threats. The full scheme, launched on 5 June 2014, enables organisations to gain one of two Cyber Essentials badges. It is backed by industry including the Federation of Small Businesses, the CBI and a number of insurance organisations which are offering incentives for businesses. Cyber Essentials is suitable for all organisations, of any size, in any sector. From 1 October 2014, Government requires all suppliers bidding for contracts involving the handling of certain sensitive and personal information to be certified against the Cyber Essentials scheme. (https://www.gov.uk/government/publications/cyber-essentials-scheme-overview)

8 | GDPR

GDRP

It is important to remember that GDPR provision for a risk-based approach is horizontal as there are not exemptions or light weight approaches based on the organization size, availability of recourses and capabilities. Similar to larger organizations, SMEs and VOs have to identify the level of risk, depending on nature, scope, context of processing along to the types and volumes of data processed[24].

Austria

1. The data protection law prior to the implementation of the GDPR was the "Data Protection Act 2000 (DSG 2000)". This law has been substantially amended in 2017 to incorporate provisions from the GDPR, and is now simply known as the "Data Protection Act".

2. Law for the enforcement of the Police Directive is the same as the GDPR law.

Bulgaria

The General Data Protection Regulation in Europe is still largely based on the previous directive, however, a number of key changes are summarized below by the team lawyers in Bulgaria:

- Extra-territorial applicability: the new regulation applies to those companies that collect and control personal data in the EU, regardless of the fact that the subsequent processing takes place in the EU. It will also apply to companies that are not established in the EU but have subjects located in an EU country from whom they collect data.

- Fines for companies: businesses that do not observe these rules are subject to fines of up to 4% of their annual turnover (and/or other applicable penalties).

- New consent rules: companies are required to draw up new accessible and intelligible consent forms.

- New subject rights: the Regulation brings forward new rights for the individuals who are subject to data collection, some of them referring to rights of access, privacy by design and the fact that companies will need to appoint data protection officers.

[24] ENISA, Guidelines for SMEs on the security of personal data processing

Belgium

Loi du 29 mai 2016 (NOT GDPR) - Loi relatif à la collecte et à la conservation des données dans le secteur des communications électroniques: Belgium is in the process of adapting its national legislation to the GDPR. This is being done in two different streams.

The first is the reform of the Belgian Privacy Commission (which became the Data Protection Authority ("DPA") on 25 May 2018), in terms of organisation as well as in terms of capabilities. This is now completed with the adoption of the law of 3 December 2017, which was published on 10 January 2018 and entered into effect on 25 May 2018, except for Section III (Appointment of the members of the DPA) which applied as of 10 January 2018 (the "DPA Act"). To this date, the new members of the DPA have not been appointed and, as a consequence, the members of the former Privacy Commission are performing the relevant duties on a temporary basis.

The second is a framework law to address the national aspects of the GDPR. A first draft was made public on 11 June 2018 and is currently being discussed in the Federal Parliament.

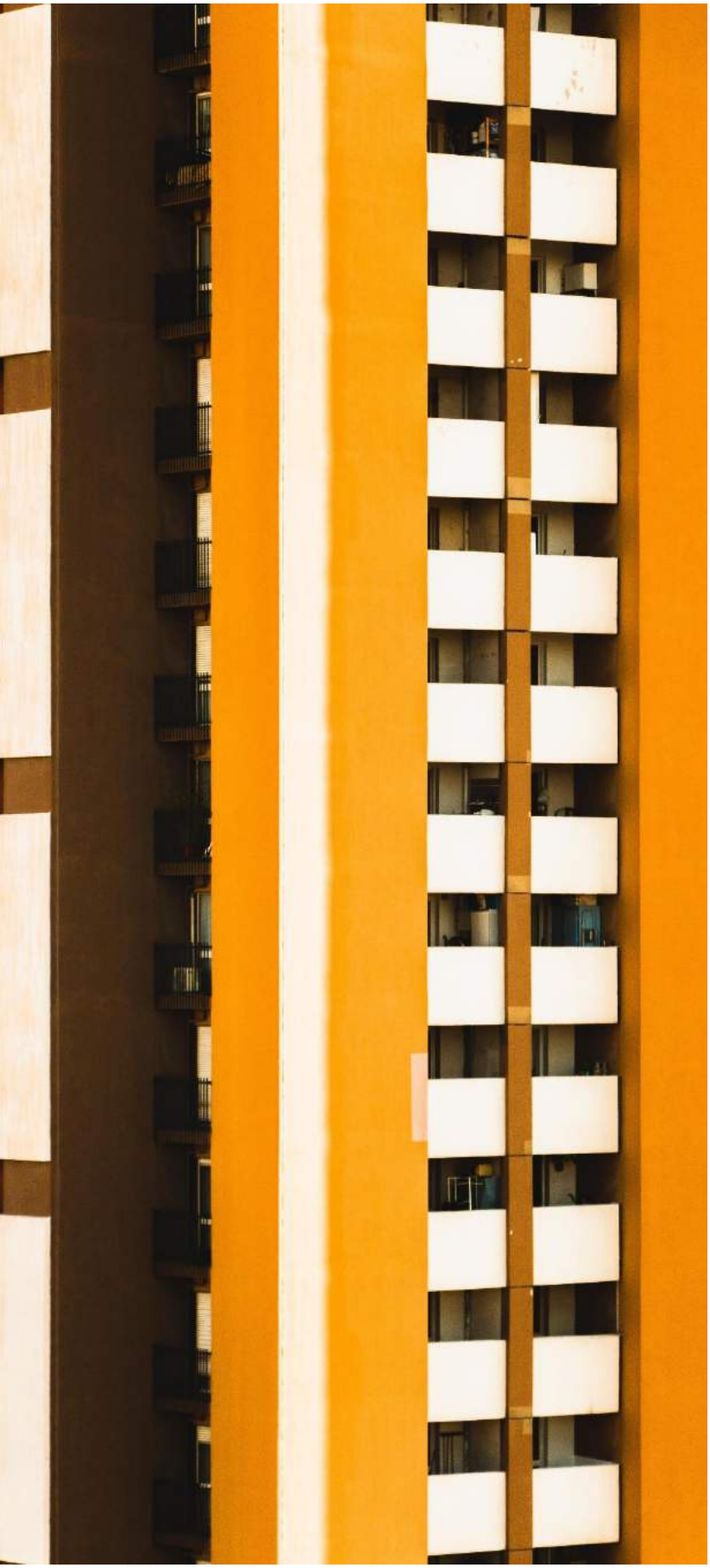
The Belgian DPA Act also entered into force on 25 May 2018, except for Section III (Appointment of the members of the DPA), which applied as of 10 January 2018.

It is not yet clear as of when the national framework law will apply.

With regard to infiltration, new rules have been introduced by the law on particular methods of research, and more specifically articles 47octies and 47nonies the Code of Criminal Procedure, which require the express authorization of the competent judge or the Prosecutor of the king. Regarding the retention of electronic communications data, all required technical and administrative measures that services and network providers must take are set by the King, by order of the Council of Ministers, upon the proposal of the Minister of Justice and after consultation with the Privacy Commission the Institute and the Belgian Institute for Postal services and Telecommunications.

The CEL prohibits the use of e-mails for advertising purposes without prior, free, specific and informed consent of the addressees. Such consent can be revoked at any time, without any justification or any cost for the addressee.

The sending of direct marketing e-mails does not require consent if they are sent to a legal entity using "impersonal" electronic contact details (e.g. info@company.be). The use of addresses such as john.smith@company.be, however, remains subject to the requirement for prior consent.



Croatia

The Act on the Implementation of the GDPR (NN 42/2018) was passed in May, 2018. A commentary on it can be found here: https://iapp.org/news/a/croatian-gdpr-implementation-law-main-features-and-unanswered-questions/

Cyprus

- The Processing of Personal Data Law L.138(I)/2001

- All type organizations including SMEs and GNOs who presses personal data have to comply with this law. The cybersecurity-related obligation includes to take the appropriate organizational and technical measures for the security of data and their protection against accidental or unlawful destruction, accidental loss, alteration, unauthorised dissemination or access and any other form of unlawful processing. •Cyprus published a new data protection law on July 21, 2018 to implement the GDPR (note- the law is available only in Greek).

Czech Republic

- All type organizations including SMEs and GNOs who presses personal data have to comply with the Protection of Personal Data Act No. 101/2000 (As amended by Act No. 301/2016).

- From cybersecurity perspective, the obligation of SMEs and NGOs include 'to adopt measures preventing unauthorised or accidental access to personal data, their alteration, destruction or loss, unauthorised transmission, other unauthorised processing, as well as other misuse of personal data'. Article 13 Act No. 101/2000

- In an effort to implement the GDPR and the Police Directive, Czech Republic has released a Draft Data Processing Act that will replace Act No. 101/2000

Note- all types of organizations in EU have to comply with the GDPR. Cybersecurity obligations include to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, and notification of cybersecurity breaches to authorities and data subjects.

Denmark

According to the GDPR. the data controller shall notify the supervisory authority of a personal data breach without undue delay after becoming aware of it. A data processor shall notify the data controller of a breach without undue delay.

Operators of essential services are required to report Incidents with an impact on the continuity of the services they deliver. The recipient of the report depends on the sector of the operator. For instance. according to the Danish Act on Net and Information Security for Domain Name Systems and Certain Digital Services. Incidents must be reported to the Danish Business Authority and the Danish Centre for Cyber Security. Such a report must namely contain information as to the number of affected users. the duration of the Incident. and the geographical spread in relation to the area affected by the Incident. The relevant regulator can publish information about specific Incidents when necessary to prevent or manage an Incident in progress.

Similarly. providers of digital services are required to report Incidents with a substantial impact on the services they deliver to the Danish Business Authority and the Danish Centre for Cyber Security.

Providers of financial services are required to report certain Incidents to the relevant authorities. primarily the Financial Supervisory Authority. the Danish Business Authority and the Danish Centre for Cyber Security.

The Danish Business Authority has oversight of the main sections of the Danish Telecommunication Act but. depending on the type of Incident. other authorities may be involved. especially the Danish Centre for Cyber Security.

The Danish Act on Payment Services puts obligations on providers of payment services to report Incidents to the authorities to the users of the payment services if there is a risk that their transactions may be affected.

The E-Commerce Act was passed in 2004. The law requires providers of services in the information society to clearly provide information about themselves and their contractual obligations.

1. The Danish Data Protection Act has been passed by the Danish parliament. The GDPR and the Danish Data Protection Act repeal the Danish Personal Data Processing Act as of 25 May 2018.
2. The Police Directive has been transposed into law, but is only available in Danish (https://hoeringsportalen.dk/Hearing/Details/60330).

Estonia

Obligations arising from the Personal Data Protection Act

§ 10. Permission for processing personal data

§ 11. Disclosure of personal data

§ 12. Consent of data subject for processing of personal data

§ 15. Notification of data subject of processing of personal data

§ 16. Processing of personal data for scientific research or official statistics needs

France

Law n° 2018-493 of 20 June "relating to personal data protection" incorporates the GDPR provisions in French national law. This new law modifies the existing French Data Protection Act (together the "revised French DPA"). The revised French DPA has retrospective effect and applies from 25 May 2018. The CNIL (Commission Nationale de l'Informatique et des Libertés) will continue to act as the supervisory authority in France.

There is no obligation to notify regulators of any processing under the GDPR, but the revised French DPA maintains the existing obligation to declare processing relating to health data to the CNIL.

The GDPR contains a general obligation to implement appropriate technical and organisational measures to protect personal data.

In addition, controllers and processors must ensure, where appropriate: (i) the pseudonymisation and encryption of personal data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of its information technology systems; (iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Specific rules governing processing by third party agents (processors):

A controller must ensure that any processor it instructs will ensure adequate security for personal data and otherwise meet the requirements of the GDPR.

The controller must have written contracts with its processor containing the enhanced processor clauses.

The DRA has created an official procedure for the disclosure of security vulnerabilities (new Article L2321-4 of the Defence Code). A person acting in good faith may inform the ANSSI – the governmental agency in charge of information security – of the existence of a security vulnerability. The ANSSI must ensure the confidentiality of the identity of its informant. The ANSSI may then investigate the reported vulnerability by performing the technical operations strictly necessary to assess its risk or danger, and warn the person in charge of the information system at issue.

A personal data breach must be notified to the relevant supervisory authority unless it is unlikely to result in a risk to data subjects. The notification must, where feasible, be made within 72 hours. If the personal data breach is a high risk for data subjects, those data subjects must also be notified.

The Article 29 Working Party has issued Guidelines on Personal Data Breach Notification (WP250).

Specific notice of breach laws apply to the electronic communications sector under the Privacy and Electronic Communications Directive.

The revised French DPA provides for a list of processing that will be exempt from the obligation to notify data subjects. That list will be established in a future Decree. However, no information is available at this time regarding the adoption of such a list.

Finland

No info

Germany

German Federal Data Protection Act (BDSG)

Greece

Like any other organization who presses personal data SMEs and GNOs are subject to the Protection of Individuals with regard to the Processing of Personal Data (Law 2472/1997) accordingly, SMEs and GNOs have the obligation to take cybersecurity measures such as implementing 'appropriate organisational and technical measures to secure data and protect them against accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure or

access as well as any other form of unlawful processing' (Article 10).

With the aim to implement the GDPR, Greece released a Draft law on the protection of data

Hungary

1. Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information

- This act applies to all type organizations including SMEs and GNOs who presses personal data
- Therefore, SMEs and GNOs have cybersecurity such as to implement adequate safeguards and appropriate technical and organizational measures to protect personal data, sec.7

2. To implement the GDPR a Draft bill on the right to information self-determination and freedom of information is released (Draft law Available only in Hungarian)

Ireland

Data Protection Bill – This Bill will give effect to and provide for derogations from the GDPR, and transpose the Law Enforcement Directive (2016/680). The Heads of Bill were published in May 2017, and pre-legislative scrutiny was completed on July 2017.

Italy

On 4 September, the Legislative Decree no. 101 of 10 August 2018 (the "Decree") for the national implementation of General Data Protection Regulation (EU) 2016/679 (the "GDPR") has been published in the Official Journal. The approach of the legislator was to maintain the structure of former Legislative Decree 196/2003 (the "Privacy Code") which, however, has been extensively amended and integrated, and now contains only some residual provisions in addition to those of the GDPR which are directly applicable. The Decree will enter into force on 19 September 2018.

Latvia

No info

Lithuania

No info

Luxembourg

On 16 August 2018, the Luxembourg Government adopted and published the law of 1 August 2018 on the organisation of the National Commission for Data Protection and implementation of 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 (the "Luxembourg Law").

The Luxembourg Law repeals the law of 2 August 2002 on the protection of persons with regard to the processing of personal data. The Luxembourg Law also amends the Labour Code and the amended Law of 25 March 2015 laying down the system of salaries and the conditions and procedures for advancement of civil servants of the State. The Luxembourg Law applies from 20 August 2018.

The Luxembourg Law suggests that the CNPD (Commission Nationale pour le Protection des Données) will continue to act as the supervisory authority in Luxembourg.

In the field of labour and insurance law, the processing of genetic data for the purpose of the exercise of the data controller's own rights is prohibited.

Luxembourg employers are entitled to require future employees to provide an extract of their criminal record in the context of the organisation and recruitment of the staff. The extract of the criminal record, and the data derived from such extract, may only be used by the employer for recruitment purposes or human resources purposes and may not be kept for more than one month.

Malta

The GDPR has been implemented through the Maltese Data Protection Act 2018 (Chapter 586 of the Laws of Malta) (the "DPA") which took effect on 28 May 2018.

Additional subsidiary legislation implementing the GDPR has also been promulgated. These regulations take advantage of various national derogations, allow the processing of health information for insurance purposes, lower the age at which a child can consent to online services and amend existing legislation.

The 'processing' of data effectively refers to the processing (automated, mechanical, manual or otherwise) of a person's data in a filing system or in what is intended to form part of a filing system.

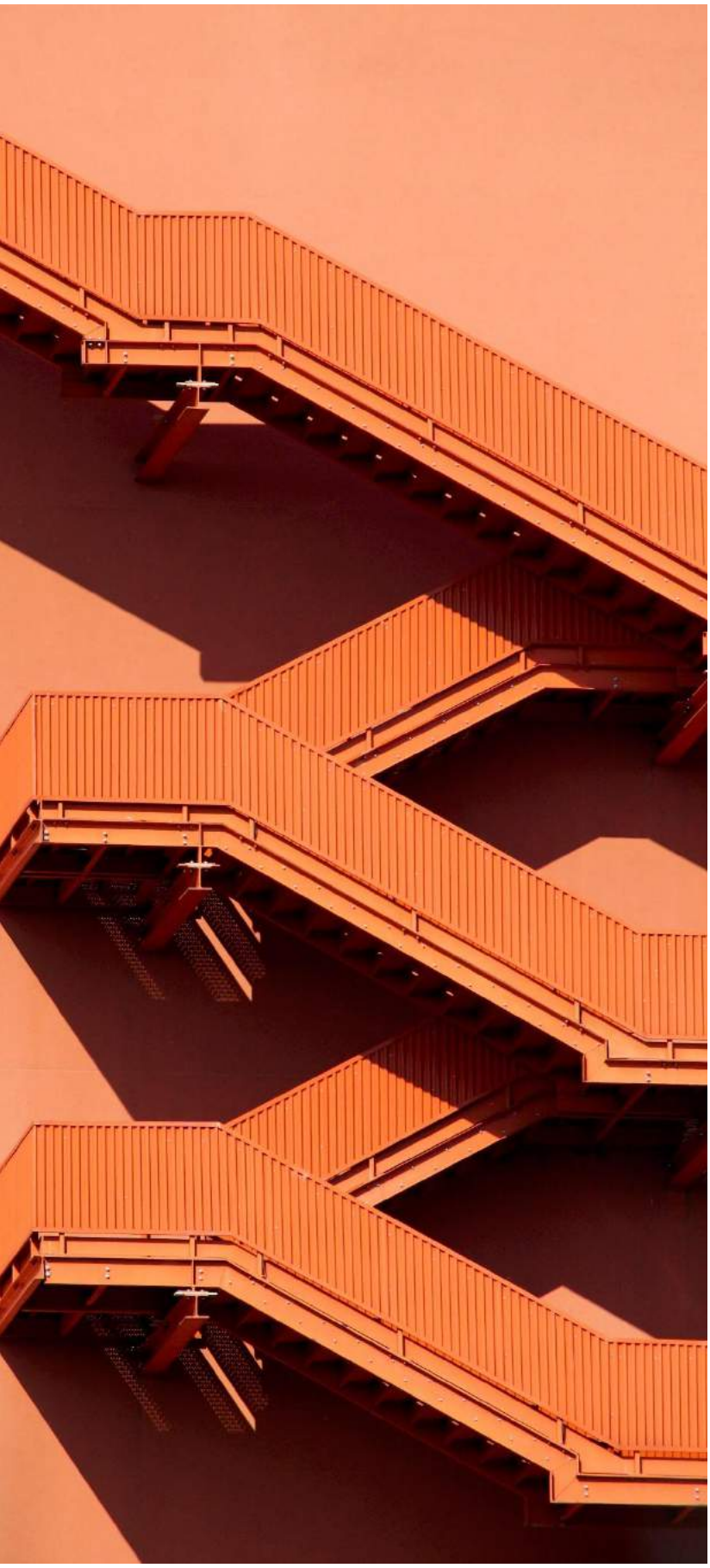
The appointment of a data protection officer (referred to by Maltese law as a 'data protection representative') is not mandatory.

The Office of the Information and Data Protection Commissioner is responsible for enforcing data protection legislation.

The Law Enforcement Directive has been implemented in Malta by Subsidiary Legislation 586.08.

The DPA establishes the Information and Data Protection Commissioner as the supervisory authority in Malta.

In Malta, the Information and Data Protection Commissioner has the power to draw up a list of "high risk" processing activities which would be subject to an impact assessment, but has not done so yet.



Netherlands

1. The GDPR has been transposed into law as the AVG (Algemene Verordening Gegevensbescherming).
2. The Police Directive has not yet been transposed, but the draft bill has been submitted.

Poland

No info

Portugal

No info

Romania

Law no. 190/2018 laying down certain measures for implementing GDPR has been promulgated by the Romanian President and is pending publication in the Official Gazette of Romania for entry into force (the "Data Protection Law").

The Law no. 129/2018 for amending and supplementing Law no. 102/2005 regarding the establishment, organization and functioning of the National Supervisory Authority for Personal Data Processing and for repealing Law no. 677/2001 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data has entered into force (the "DPA Authority Law" and, together with the Data Protection Law, the "Laws").

The Data Protection Law will apply five days after its publication in the Official Gazette.

The DPA Authority Law applies since 24 June 2018.

Privacy notices: Accoriding to the GDPR, a controller must provide data subjects with a privacy notice setting out how the individual's personal data will be processed. The privacy notice must contain the enhanced transparency information. The Article 29 Working Party has issued Guidelines on Transparency (WP260).

Slovakia

The GDPR has been transposed into law as "Act No. 122/2013 Coll. on Protection of Personal Data and on Changing and Amending of other acts, resulting from amendments and additions executed by the Act. No. 84/2014 Coll.

Slovenia

According to the different articles, Slovenia has not passed the GDPR act yet, according to other sources it has adopted a bill, however, there is no information about its implementation. Slovenia is one of the EU member states that has not adopted a GDPR implementing law before 25th of May 2018. In fact, Slovenia might not have such a law for quite some time since, while a draft of the new data protection act is in the parliamentary process since April, the matter has been stalled due to early parliamentary election. Furthermore, it is also uncertain if the draft will be adopted in the current version as there has been notable criticism as to its content, so a revised version of the draft is envisaged to be published in the next months.

Spain

Section 47 European Data Protection Regulation (pg. 953, 971, 978, 985, 1010, 1012 Code of Cybersecurity Law); Section 45 Organic Law on the Protection of Personal Data (pg. 880, Code); Section 47 European Data Protection Regulation (961, 992 Code).

Sweden

On 25 May, 2018, the new EU General Data Protection Regulation (GDPR, in Swedish Dataskyddsförordningen) replaced the Swedish Personal Data Act (PuL 1998:204).

The General Data Protection Regulations outline how personal data is to be processed by European Union member states. These regulations pertain to you and the information you provide to the Swedish Council for Higher Education (UHR).

United Kingdom

Data Protection Act 1998 - Section 55 of the Data Protection Act creates criminal offences that may be committed alongside cyber-dependent crimes.

These include:

- Obtaining or disclosing personal data;
- Procuring the disclosure of personal data;
- Selling or offering to sell personal data.

For example, Trojans can appear as legitimate computer programs but facilitate illegal access to a computer in order to steal personal data without a user's knowledge.

9 | CYBER SECURITY STRATEGIES

Cyber Security Strategies

Austria

The Austrian Cyber Security Strategy (ACSS) includes several references to SMEs and VOs.

1. Obligation to protect the integrity of their own systems
    - All Austrian enterprises should protect the integrity of their own applications as well as the identity and privacy of their customers.[25]
2. Importance of cooperation & knowledge transfer
    - Supporting close and systematic cooperation among enterprises;
    - Promoting mutual understanding of challenges and opportunities for action of all partners involved in cyber security issues;
    - Exchanges of experts should be intensified between governmental, private and academic organisations.
3. Development of technological instrument to facilitate cooperation
    - Creation of the Austrian Cyber Security Platform under the leadership of the Cyber Security Steering Group.[26]
4. Raise awareness of cyber security issues
    - Launch of priority programmes on cyber security to raise the awareness of SMEs27 and to prepare them for hazardous situations;
    - Publication of online information tailored to the needs of the SMEs and initiating cyber security campaigns;
    - Development of sector-specific cyber risk management plans with the support of governmental bodies and sector-specific information platforms, which should also be coordinated with governmental crisis management plans;

[25] Austrian Cyber Security Strategy available at , Pg. 9,
[26] Idem, Pg. 13(8),
[27] One of the ways of achieving his was the development of the "Austrian Security Portal". The initiators are the Federal Ministry of Finance (BMF), the Federal Chancellery (BKA) and the Centre for Secure Information Technology – Austria (A-SIT). See https://www.digital.austria.gv.at/documents/333663/355318/eGovernment-ABC-Guide-2017_SigStS.pdf/3af80626-c057-40db-9799-2aa969a8d97d.

- Organization of cross-sectoral cyber exercises for SMEs at periodical interval and inclusion of SMEs from specific sectors into governmental cross-sectoral cyber exercises upon request.[28]

Belgium

Belgium has an officially recognized national cybersecurity strategy known as Belgian Cyber Security Strategy Guide 2012. The aim of this strategy is to: (a) target a secure and reliable cyberspace that respects the values and rights of a modern society; (b) to ensure optimal protection against cyber- threat of public systems and critical infrastructures; and (c) develop national cybersecurity capabilities for independent security policy and a suitable response to security incidents.

The CERT.be, Fedict and the Centre Cyber Security Belgique (CCSB) monitor and coordinate the implementation of the national cybersecurity strategy and policy.

There are several ways in which the Belgian Cyber Security Strategy Guide targets SMEs and/or VOs:

1. Funding cyber security research

    - Encourages the design and implementation of national research and development (R&D) programs/projects aimed at developing cybersecurity standards, and identifying best practices and guidelines to be applied in either the private or the public sector.

2. Establishing a public-private partnership

    - The development of a PPP for cyber security in Belgium is a main goal. The PPP shall act as an Information Sharing and Analysis Centres (ISAC), with the following tasks: (a) fostering of partnerships; (b) fostering of information sharing; and (c) sharing of expertise and knowledge.

Bulgaria

Bulgarian National Cybersecurity makes several references that are applicable to SMEs and VOs:

1. Importance of cooperation and information sharing

    - Development of an effective mechanism and environment for sharing information and interaction between the government, the business sector and society.

2. Creation of programmes to improve SMEs and micro enterprises and raise awareness of cyber security issues

[28] Austrian Cyber Security Strategy available at (Pg. 13(9))

- Organisation of business networks or clusters to share information and best practices.

Croatia

The Croatian National Cyber Security Strategy (2015), specifically Objective E.5 seems relevant for SMEs and VOs as it discusses the importance of encouragement and constant development of cooperation with the economic sector.

1. Importance of cooperation and information sharing

    - Strengthen cooperation with the economic sector (especially with national regulatory authorities and legal entities in the public electronic communications sector and the electronic financial services sector);

    - Stimulate information sharing, especially regarding new computer security incidents;

    - Enable the economic sector to recognize potential incidents that could constitute criminal offences and update their security systems in a timely manner, thus enabling governmental organizations to react promptly.

2. Educate end users

    - Use communication initiatives aimed at educating end users of certain services.

Cyprus

Cyprus has a National Cybersecurity Strategy in place, which was adopted in 2013. The only reference made to SMEs and NGOs is in the context of the importance of collaboration between the public and private sectors.

Czech Republic

The Czech Republic has adopted the National Cyber Security Strategy 2015-2020. The document contains several references to SMEs and civil society:

1. Fostering trust building and cooperation among public and private sector, and civil society in the area of cybersecurity

2. Acknowledging the insufficient security of SMEs

    - This is explicitly identified as one of the challenges for the country's cyber security readiness.

3. Educating and raising awareness on cyber security issues;

    - Identification of the private sector as a key contributor in initiatives aimed at educating, raising awareness and informing society on cyber security-related issues.

Denmark

The Danish Cyber and Information Security Strategy 2018-2021 makes specific references to the role played by SMEs and VOs in the field of cybersecurity:

1. Importance of cooperation and information sharing in the private sector

    - Creating a framework for a joint effort to promote ICT security and responsible handling of data and to disseminate joint solutions to cross-sectoral issues. The partnership will develop preventive security measures and launch efforts to promote businesses' use of international security standards. It will also focus on how to implement efforts to increase insight into ICT security on the part of primary advisors in businesses, such that these advisors are in a position to promote ICT security at Danish SMEs.[29]

2. Importance of cooperation and information sharing with civil society

[29] https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf

- Strengthening interactions with the public sector, private businesses, trade organisations and NGOs are also contributing to finding common solutions for the digital transition and helping to secure the foundation for a strong and secure Digital Denmark.

Another strategic document published by the Threat Assessment Branch under the Danish Centre for Cyber Security also made specific reference to Danish NGOs and SMEs as being direct targets of cyber espionage.[30]

Estonia

The Estonian Cyber Security 2014-2017 includes several references applicable to SMEs and VOs:

1. The development and large-scale implementation of a system of security measures

    - Development of adequate security measures. Every information system owner must acknowledge the risks related to the disturbance of the service he or she provides. Up-to-date and economically expedient security measures must therefore be developed and implemented.[31]

2. Increasing competence in cyber security by developing training and research in the field of cybersecurity

    - Providing high quality and accessible information-security related training to both public and private actors;
    - Establishing common requirements for IT staff competence in information security;
    - Setting-up a system for in-service training and evaluation;
    - Enhancing international research cooperation in cyber security;
    - Ensuring readiness in managing cyber security crises in both the public and private sectors;
    - Fostering innovative research and development in the field of cyber security.[32]

3. Raising awareness on cyber security

    - Sharing Estonia's expertise and experience in the area of cyber security both nationally and internationally, and supporting co-operative networks;

[30] https://fe-ddis.dk/cfcs/CFCSDocuments/Threat%20Assessment%20-%20The%20cyber%20threat%20against%20Denmark.pdf
[31] https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf
[32] Idem.

- Raising awareness of cyber security issues among all computer users with a particular focus on individual users and SMEs. This should be achieved by informing the public about cyber threats and by improving knowledge on the safe use of computers; and

- Co-ordinating the distribution of information on cyber threats and organising awareness campaigns in co-operation with the private sector.

Finland

The Finnish Cyber Security Strategy was published in 24th January 2013 and provides some strategic guidelines on means of improving cyber expertise and awareness among societal actors SMEs and VOs includes:

1. Increasing competence and awareness in the area of cyber security

    - Develop and implement training programmes in the area of cyber security for both business and non-governmental actors;

    - Creation of a strategic cyber security centre of excellence will be established under the existing Finnish Future Internet Programme - ICT-SHOK (TIVIT). This will provide an opportunity for research teams and companies using the research results produced by the centre to engage in long-term effective cooperation under the framework of a cyber security research cluster.

    - Multiply initiatives aimed at improving cyber security know-how in the whole of society.[33]

2. Strengthening the ability of critical business and organisations to detect and repel cyber threat

    - Ensuring the security of supply chains.[34]

France

An inter-ministerial working group was tasked to prepare a report on a General strategy for the fight against cybercrime. It submitted its report containing 55 recommendations to the Government on 30 June 2014. Moreover, following the establishment in 2009 of an Agency responsible for information systems security (the "ANSSI"), a Cybersecurity strategy was published in February 2011 ("Défense et sécurité des systèmes d'information: Stratégie de la France"). Cybersecurity is also labelled as a priority in the last White Paper on defence and national security published in April 2013. In addition to this, France has adopted a Digital Strategy in 2015 and has released an Action Plan of the Ministry of Interior against cyber threats and a current state of cyber threats in January 2017.

[33] https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf
[34] Idem.

The French National Digital Security Strategy (2015) includes several provisions, which can be applicable to SMEs and VOs:

1. Strengthening security

    - Development of a range of digital security products tailored to the general public. Remedial actions will be structured around aid to victims of cybermalevolence, providing technical and legal assistance.

2. Awareness raising, initial training, continuing education

    - Raise the awareness of individuals as well as organizing training programmes the area of cybersecurity for the public and private sectors.

3. Specific regulations for operators of critical infrastructure[35]

    - All OIVs are required to comply with the obligations listed in Article 22 of the French CIIP law ("Loi de programmation militaire 2014-2019"). These obligations include compliance with rules for the protection of information systems set by ANSSI on behalf of the Prime Minister. These rules can be technical or organisational. According to the CIIP law, OIVs are obligated to report cybersecurity incident notifications to ANSSI. The nature of incidents to be notified will be specified by sectorial orders. During major crisis that threaten the security of information systems of critical infrastructure, the Prime Minister may decide on additional measures that OIVs would have to implement. According to the CIIP Law, OIVs are obligated to undergo cybersecurity audits, performed by either ANSSI or a service provider qualified by ANSSI.[36]

Germany

Cyber Security Strategy for Germany (Federal Ministry of the Interior) adopted in 2011 and updated in 2016 directly addresses the needs of SMEs:

Support for SMEs in the secure use of IT systems

- Setting-up a task force on IT security in industry, which includes the participation of industry actors.[37]

[35] These may be applicable to SMEs which are part of the supply chain for critical infrastructure operators.
[36] https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/
[37] https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile

Greece

Greece has adopted the National Cyber Security Strategy – Version 3.0 in September 2017. The document does not include any specific references to SMEs[38] or NGOs.

Hungary

The National Cyber Security Strategy of Hungary was adopted through Government Decision No. 1139/2013, and it includes several short references to SMEs and VOs:

1. Need for coordination between government, academia, business sector and civil society
    - Using cooperation among different societal actors (including SMEs and VOs) to support activities for the secure use of cyberspace and
2. Awareness raising and development of practical cybersecurity skills
    - The awareness raising initiatives should be specifically targeting individual users and SMEs.[39]

Ireland

The Irish National Cyber Security Strategy 2015-2017 includes specific references to SMEs:

1. Developing education and training in the field of cybersecurity for individuals and SMEs
    - Revising Make IT Secure website and including resources, which can help citizens and SMEs to better protect themselves online.[40]

Italy

Italy has adopted in 2013 the National Strategic Framework for Cyberspace Security, which includes several provisions that could also be applicable to SMEs:

1. Strengthening public-private partnerships in the area of cyber security
    - Establishing ad hoc agreements with the aim to substantiate even further public-private cooperation. The synergies with the private sector should be extended so as to include all

[38] Except references to the need of strengthening public-private partnerships in the area of cybersecurity.
[39] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy.
[40] https://www.dccae.gov.ie/documents/NationalCyberSecurityStrategy20152017.pdf.

entities that, independently of their size, are of strategic value for the scientific, technological, industrial and economic progress of the country.[41]

2. Planning of public services of assistance and support, in particular to small and medium enterprises

Latvia

The Cyber Security Strategy of Latvia 2014-2018 was adopted in 2014. There are several provisions within the document which relate directly to SMEs and VOs:

1. Improve coordination among public, non-governmental and private sectors in the area of cyber security
    - Improve coordinated development, implementation and evaluation of the national cyber security policy through the National IT Security Council, which includes both private and public representatives
2. Improve exchange of information among public and private actors
    - Create an information exchange medium (platform) which would assist entrepreneurs in exchanging information regarding cyber security threats, problems, solutions, good practices and their application.
3. Improving cyber security standards and practices
    - Improving understanding of ICT security in the business environment;
    - Organizing regular training programmes for employers.[42]

Lithuania

The Lithuanian Cyber Security Strategy for 2011-2019 and its follow-up adopted in 2018 refer to private sector entities, which can also apply to SMEs:

1. Lack of cooperation among Lithuanian public and private sector entities
    - This prevents an efficient planning of the development of cyber security;
    - To enhance cooperation, the state will promote initiatives aimed at developing cyber security innovation. This objective will be fulfilled by identifying the common needs of

[41] https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf.
[42] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/latvian-national-cyber-security-strategy

private and public sectors, their importance to scientific cyber security research, by creating technical measures, methods and other resources, by developing competences to resolve cyber security problems and carry out specific cyber security objectives.

2. Secure cyberspace is the concern of all entities, both public and private whose activities are related to the provision of services in cyberspace.

    - A potential way forward for increasing cyber security is the implementation of collaborative electronic information security projects.[43]

3. Develop creativity, advanced capabilities and cyber security skills and qualifications

    - Creating a cyber security competence model, establishing cyber security competence standards, developing systems of training, accreditation and certification oriented towards the needs of the labour market;

    - Attracting and developing talents, creating training and testing environment of cyber security, teaching the beginners/newcomers and providing opportunities of re-training/re-qualification to persons working in the ICT field;

    - Improving knowledge on cyber security of persons who work with sensitive data. [44]

Luxembourg

Luxembourg has adopted in 2018 the National Cybersecurity Strategy III, which includes several provisions applicable to SMEs:

1. Building public trust in the digital environment

    - Ensuring knowledge sharing between all stakeholders;

    - Systematic dissemination of on threats, vulnerabilities and common security measures;

    - Raising awareness of information security;

    - Promoting responsible disclosure of detected computer vulnerabilities.

2. Promoting the economy
    - Strengthening public-private partnerships;

[43] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf
[44] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/LRV+818+National+Cyber+Security+Strategy+%28Lithuania%29.pdf

- To pool risks and encourage victims of digital cyber incidents to seek help from experts to manage the incident and restore a system affected by a malicious act, insurance companies will be encouraged to create specific products for the area of cyber insurance;
- Releasing standard requirement benchmarks for the most widely operated systems;
- Prioritizing and promoting research carried out by start-ups offering innovative solutions in the field of cyber security.[45]

Netherlands

The Dutch National Cyber Security Agenda makes the importance of SMEs clear:

1. Promoting transparency in (chain) interdependencies between organisations
    - All organisations need to be able to respond appropriately when the continuity of their services is at risk;
    - The Digital Trust Center, currently in development, aims to help parties in this regard by raising awareness and offering perspectives for action. The center will do this in consultation with the NCSC and various other parties, including small and medium businesses;
    - Computer networks and sensitive information should be dealt with in a professional manner and with integrity.[46]

Poland

The National Framework of Cybersecurity Policy of the Republic of Poland (2017-2022) was adopted in 2017 and includes some brief references to the role played by NGOs and SMEs in ensuring cyber security:

1. Developing awareness campaigns regarding cybercrime threats
    - Providers of essential services, digital services, Internet access services and NGOs play an important role in this type of activity;
2. Need for cooperation between public administration, NGOs and academic centres
    - This cooperation is required to undertake systematic actions aimed at raising public awareness of the threats of cyberspace, as well as educational activities on rights and freedoms in the digital environment.

[45] https://hcpn.gouvernement.lu/fr/publications/strategie-nationale-cybersecurite-3/strategie-nationale-cybersecurite-3.html
[46] https://www.ncsc.nl/english/current-topics/national-cyber-security-agenda.html

3. Creation of innovation hubs

    - The innovation hubs will offer comprehensive services for companies and start-ups, including testing new solutions, market research, support in applying for funding for development of innovation solutions, advice on access to new markets and assistance in establishing cooperation with other entrepreneurs.[47]

Portugal

The National Cybersecurity Strategy Portugal was published by the government in May 2015. The strategy establishes special programmes for Small and Medium Enterprises (SME), socio-professional associations and, in particularly, freelance professionals.[48]

Romania

In 2013 the Government of Romania adopted the Cyber Security Strategy and the National Action Plan on the implementation of the Cyber Security National System (Government Decision No. 271/2013 published in Official Journal No. 296/23 May 2013). The strategy includes provisions applicable to SMES:

1. Complete and harmonize national legislation, including the establishment and enforcement of minimum security requirements for a national cyber infrastructure;
2. Develop cooperation between the public and private sector, including by fostering information exchange on threats, vulnerabilities, risks, and that related to cyber incidents and attacks;
3. Provide adequate professional training to people working in cyber security and promote widespread professional certification in this field;[49]

Slovakia

The Cyber Security Concept of the Slovak Republic 2015-2020 includes among its "implementation tools" for building a national cyber security space the need for cooperation and partnerships at national and international levels of all relevant entities from public, private and academic sectors and the civil society.[50]

[47] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/govermental-program-for-protection-of-cyberspace-for-the-years-2011-2016-2013
[48] https://www.cncs.gov.pt/content/files/rcm_36-2015.pdf
[49] https://www.mae.ro/node/28367
[50] http://www.nbusr.sk/en/cyber-security/national-cyber-security-strategy/index.html

Slovenia

The National Cyber Security Strategy of Slovenia includes the following provisions, applicable to all public and private sector actors (SMEs and VOs includes):

1. Development and introduction of new technologies in the field of cyber security;
2. Regular implementation of awareness raising programmes on cyber security for business entities.

Spain

The Spanish Cyber Security Strategy adopted in 2013 includes several provisions applicable to both SMEs and VOs:

1. Strengthening cooperation between the public and private sectors
    - Promoting the exchange of information on vulnerabilities, cyber threats and their possible consequences;
    - Conducting cyber exercises for both public and private sector actors;
    - Each type of organization has its own CSIRT for managing the incidents according to a specific procedures;
2. Fostering research in the area of cyber security
    - In the area of financing of innovative and technological companies, The Centre for the Development of Industrial Technology –CDTI- has instruments for the set up and consolidation of technology basis companies and to improve their growth and development.
    - Offering grants for advanced cybersecurity research team excellence.[51]

Sweden

The National Cyber Security Strategy of Sweden makes indirect reference to SMEs and VOs when discussing the importance of effective collaboration in the field of cyber security. Good collaboration among the different actors of society is required to create a good operational capability to manage serious disruptions. The collaboration built up as part of preventive efforts often lays the foundation for the collaboration needed during serious incidents. This involves collaboration between different

[51] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/the-national-security-strategy

stakeholders in Sweden, such as central government authorities, municipalities and county councils, trade and industry and interest organisations, but also international collaboration.

United Kingdom

The National Cyber Security Strategy 2016-2021 was adopted in 2016 and includes direct references to the situation of SMEs and indirectly VOs:

1. Funding gaps
    - There are funding gaps that prevent SMEs from growing and expanding into new markets and territories. Ground-breaking products and services struggle to find customers who are willing to act as early adopters;
2. Importance of collaboration
    - To overcome existing challenges government, industry and academia must work effectively together;
3. Lack of adequately trained staff
    - In businesses, many staff members are not cyber security aware and do not understand their responsibilities in this regard, partially due to a lack of formal training;
4. Development and deployment of technology in partnership with industry
    - This would improve the understanding of the threat and strengthen the security of the UK public and private sector systems and networks.

Malta

The National Cyber Security Strategy was adopted in 2016. As one of its measures, the National Cyber Security Strategy calls for a National Cyber Security Awareness campaign that addresses the various strata of society, business, and public sector along with their specific needs, expectations and ICTs applied.

The Campaign shall seek to ensure a nation-wide understanding of what cyber security means, and implies, with an increasing focus to the realities of the various stakeholders of Maltese society and economy, so as to ensure better protection and preparedness within cyber space.

10 | EMERGING PRACTICES

Emerging Practices for Maltese VOs & SMEs

Security obligations

The controller and the processor shall implement appropriate technical and organisational measures, to ensure a level of security appropriate to the risk, including inter alia, as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data; (c) the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

It is important to note that the reference to the "state of the art and cost of implementation" should not be interpreted as an excuse not to act, but rather as a call to all the stakeholders to simplify and reduce the costs, in order to spread the adoption of security measures. In that sense approaches towards simplification of the notion of risk and adoption of appropriate measures are key to the proper implementation of this.

Data breach

The GDPR introduces a duty on all organisations (SMEs & VOs) to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.

You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

Recommendations

As the international, European and national legal frameworks do not include special provisions for SMEs and/or VOs, the only recommendations identified refers not to legal provisions but to methods of implementation and accessibility of legal information.

a. Methods of implementation

The GDPR requires all organizations to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. However, what constitutes appropriate security measures varies from country to country. [52]

Emerging Practice 1:

Supporting VOs and SMEs in better understanding and implementing appropriate measures.

This can be achieved in several ways:

1. **By making reference to specific ISO standards (though it is not mandatory to follow this standards) – e.g. Germany**
2. **By developing certification programmes for basic technical controls. These help organisations protect themselves against common online security threats. – e.g. UK Cyber Essentials scheme**

[52] In the UK the Government worked with the Information Assurance for Small and Medium Enterprises (IASME) consortium and the Information Security Forum (ISF) to develop Cyber Essentials, a set of basic technical controls to help organisations protect themselves against common online security threats. The full scheme, launched on 5 June 2014, enables organisations to gain one of two Cyber Essentials badges. It is backed by industry including the Federation of Small Businesses, the CBI and a number of insurance organisations which are offering incentives for businesses. Cyber Essentials is suitable for all organisations, of any size, in any sector. From 1 October 2014, Government requires all suppliers bidding for contracts involving the handling of certain sensitive and personal information to be certified against the Cyber Essentials scheme. More information on the Cyber Essentials scheme is available at https://www.gov.uk/government/publications/cyber-essentials-scheme-overview)

b. Accessibility of legal information

Because of the complexity and diversity of legislation related to cybercrime it can be very difficult for VOs and SMEs to find the right legal information applicable to their individual circumstances.

Emerging Practice 2:

Setting up a one-stop shop for cyber security information

This can be achieved in several ways:

1. **Building a public information platform (or alternatively including such resources on the website of national authorities in the field of cyber security) – UK and Spain (https://www.incibe.es)**
2. **Grouping all relevant legal provisions dealing with cybercrime in one Code – e.g. Codigo de Derecho Ciberseguridad in Spain.**

While the legal framework does not include special provisions for SMEs and/or VOs, European and national cyberstrategies do make specific references to such organizations. We have tried below to summarize some of the key ideas associated with these two categories of actors:

1. SMEs and VOs need special focus and additional support/No "one size fits all" policy
   - Providing funding and know-how for SMEs and VOs to enable them to meet cybersecurity standards;
   - Providing adequate and easily accessible informational resources regarding their rights and obligations in the area of cybersecurity;
   - Setting-up certification mechanisms, which would ensure they meet the required cybersecurity standards.

2. Importance of knowledge transfer between government, academia and private entities and importance of public-private partnerships
   - Fostering exchange of information between government, the private sector, academia and civil society;
   - Create platforms where different actors can collaborate on issues related to cybersecurity.

3. More supply-chain transparency
   - Ensuring that SMEs which are part of the supply-chain of critical infrastructure operators follow the same security procedures;

4. Fostering research & innovation in the area of cyber security
    - Supporting start-ups developing innovative cyber security solutions;

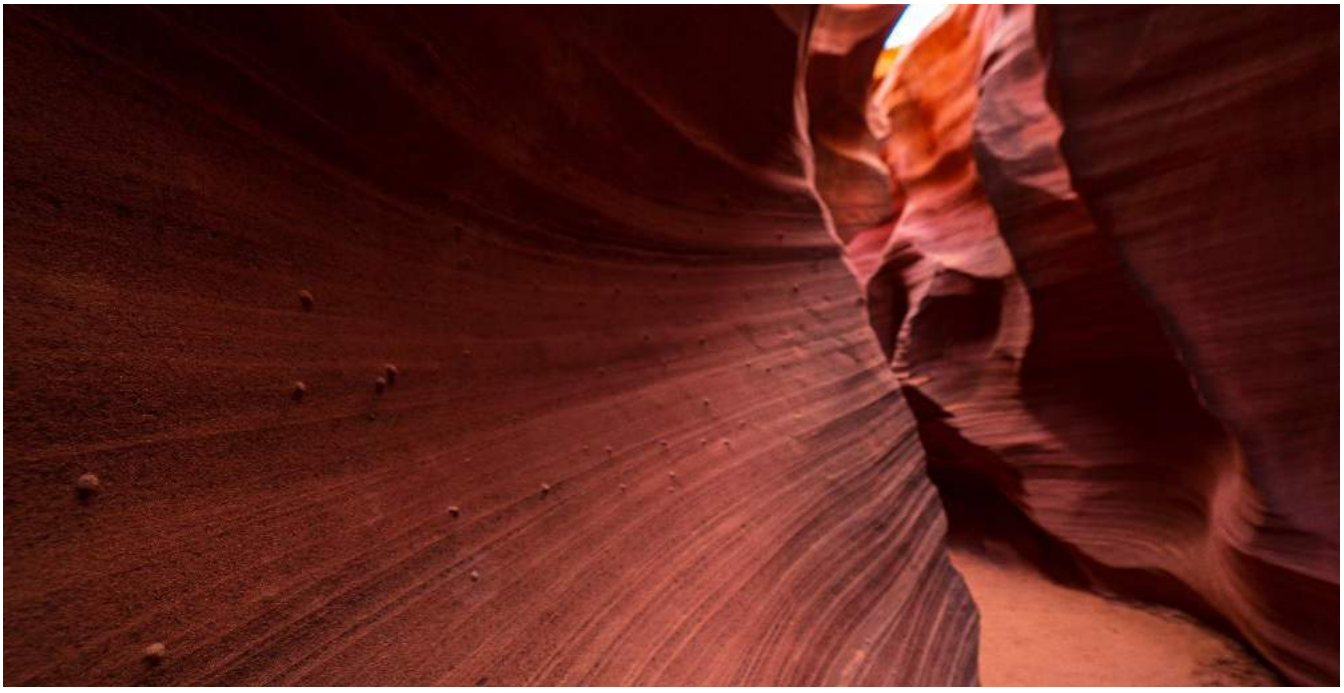
5. Developing skills of SME and VO personnel in the area of cybersecurity
    - Organizing training programmes for SMEs and VOs;
    - Organizing cybersecurity exercises, which include different societal actors.

6. Raising awareness of cybersecurity issues (e.g. safe behaviour online)

Different European bodies dealing with cybersecurity have also made recommendation on how to better improve cybersecurity readiness of SMEs (which can reasonably be extended to VOs as well).

One such set of recommendations was put forward by ENISA:

1. Development of practical guidance documents which would support and assist different types of data controllers. This should be developed by competent EU bodies and/or by national Data Protection Authorities and should also refer specifically to different categories of organizations, such as VOs and SMEs.
2. Increased European efforts (in both policy and research areas) to produce innovative solutions and development guidelines for cybersecurity[53]



[53] ENISA, Guidelines for SMEs on the security of personal data processing, December 2016, p. 6