Interreg
Italy – Croatia
Co-funded by the European Union
D.E.C.
EU RELATIONS G.E.I.E.
Grad Metković
odòs

INTERREG ITALY-CROATIA PROGRAMME 2021 – 2027

A.1.2 Studies on the professional sectors more vulnerable and exposed in the data protection and digital rights

D.1.2.1 Manual on Regulations and Professional Sectors

INDEX

Introduction

The *Manual on Regulations and Professional Sectors* is a vital component of the **Digital Ethics Culture** (**DEC**) project, co-financed by the European Commission's Interreg Italy-Croatia Programme 2021-2027. Emphasising values, understanding, and ethical implications of digital policies and rights over mere rule-following and fine avoidance, the project partners **Eurelations EEIG**, **Cooperativa ODOS**, and the **Municipality of Metkovic** aim to help Italian and Croatian citizens understand and comply with digital regulations. They seek to empower users and enhance their trust, encourage companies to integrate and monitor ethical practices, and ensure regulations reflect those principles and behaviours rather than just serving as a checklist of rules. By providing this comprehensive guide, the partners aim to deepen the understanding of digital regulations and identify the professional sectors most vulnerable to digital rights violations.

The Manual covers a wide array of crucial topics, beginning with the **regulatory frameworks that govern data protection and digital rights** (Chapter 1). A detailed exploration of the General Data Protection Regulation (GDPR) lays the foundation, explaining its scope, fundamental principles, legal bases for processing, and the rights of data subjects (Chapter 1.1). In addition to the GDPR, the Manual analyses the national data protection laws in the Programme Area, highlighting the roles and responsibilities of the Italian and Croatian regulatory authorities (Chapters 1.2 and 1.3). Furthermore, it offers an overview of the EU Commission's AI Act and its implications for data protection and digital rights (Chapter 1.4).

The Manual later delves into the **most vulnerable professional sectors in data protection and digital rights**, providing an in-depth analysis of the specific challenges and regulatory shortcomings (Chapter 2). In the Health sector (Chapter 2.1), it examines the importance of digital rights in healthcare, focusing on privacy, security, and the accessibility of personal health information. The Social sector is explored with an emphasis on the challenges faced by homeless individuals and refugees, including digital exclusion and surveillance issues (Chapter 2.2). For the E-commerce sector (Chapter 2.3), the Manual identifies specific threats to digital rights, such as misleading information and fraudulent practices. The Education sector is also covered, discussing the specific digital risks affecting students, educators, and institutions, with a special focus on primary schools (Chapter 2.4). Lastly, the Telecommunications sector is scrutinised, highlighting vulnerabilities in data privacy, security, transparency, net neutrality, and censorship (Chapter 2.5).

At the end of the document, the **Reference List** provides a comprehensive collection of sources and references used in the development of the Manual.

Chapter 1 – The main regulations on data protection, digital rights, and new technologies such as AI with a focus on the new European AI Act

1.1 The Regulation (EU) 2016/679 of the European Parliament, or GDPR

During the second half of the 20th century, the digital transition compelled regulators worldwide to expand the concept of 'privacy' beyond the traditional aspects of confidentiality and the right to be left alone and include the idea of **control over one's data**.

While various national legal systems followed this trend, it was only in 1981 that the first supranational law was introduced with the Council of Europe's **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data** (Council of Europe 1981), which came into force on 1 October 1985. The European Court of Human Rights (ECHR) helped shape the right to control personal information by interpreting **Article 8 of the European Convention on Human Rights**, which protects private and family life, home, and correspondence (*Cour Européenne des Droits de l'Homme* 2022). In 1995, the European Parliament and the Council adopted the principles of the Convention with the **Data Protection Directive**, establishing a robust framework to manage the complex relationship between technological innovation and information management (European Parliament and Council 1995).

Repealing the Directive in 2016, the European Regulation 2016/679, better known as the **General Data Protection Regulation (GDPR)**, represents the culmination of this legislative transformation (European Parliament and Council 2016). With 99 articles and 173 recitals, the GDPR applies since 25 May 2018 and inspired similar legislative efforts worldwide since then.

1.1.1 General Aspects, Scope, and Definitions

The GDPR's ultimate goal is the **protection of personal data**, considered as a "*fundamental*" (Recital 1), although not absolute, right that must be "*balanced against other fundamental rights, in accordance with the principle of proportionality*" (Recital 4).

Examples of *Personal* Data	Examples of *Non-personal* Data
name and surname	company registration number
personal email addresses	generic company email address: e.g. info@xxxxxx.com
sensitive data (e.g. criminal records, political opinions, sexual orientation, health, genetic, or biometric data)	irreversibly anonymised data (impossible to trace the identification of the person by any means or technology)
IP address	statistical data, such as the percentage of users preferring a certain feature in a software application

The **material scope** of the Regulation is the wholly or partly automated processing of personal data, as well as the non-automated processing of data which are (or are intended to form) part of a failing system. The **territorial scope** of the Regulation (Article 3) encompasses the processing of personal data of European citizens:

- by data controllers or processors established in the Union "*regardless of whether the processing takes place in the Union or not*;"

- "*by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law*;" and
- by a controller or processor not established in the Union whose processing activities relate to offering European citizens goods and services or monitoring their behaviour within the Union's borders.

GDPR's Territorial Scope: a Case Study	
Q1. The US-based company "YORK" sells goods to European consumers (therefore subject to the GDPR) and hires the US-based company "CITY" for market analysis and statistical purposes. Is the company "CITY" subject to the GDPR, even though it is not based in the EU nor does it sell goods or services to EU customers?	**A1**. Yes, if the market analysis and statistics activity require the monitoring of European customers' behaviours

The entity that is legally responsible for compliance with national and international legislation is the

Data Controller: Definition
"*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*" (Art. 4(7))

Data controllers are required to adopt all the **technical and organisational measures** necessary to properly secure their processing activities against the risks posed to the rights and freedoms of natural persons, such as data pseudonymisation and encryption (Art. 32(1)).

Data Processor: Definition
"*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*" (Art. 4(8)).

Data processors are appointed by controllers to carry out processing activities according to the controllers' methods and purposes. Their relationship must be documented legally, ensuring the processor provides sufficient guarantees of compliance with the controller's instructions and regulations. Both parties must also designate a **Data Protection Officer** (**DPO**) to advise, supervise legislation implementation, and cooperate with supervisory authorities (Art. 39).

1.1.2 The Fundamental Principles of Data Processing

Article 5 of the GDPR enshrines a series of principles governing data processing, according to which personal data must be:

i. "*Processed lawfully, fairly and in a transparent manner in relation to the data subject*" (**Principle of *Lawfulness, Fairness, and Transparency***)

Whoever intends to process personal data must comply with European and national laws, including those governing specific sectors (e.g. the Italian Workers' Statute), and provide data subjects with the information needed for them to effectively exercise their rights.

ii. "*Collected for specified, explicit and legitimate purposes*" and subsequently processed in a way that is compatible with those purposes (**Principle of *Purpose Limitation***)

Data collection and processing are bound to a specific purpose of which data subjects must be aware. When data controllers want to process data for purposes other than that for which the data has been collected, they must verify the compatibility of the new and the initial purposes (Article 6(4)).

<table>
<tr><td rowspan="2">Original Purpose</td><td colspan="2">must be explicit</td></tr>
<tr><td colspan="2">must be communicated to the data subject before the start of the processing</td></tr>
<tr><td rowspan="2">New Purpose</td><td rowspan="2">Compatibility Assessment:
connections with the initial purposes;
relation between data subjects and the controller;
categories of personal data processed;
possible consequences for the data subjects;
existence of adequate safeguards (e.g. encryption or pseudonymisation)</td><td>If compatible, a new consent is not necessary</td></tr>
<tr><td>If incompatible, a new consent is necessary</td></tr>
</table>

iii. "*Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*" (**Principle of *Data Minimisation***)

Only necessary data for a specific purpose should be collected and processed. This includes the amount and type of data, storage duration, and access. Data minimisation also means preferring alternatives like anonymised or pseudo-anonymised data whenever possible.

Data Minimisation: an Example

Hotel Y does not provide breakfast or meals and limits its services to overnight stays only. Therefore, the hotelier will only process data necessary to fulfil its legal obligations (i.e. the general personal information of its customers for communications to the Police Headquarters). Any other data, such as clients' food intolerances, will not be processed. If Hotel Y wishes to process such different data, it must request specific consent. In any case, access to customers' data must be reserved only for those employees that are inherent to the intended purposes (i.e. administrative staff in the reception office, rather than waiters)

iv. accurate and, if necessary, updated (**Principle of *Accuracy***)

v. stored for a period not exceeding the achievement of the processing purposes (**Principle of *Storage Limitation***)

Once the processing purposes have been achieved, the collected data should be deleted or subject to review.

vi. processed through "*appropriate technical and organisational measures*" that ensure adequate security of personal data (**Principles of *Integrity and Confidentiality***)

Data processors and controllers must ensure security throughout the entire data processing cycle, not just for the final data (Article 32). This includes protection against unauthorised processing, accidental loss, destruction, or damage.

Finally, responsibility for and ability to demonstrate compliance with all the aforementioned principles fall within the data controller's hands (**Principle of *Accountability***).

1.1.3 The Lawfulness of Processing: Legal Bases

The lawfulness of personal data processing (Art. 6) is ensured if *at least one* of the following conditions occurs:

i. **legal obligations** to which the controller is subject;
ii. safeguarding the **vital interests** of the data subject or another natural person;
iii. pursuing a **public interest** or exercising public authority by the controller;
iv. **contractual obligations** or execution of pre-contractual measures to which the data subject is a party

Data Processing on a Contractual Basis: an Example
Jessica wants to stipulate a contract with a real estate company that now has to draft the document. In this case, Jessica's interest in achieving the agreement's purpose and the pre-contractual measures to which she is a party already entail her consent to data processing. Similarly, should Jessica terminate the contract, the corresponding data processing should also cease

The possibility of grounding the lawfulness of data processing based on the overriding legitimate interest and/or consent requires a more in-depth discussion.

v. **Prevailing legitimate interests** of the controller or a third party.

Organisations can process personal data for their legitimate interests or those of a third party, provided these do not override the data subject's rights and freedoms. The data controller must balance these interests against the data subject's rights through a **'Legitimate Interest Assessment**' (**LIA**). Legitimate interests can include marketing, fraud prevention, and IT security but should be avoided if objections or less intrusive alternatives exist. Public authorities cannot use legitimate interests as a legal basis for their tasks.

Data Processing on Legitimate Interest Bases: Example 1
The company QWERTY is an online retailer that wants to analyse customer behaviour on its website to improve its services and marketing strategies. Per Article 6(1)(f), *before* proceeding with data processing, and *any* time someone raises concerns or objections, QWERTY must conduct an LIA to balance its legitimate interests (enhancing user experience and increasing sales) against the rights and freedoms of the data subjects
Data Processing on Legitimate Interest Bases: Example 2
The financial company ASD is looking for some of its customers who are late with payments. The company has a legitimate interest in obtaining the customers' new addresses even in the absence of specific consent – provided that it can prove that the processing of its customer's data is necessary for this interest

vi. The **"*freely given, specific, informed and unambiguous*" consent** of the data subject (Art. 4(11)).

For consent to be **free**, it is not sufficient that data subjects "*have the right to withdraw their consent at any time*" (Art. 7(3)). A valid and legally binding consent rests upon unambiguity and informativeness.

Data Processing on Consent Bases: Exception 1
Regarding the *"processing of special categories of personal data*," the so-called 'sensitive data' (Art. 9), as well as "*decisions based solely on automated processing, including profiling*" (Art. 22), consent must also be "***explicit***"
Data Processing on Consent Bases: Exception 2
At the European level, **the processing of children's data** to offer of digital services can be lawfully based on their consent only when children are at least 16 years old. Below that age, the processing is lawful only when "consent is given or authorised by the holder of parental responsibility over the child." However, at the national level, Member States can lower this threshold (e.g. in Italy it is 14 years old), as long as it remains higher than 13 years (Art. 8(1))

For consent to be **unambiguous**, it must be requested in clear, plain language and be easily accessible (Recital 39). It should be clearly distinguishable from other requests (Art. 7(2)) and shown by a clear affirmative action (Art. 4(11)). Consent need not be written but must be demonstrable by the data controller (Art. 7(1)). Tacit or presumed consent, such as pre-ticked boxes, is not allowed.

For consent to be **informed**, data subjects must be "*aware of the fact and extent to which consent is given*" (Recital 39). Informing data subjects about the collection and processing of their data is usually achieved through a **policy notice**, which must always be disclosed to the data subject when data collection occurs (Art. 13) and include *at least* the following information:

1) **Identity and contact details of the data controller**	5) **International transfers of data:** how the transfer will take place and what security measures have been taken
2) **Processing purposes**	6) **Data retention period**
3) **Legal basis for the processing**	7) **Data subject rights**: e.g. the right to access, rectify, erase, restrict, and/or object processing; the right to withdraw consent, and/or to lodge a complaint.
4) **Recipients of personal data**: whether the data will be shared with third parties and, if so, who these recipients are	8) **Obligation or discretion to provide data**: whether the provision of personal data is mandatory or optional and the consequences of any refusal

When personal data are *not* collected directly from the data subject, the information must be provided within a reasonable period that cannot exceed one month from the collection.

1.1.4 Rights of the Data Subject

The GDPR grants users certain rights regarding privacy and data control:

1. **Right of Access:** Data subjects must be informed about the data processed by controllers and processors, as well as the nature of their processing activities (purpose, retention, disclosure to recipients, etc.), and should be able to access, view, and request a copy of this information (Art. 15).
2. **Right to Rectification:** Under Article 16, data subjects have the right to request that inaccurate, incomplete, or outdated data be corrected, completed, or updated.
3. **Right to Erasure (or 'to be forgotten'):** Data subjects can oblige data controllers to erase their data under *one* of the following circumstances (Art. 17):

• the data is no longer necessary for the purpose it was collected
• the subject withdraws their consent
• the subject objects to the processing of their data and there is no overriding legitimate ground
• the data has been unlawfully processed
• data erasure is necessary for compliance with other legal obligations to which the controller is subject under European or national law
• the data was collected to offer digital services to a child or a child who has now reached maturity

4. **Right to Restriction of Processing** Data subjects can request controllers to restrict their data processing depending on the following circumstances:
    - inaccuracy of the personal data;
    - unlawful processing;
    - establishment, exercise, or defence of legal claims;
    - pending verification of the legitimacy of the data subject's objection to processing

Once restricted, data processing may only take place with the data subject's consent, or for reasons of EU or national public interest (Article 18).

5. **Right to Data Portability:** When data processing is based on consent or contractual obligations, or where the processing is carried out by automated means, data subjects have the right to receive the data from the controller "*in a structured, commonly used and machine-readable format*" and may also transmit that data to another controller (Article 20(1)).
6. **Right to Object:** Individuals can exercise their right to object data processing and force a data controller to stop its processing activities in two cases (Art. 21):
    - when the data is used for direct marketing purposes;
    - when the processing is based on the controller's legitimate interest or public interest

In both cases, data controllers can challenge the right to object by demonstrating "*compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject*" (Art. 21(1)).

7. **Right not to be subject to automated decisions:** Unless under the data subject's consent, contractual obligations, or public authorisation, data subjects have the right not to be subject to a decision that significantly affects them based solely on the automated processing of their personal data (Article 22). With the cooperation of data processors (Article 28(3e)), controllers must adopt all the appropriate technical and organisational measures to ensure the data subject can express his or her point of view, contest the decision, and request human intervention on the part of the controller.

1.1.5 Main Regulatory Aspects

Among the major innovations introduced by the GDPR are the principles of **Privacy by Design** and **Privacy by Default**, which make data controllers responsible in every phase of data processing. Their application requires the development of technical and organisational measures aimed at protecting data from the very beginning of the processing. This means that essential guarantees and safeguards must be provided upstream, "*both at the time of*

determining the means of processing and at the time of the processing itself" (Article 25(1)), and data controllers must conduct the appropriate analyses before the data processing.

The **Data Protection Impact Assessment** (DPIA) is a tool provided by the GDPR to identify, assess, and reduce the (*high*) risks inherent to processing activities that may negatively impact data subjects' rights and freedoms (Article 35):

NECESSARY DPIA CASES	EXAMPLES
Evaluation Treatments	*bank or financial scoring*
Processing Based on Automated Decisions	*tracking of online behaviours*
Systemic Monitoring	*tracking the location of data subjects*
Processing of Data Relating to Vulnerable Persons	*minors, migrants, or generally subjects who are in conditions of psychological or other subjection than the controller*
Large Scale Processing	*video surveillance*
Database Comparisons	*machine learning used for word transcription or as digital assistants*

Data controllers and processors must notify the supervisory authority of personal data breaches (Article 33). A "*data breach*" includes accidental or illicit security violations like destruction, loss, modification, or unauthorised disclosure/access of personal data. Notification is required only if breaches likely violate individuals' rights and freedoms, based on the controller's risk assessment. If so, controllers must notify authorities within 72 hours, including:

- The nature of the breach, affected data categories, and the number of data subjects/records
- Contact details of the data controller
- Possible consequences of the breach
- Measures taken or proposed by the data controller

Finally, the Regulation sets forth **responsibilities for data controllers and processors in case they fail to adopt satisfactory security measures**. These failures are often due to the inadequate management of the relations between the data controller and the data processor and may result in sanctions from the DPA. Depending on the type of provisions that have been violated, administrative fines can be:

- up to 10,000,000 euros, or for companies, up to 2% of the total worldwide annual turnover of the previous financial year, whichever is higher;
- up to 20,000,000 euros, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

1.2 Italian Privacy and Data Protection Regulations

In Italy, personal data protection is mainly governed by the so-called 'Privacy Code,' as amended by Legislative Decree 101/2018 for the adaptation of national legislation to the provisions of the GDPR.

For a long time, Italy had no laws defining and protecting privacy and personal data. In the 1950s, privacy was still considered in its 'domestic' dimension and governed by laws protecting people's private lives. While the 1970 Workers' Statute introduced some provisions to protect the privacy of workers, one of the main jurisprudential contributions to the configuration of privacy as a right per se within the Italian legal system was carried out by the Court of Cassation. In the 1975 ruling on the so-called '**Soraya Case**,' the Court formally recognised the existence of the right to privacy to protect strictly personal and family situations and events, which, even if not occurring in the domestic sphere, have no socially appreciable interest for third parties (Saetta 2022). References were found also in the Italian Constitution, which, although not providing for the right to the protection of personal data, considers **privacy as connected to the right to self-determination** (Constitution of the Italian Republic, 1947, Art.2).

With the 1985 Schengen Treaty putting to the fore the necessity of regulating the processing of people's data to achieve freedom of movement within the European Union, Italy followed the 1995 European Data Protection Directive and promulgated **Law n. 675 of 31 December 1996**. This piece of legislation significantly broadened the scope of the Directive's application, including the dignity of natural persons and personal identity in Article 1, as well as protections for data processing not organised in databases and data of legal persons (Official Journal of the Italian Republic. Law n. 675 of 31 December 1996.). With the same law, the Italian Data Protection Authority, or '***Garante per la Protezione dei Dati Personali***,' was also established as a guarantee institution to supervise the application of the regulation.

Increasing regulatory complexity eventually led to the enactment of the **Italian Data Protection Code** in 2003 – Italy's primary data protection law before the GDPR (Official Journal of the Italian Republic. Legislative Decree n. 196 of 30 June 2003). Also known as '*Codice in Materia di Protezione dei Personali*,' the Code represented a significant legal innovation as it moved away from a conception of privacy as the 'right to be left alone' to a new vision focused on 'informational self-determination' and control over one's data. The Code is composed of three parts:

1. the first one contains the basic definitions and general provisions on data processing;
2. the second part analyses the specific discipline applicable in various fields, including, for example, public administrations, the health sector, and the labour sector;
3. the third part regulates the structure and functions of the Data Protection Authority, as well as the administrative and judicial protections granted to data subjects who suffer privacy violations.

The 2003 Italian Data Protection Code: Territorial Scope

The law regulates the processing of personal data (also when held abroad) carried out by anyone based in Italy (**Principle of Origin or Establishment**) or in a State which does not belong to the EU but uses processing facilities located in Italy (**Principle of Location of Electronic Means**). If the processing is subject to Italian laws, the data controller must designate a representative established in the territory of the Italian State

The Code was amended in 2018 by **Legislative Decree 101/2018** ("*Adeguamento della normativa nazionale alle disposizioni del regolamento UE in materia di privacy*") to align with the GDPR's new requirements, especially with respect to:

- particularly complex and delicate treatments (i.e. **sensitive data**);
- the obligation for data controllers and processors to implement **security measures**;
- the **powers of the Supervisory Authority** to establish specific safety measures.

1.2.1 The 'Garante' – the Italian Data Protection Authority

The Data Protection Supervisor is an independent administrative authority established to ensure that the processing of personal data is carried out in compliance with the rights of individuals, **balancing the needs of protection with those of innovation and technological development**.
Its main **functions** include:

Supervisory Functions	**Legislative** Functions	**Disciplinary** Functions	**Other** Functions
• Compliance with data processing rules • Cooperation with national bodies	• Measures for data controllers and processors • Ethical rules • Guidelines • Resolutions • Opinions • Recommendations • Assistance in implementing other laws in data protection matters	• Data subjects' complaints • Crime reporting • Data processing prohibitions or blocks • Fines and sanctions	• Raising awareness

The Data Protection Authority publishes various documents to facilitate compliance and implementation or address specific privacy and data protection issues, including (Olivi 2024):

General Guide on the Application of the GDPR	An **overview of the main aspects** that companies and public entities must consider to fully implement the Regulation
Specific Guidelines	Published periodically on **various topics** related to the application of the GDPR: e.g. the 2021 *Guidelines on the use of cookies and other tracking tools*
FAQs	Answers to **common questions** and clarifications on specific aspects of the GDPR
Code of Conduct for Telemarketing and Teleshopping	**Not yet enforced** pending appointment of the competent supervisory body
Simplified Procedures For SMEs	**Not yet introduced**

1.2.2 The Italian Legislation: Adaptation of the GDPR

Although the GDPR applies directly across the Union, Member States must align their national laws with its provisions and address specific aspects left to their discretion.

The Italian Code acknowledges the **data subjects' rights** established by the GDPR (Articles 15-22). However, the GDPR states that these rights are not absolute and must be balanced with other fundamental rights and freedoms (Recital 4).

A landmark case in Italy played a significant role in **shaping this equilibrium in the national adaptation of the GDPR**. Judgment 19681/ 2019 of the Court of Cassation concerned the **balance between the right to be forgotten** (Article 17 of the GDPR) **and freedom of the press** (Article 21 of the Italian Constitution) in relation to an online article about a crime that had happened decades before. A man who had killed his wife had been condemned, served his sentence, and had been reintegrated into civil society, but the re-enactment of the news brought him to the media pillory again provoking damage to his image and reputation. The Supreme Court intervened to put an end to the matter:

- the right to freedom of the press is a subjective public right, which encounters three limits: social utility of the information, objective truth, and civil form of exposure (i.e. always respectful of the dignity of the person);
- the right to be forgotten can thus be exercised when the social utility in informing the public is no longer appreciable, when the news is outdated, or when the disclosure is not commensurate with its informative purposes and respect for the dignity of the interested party.

The Supreme Court therefore considered the need to evaluate the concrete and current public interest in the information identifying those who partook in the events at hand: such disclosure is lawful only if it refers to people of public importance, whether in terms of notoriety or public role; in all the other cases, the right to confidentiality shall prevail over the right of the press to disclose information about past events. (Iaselli 2019).

Certain **legal bases for data processing** (e.g. performance of tasks in the public interest or exercise of public authority) and **provisions for data controllers and processors** (e.g. international data transfers) are also laid down at the national level. Interestingly, the Italian legislation had to introduce provisions for **joint data** controllers, aligning with GDPR's new level of complexity in the allocation of responsibilities.

Although sharing the fundamental principles and provisions of the GDPR, the Italian Code also contains additional aspects addressing particular national needs. For example, it extends the scope of data subjects' rights to **deceased persons**: while the GDPR does not address post-mortem protection, Article 2-terdecies of the Italian Code establishes that these rights can be exercised by individuals with their own interest in the data, acting as the deceased data subject's agent, or for family reasons worthy of protection (Saetta 2022).

Similarly, the GDPR lets Member States choose the **age of consent for data processing** between 13 and 16 years, and Italy has set its threshold at 14 (Ibidem).

Another example of this is **how the provisions of the Italian Code and the GDPR are harmonised from a sanctioning point of view**. The GDPR establishes a general framework for administrative sanctions (Articles 83 and 84), but it

leaves the definition of the role of the Data Protection Authority, the regulation of criminal offences, and the specification of sanctioning procedures to the discretion of each Member State.
The GDPR provides **administrative fines** that vary depending on the severity of the crime:

GRAVITY OF CRIME	EXAMPLES	PENALTY AMOUNT
Less Serious	• failure to appoint the DPO; • failure to communicate a data breach; • violation of the consent conditions for minors; • unlawful data processing	Up to **€10 million** or **2%** of the previous year's annual turnover
More Serious	• illicit transfer of personal data to other countries; • failure to comply with the Authority's orders	Up to **€20 million** or **4%** of the previous year's annual turnover

The Italian Code (Article 166) defines the types of violations subject to each sanction category and appoints the National Data Protection Authority as the entity responsible for outlining the procedures for the implementation of measures and sanctions (Panetta 2018).

As regards **criminal offences**, Articles 167 to 172 of Legislative Decree 196/2003 provide for different types of offence ranging from telephone traffic and unwanted communications to dissemination or illegitimate acquisition of an archive, entailing prison sentences of up to six years. (Panetta 2018).

Notably, the Italian legislator reviewed the cases identified by the 2003 Code, introducing the **prediction of damage** as an alternative to the **purpose of profit**. By holding violations not only against the perpetrator's economic profit but also against the image and reputation damage caused to the victims, the Italian law covers also cases of revenge porn.

1.3 Croatian Privacy and Data Protection Regulations

1.2.1 Introduction: A Brief Historical Overview

Croatia's privacy and data protection laws have evolved to align with European standards and address technological challenges, demonstrating a commitment to safeguarding personal information in a digital world (Cizmic and Boban, 2018).

The roots of data protection in Croatia can be traced back to the early 1990s, following the country's independence. The **1990 Constitution** laid the groundwork by recognising privacy and guaranteeing confidentiality and protection of personal data in **Article 37**. This set the stage for more comprehensive laws.

In **2003**, Croatia enacted its first comprehensive data protection law, the **Law on Personal Data Protection**, based on the EU Data Protection Directive 95/46/EC. This law introduced key principles like necessity, proportionality, and legality of data processing, and established the **Croatian Personal Data Protection Agency** (**AZOP**) to oversee compliance and enforcement (Cizmic and Boban 2018).

Between 2006 and 2012, the 2003 Law underwent several **amendments** to better align with European standards, notably the introduction of stricter rules emphasising explicit consent and providing robust mechanisms for individuals to access, rectify, and delete their data (Politiscope 2021). With the enforcement of the GDPR in 2018, Croatia's data protection framework underwent a comprehensive overhaul to align with the new emphasis on transparency, accountability, and data subjects' rights of the European regulation. As a result of this process, the **2018 Law on Implementation of the General Data Protection Regulation** provided detailed guidelines on implementing the GDPR provisions and strengthened AZOP, giving it greater powers to monitor compliance, conduct investigations, impose sanctions, and raise public awareness about data protection (Politiscope, 2021).

1.2.2. AZOP – The Croatian Regulatory Authority: Main Powers, Duties, and Responsibilities

The Croatian data protection regulatory landscape is primarily overseen by the **Croatian Personal Data Protection Agency**, also known as '*Agencija za Zaštitu Osobnih Podataka*' (**AZOP**), which is tasked with the following responsibilities:

Main Powers and Responsibilities of AZOP			
Supervisory Functions	**Legislative** Functions	**Disciplinary** Functions	**Other** Functions
• Compliance with data processing rules • Coordination with other national authorities for data protection matters	• Guidance and advisory for data controllers and processors • Assistance in understanding data protection obligations • Guidelines, draft legislations, and data protection policy review	• Data subjects' complaints and crime reporting • Data breach management • Fines and sanctions	• Public and stakeholder awareness • Cooperation with national and international bodies

AZOP fulfils its functions together with other authorities such as the **Croatian Regulatory Authority for Network Industries** (**HAKOM**). HAKOM plays a significant role in regulating electronic communications in Croatia and ensures that data protection is upheld also within this sector, including by monitoring data processing by telecom operators, guaranteeing the confidentiality of communications, guiding consumers on data rights and redress for violations, enforcing cybersecurity standards to prevent data breaches, ensuring consistent enforcement of data protection laws across borders, conducting audits and inspections, and raising public awareness.

Case Study: Unauthorised Surveillance of a Public Area by Apartment Owner

Background: An anonymous complaint was lodged against an apartment owner who installed two fixed surveillance cameras that recorded a parking lot, a street, and individuals passing through the area. The complaint noted the lack of city permits and privacy violations.

Unauthorised Surveillance: Monitoring public areas (entrance and street) without adequate permits is restricted to public authorities and specific legal entities under the Croatian Law on Implementation of the General Data Protection Regulation (Art. 32(1)).

Data Processing Violation: The apartment owner illegally processed personal data by monitoring the public street, violating Article 6(1) of the GDPR.

Outcome: AZOP mandates the removal of the unauthorised cameras

1.2.3. Relationship with European Regulations: Similarities and Differences

Croatian data protection laws closely mirror EU regulations under the GDPR. The **rights of data subjects**, including access, rectification, erasure, restriction of processing, data portability, and the right to object are directly transposed from the GDPR into the Croatian legislation, ensuring consistency across EU member states. The **legal bases** for processing personal data in Croatia are the same as those outlined in the GDPR too. These include consent, contract performance, legal obligations, protection of vital interests, public interest tasks, and legitimate interests. Croatian regulations particularly emphasise explicit consent for sensitive data, following GDPR guidelines. Croatian law also imposes similar **obligations on data controllers and processors** as the GDPR. These include implementing adequate security measures, conducting data protection impact assessments, and maintaining processing records. Both Croatian and EU laws require transparency in data processing and clear communication to data subjects about their rights and data usage. The **penalty structure** in Croatian law aligns with the GDPR, with fines for non-compliance reaching up to 20 million euros or 4% of the annual global turnover, whichever is higher. AZOP, the Croatian data protection authority, has the power to impose these fines and enforce compliance.

While Croatian law closely follows the GDPR, however, there are specific national enhancements and provisions tailored to the local context. For instance, the recent amendments related to the ratification of the additional protocol to Convention 108 (**Convention 108+**) reflect Croatia's commitment to modernising its data protection framework in line with international standards. Moreover, while providing guidelines on how certain GDPR provisions are to be applied within the country, the 2018 Law also defined a **more pronounced role for AZOP**. Unlike some other EU countries where multiple agencies might share enforcement responsibilities, the Croatian Data Protection Authority serves as the central authority for all data protection matters in Croatia, providing a more streamlined approach to enforcement. Finally, **several sector-specific regulations in Croatia complement the GDPR**, such as the Electronic Commerce Act, the Consumers Protection Act, the Employment Act, and the Credit Institutions Act. These laws address specific aspects of data protection and provide detailed guidelines for various sectors (Central State Office 2022). For instance, the Electronic Communications Act and the Act on Data and

Information in Health Care provide more detailed rules for data processing in the telecommunications and healthcare sectors, respectively. Another notable example is the **Act on the Protection of Natural Persons**, which reinforces GDPR principles and the protection of natural persons' data by emphasising data subjects' rights and enhancing AZOP's powers.

Case Study: Use of a Child's Photograph for Promotional Purposes Without Consent

Background: In May 2022, AZOP received a complaint from a mother regarding the unauthorised use of her minor daughter's photograph by a tourist board for promotional purposes. The photograph was taken during a public sports event and was later used in promotional materials without the mother's consent.

Issue: The mother's complaint highlighted the lack of consent for the use of her daughter's photograph in promotional materials, which included postings on the town's Facebook, Instagram, and official websites.

Response: The mother contacted the tourist board, which removed the photographs from Facebook and the town's website. However, the photograph remained on Instagram.

Legal Findings: While determining that the event being held in a public space with public interest justified general photography of the event, AZOP found the tourist board's use of the photograph without consent to be a violation of data protection laws. For identifiable individuals used in promotional materials, explicit consent is required. The legitimate interest does not override the need for consent when an individual's image is prominently featured. AZOP The appropriate legal basis would have been explicit consent, as per Article 6(1)(a) of the GDPR.

Understanding both the GDPR and national laws, including sector-specific regulations and amendments poses a serious **challenge to data protection professionals in Croatia**. While risk management and data security became critical due to increasingly stringent penalties for non-compliance, ensuring it requires continuous education and training. Professionals must implement advanced security measures, conduct data protection impact assessments, prepare for potential breaches, an develop comprehensive data protection policies in line with the different regulations. Moreover, detailed requirements related to specific sectors like telecommunications and healthcare demand enhanced compliance efforts, including regular audits, maintaining detailed records, and transparent communication with data subjects. In this regard, effective **collaboration with AZOP and other authorities is key**: professionals should seek guidance from them, participate in industry forums, and stay updated on best practices

1.2.4 Challenges and Future Directions

Despite the robust legal framework established by the GDPR and its implementation in Croatia, several challenges remain.

One significant challenge is **ensuring that AZOP has the necessary resources and technological capabilities** to effectively oversee modern data processing activities (Bulat, 2019). As highlighted in various analyses, including those by Politiscope and legal scholars, there is a need for increased investment in technological infrastructure and human resources to enhance AZOP's capacity to enforce data protection laws.

The **COVID-19 pandemic** has further underscored the importance of data protection, particularly concerning the collection and processing of health data. The Croatian government's initiatives, such as the digital assistant Andrija and the Stop COVID-19 application, have raised concerns about the adequacy of privacy measures and the involvement of AZOP in ensuring compliance with data protection principles.

1.4 The AI Act of the EU Commission

The EU AI Act (AIA) represents a significant milestone in the regulatory landscape, aiming to ensure that artificial intelligence (AI) technologies are developed and used in ways that respect fundamental rights, promote innovation, and ensure trust and safety. Like the GDPR's comprehensive approach to data protection, the European AI Act establishes a framework for regulating AI, focusing on **transparency, accountability, and human-centric values**.

1.4.1 The Development of the AIA

The rapid development and deployment of AI across various sectors spurred the need for comprehensive regulation to ensure these technologies are safe, ethical, and aligned with fundamental rights long before the AIA was formally proposed.

1.4.1.1 First Steps and Guidelines

Recognising the transformative potential of AI and its implications for society and the economy, the European Commission unveiled the **European AI Strategy in April 2018**, outlining a vision to boost the EU's technological and industrial capacity in AI. The strategy emphasised the need for ethical guidelines and regulatory frameworks to ensure AI's responsible development and use. To operationalise the strategy, the Commission established a **High-Level Expert Group on Artificial Intelligence** (**HLEG**) **in June 2018** composed of AI experts, academics, industry leaders, and civil society representatives who were tasked with drafting ethical guidelines and policy recommendations for AI.

In April 2019, the HLEG published the **Ethics Guidelines for Trustworthy AI**, outlining key principles for AI development: human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination, fairness, societal and environmental well-being, and accountability. These guidelines served as a foundational document for future regulatory efforts.

Building on the HLEG's work, the Commission released the **White Paper on Artificial Intelligence in February 2020**. The White Paper proposed a risk-based regulatory framework for AI, distinguishing between high-risk and low-risk AI applications. It highlighted the need for a clear legal framework to address safety, liability, fundamental rights, and ethical aspects of AI.

The White Paper also initiated a **broad public consultation**, seeking input from stakeholders across sectors, including industry, academia, civil society, and Member States. Suggesting the need to balance innovation and protection of fundamental rights and safety, the consultation laid the ground for the Commission's **Draft Proposal for the Artificial Intelligence Act (AI Act) in April 2021**. Marking **the first comprehensive attempt to regulate AI at a supranational level**, the draft outlined a risk-based approach, classifying AI systems into four categories: unacceptable risk, high-risk, limited risk, and minimal risk. It proposed stringent requirements for high-risk AI systems, including mandatory conformity assessments, transparency obligations, and human oversight mechanisms.

Key Elements of the Draft Proposal		
Prohibited AI Practices	**High-Risk AI Systems**	**Governance and Enforcement**
The draft prohibited certain AI practices deemed to pose unacceptable risks, such as social scoring by governments and AI systems that exploit vulnerabilities of specific groups	The draft required high-risk AI systems to undergo rigorous conformity assessments, ensuring compliance with safety, transparency, and accountability standards	The draft established a governance framework, including national supervisory authorities and a European Artificial Intelligence Board (EAIB) to oversee implementation and ensure consistency

The draft proposal underwent extensive scrutiny and feedback from various stakeholders. Industry representatives expressed concerns about compliance costs and potential stifling of innovation, while civil society groups expressed the need for robust safeguards to protect fundamental rights. Member States also provided input, highlighting the importance of flexibility and proportionality in the regulatory framework.

1.4.1.2 Legislative Process and Negotiations

- **Council of the European Union**

The Council, representing EU Member States, examined the draft proposal, balancing national interests with the overarching goal of a harmonised AI framework. Negotiations focused on ensuring the Act's provisions were practical and enforceable, addressing concerns about administrative burdens and regulatory overlap with existing laws.

- **European Parliament**

Parallel to the Council's work, the European Parliament engaged in its own review, with various committees, including the Committee on Civil Liberties, Justice and Home Affairs (LIBE) and the Committee on Industry, Research and Energy (ITRE), scrutinising the proposal. The Parliament stressed the importance of protecting fundamental rights and fostering innovation.

- **Trialogue Negotiations**

The final stage of the legislative process involved trialogue negotiations between the Commission, the Council, and the Parliament. These negotiations aimed to reconcile differing positions and finalise the text of the AIA. Key areas of discussion included the scope of high-risk AI systems, the definition of prohibited practices, and the roles and responsibilities of national supervisory authorities and the EAIB.

1.4.1.3 Adoption and Approval

After extensive negotiations, a **final agreement** on the AI Act was reached in late 2023. The agreed text struck a balance between ensuring robust safeguards and promoting innovation, incorporating input from all stakeholders. The AI Act was **formally adopted by the European Parliament and the Council of the European Union in early 2024**. The Act entered into force shortly thereafter, with a phased implementation plan to allow stakeholders time to adapt to the new regulatory requirements.

The AI Act represents a landmark achievement in the EU's efforts to regulate AI. It establishes a comprehensive and flexible framework that addresses the diverse risks and opportunities posed by AI technologies. Moving forward,

the focus will be on effective implementation, monitoring compliance, and adapting the regulatory framework to keep pace with technological advancements and emerging challenges.

1.4.2 General Aspects, Scope, and Definitions

The European AI Act outlines several key objectives and definitions critical to its implementation:

Objective	Ensuring that AI systems used within the EU are safe, respect fundamental rights, and promote trustworthy and human-centric AI development and usage
Scope	The Act applies to providers and users of AI systems • within the EU, and • outside the EU, *if* the systems affect EU citizens
Definitions	• **AI System:** Software designed to operate with a level of autonomy, using techniques such as machine learning, neural networks, and deep learning; • **Provider:** Any natural or legal person who develops an AI system or has it developed and markets it under their name or trademark; • **User:** Any natural or legal person using an AI system, except when it is used in the course of a personal or household activity

1.4.3 Risk-Based Approach and Classification of AI Systems

The AIA adopts a risk-based approach, classifying AI systems into four categories based on their potential risk to fundamental rights and safety:

- **Unacceptable Risk AI Systems:** AI systems that pose a clear threat to safety, livelihoods, and rights of people. Examples include social scoring by governments and systems that manipulate human behavior in ways that could result in harm.
- **High-Risk AI Systems:** These are systems used in critical infrastructure, education, employment, essential public and private services, law enforcement, border control, and administration of justice. High-risk AI systems must meet stringent requirements before they can be placed on the market or put into service.
- **Limited Risk AI Systems:** These systems have specific transparency obligations but are not subject to the stringent requirements of high-risk systems. Users must be informed that they are interacting with an AI system unless it is obvious.
- **Minimal Risk AI Systems:** These include applications such as spam filters and AI-driven video games. They are subject to the least regulatory requirements.

1.4.4 Requirements for High-Risk AI Systems

High-risk AI systems must comply with several key requirements to ensure safety and respect for fundamental rights:

- **Risk Management:** Providers must establish a risk management system to identify, analyse, and mitigate risks throughout the lifecycle of the AI system;
- **Data and Data Governance:** The data used to train, validate, and test AI systems must be relevant, representative, free of errors, and complete;
- **Documentation and Record Keeping:** Comprehensive documentation, including technical specifications, risk assessments, data sets, and design choices, is required to ensure transparency and accountability;
- **Transparency and Provision of Information:** AI systems must provide clear and accessible information on their capabilities, limitations, and usage conditions to foster users' understanding of how to operate the AI system safely and effectively;
- **Human Oversight:** High-risk AI systems must include measures for human oversight to prevent or minimise risks, such as allowing for human intervention and the ability to override AI decisions when necessary;
- **Accuracy, Robustness, and Cybersecurity:** AI systems must achieve a high level of accuracy, robustness, and cybersecurity, ensuring they perform reliably and securely under normal and foreseeable conditions.

High-Risk AI Applications: Examples
Healthcare: AI systems for medical diagnostics, such as imaging analysis tools used to detect cancer, must be trained on diverse, high-quality medical data, ensure transparency in their diagnostic recommendations, and allow medical professionals to review and override AI-generated diagnoses. **Education**: AI-driven personalised learning platforms that adapt educational content to the needs of individual students must ensure data privacy, provide transparent information about how recommendations are made, and allow educators to oversee and adjust the AI's decisions. **Employment**: AI systems used for recruitment, such as resume screening and candidate assessment tools, must ensure non-discrimination, provide clear criteria for evaluation, and allow human resources professionals to review and adjust AI decisions. **Transportation**: Autonomous driving systems used in vehicles must meet stringent safety standards, ensure robust performance under various conditions, and allow human drivers to take control when necessary

1.4.5 Rights of the Data Subject in AI Context

Mirroring the GDPR, the European AI Act foresees individual rights for people affected by AI systems, including:

Right to Explanation
Maria applied for a position at a large corporation that uses an AI-powered recruitment system to screen and rank candidates. Maria's application is rejected, and she requests an explanation. Under the AI Act, the company must provide a detailed explanation of the AI system's decision-making process, including the **criteria used to evaluate candidates and the reasons for Maria's rejection**. This transparency allows Maria to understand the basis of the decision and to seek further recourse if necessary
Right to Contest

Consider a scenario where an AI system is used to determine creditworthiness for loan applications. John, a loan applicant, is denied a loan based on the AI system's assessment. John believes that the decision is unfair and requests a review. Under the AIA, John has the right to contest the AI decision, **prompting a human loan officer to review his application manually**. This ensures that any potential errors or biases in the AI system can be identified and corrected.
Right to Data Protection
An AI system used in a healthcare setting collects and analyses patient data to provide diagnostic recommendations. Patients like Sarah have the right to ensure that their personal health data is processed in compliance with data protection laws. This means the healthcare provider must obtain Sarah's *consent*, inform her of **how her data will be used**, and ensure that the **data is securely stored and processed**. If Sarah's data is to be shared with third parties, she must be informed and her consent obtained too.
Right to Non-Discrimination
An AI system is used by a housing authority to allocate public housing. Emma, an applicant, suspects that the system is biased against certain demographic groups. She has the right to request information on how the AI system ensures non-discrimination. The housing authority must demonstrate that the AI system has been **tested for biases** and that **measures are in place to mitigate any potential discriminatory impacts**. If Emma's suspicions are confirmed, she can take further action to challenge the system's fairness.

To effectively implement these rights, the European AI Act mandates several procedural and technical measures:

- **Transparency Obligations:** AI providers must ensure that users and affected individuals receive clear and accessible information about the AI system's functionality, limitations, and decision-making processes.
- **Human Oversight Mechanisms:** High-risk AI systems must incorporate mechanisms for human oversight, allowing for human intervention and review of automated decisions.
- **Accountability Frameworks:** AI providers and users must establish robust accountability frameworks, including documentation and reporting obligations, to demonstrate compliance with the AI Act's requirements.
- **Data Protection Impact Assessments (DPIAs):** For high-risk AI systems, providers must conduct DPIAs to identify and mitigate risks to data protection and fundamental rights. These assessments help ensure that AI systems are designed and operated in a manner that respects data subjects' rights.

1.4.6 Governance and Enforcement

To ensure its effective implementation and enforcement, the AIA establishes a comprehensive governance framework designed to promote consistency, accountability, and transparency across the EU and provide a robust structure to monitor and manage the use of AI technologies.

At the European level, the **European AI Office**, previously known as the **European Artificial Intelligence Board** (**EAIB**), is established as a central body at the European level to coordinate and ensure the consistent application of the AI Act across all Member States. Its functions and powers include

- **Implementing the AI Act**, especially for general-purpose AI, by enforcing rules for AI models, deploying market surveillance mechanisms, conducting evaluations, and ensuring compliance with legal requirements;

- **Fostering trustworthy AI development and use** to safeguard against AI risks and promote an innovative ecosystem through collaborations with experts, industry, and civil society;
- **Cooperating internationally** to advocate for trustworthy AI at the global level and assist in developing international AI agreements;
- **Monitoring, supervising, and enforcing the Act's requirements** for general-purpose AI models across the 27 EU Member States, including through risk analyses and reviewing compliance documentation from AI providers

At the national level, each EU Member State is required to designate a **national supervisory authority** responsible for:

- **Supervising and monitoring** the implementation of the AI Act, ensuring that AI providers and users adhere to the regulatory standards;
- Conducting regular **inspections and audits** of AI systems to assess their compliance with safety, transparency, accountability, and fundamental rights protection standards, investigate potential violations, and require corrective actions where necessary;
- **Providing guidance and support** to AI providers and users in understanding and implementing the Act's requirements, by issuing guidelines, best practices, and advisory opinions;
- **Imposing sanctions**, such as financial penalties, operational restrictions, and other corrective measures, in cases of non-compliance, which can also be publicly disclosed to enhance transparency and accountability;
- **Coordinating with other authorities**, such as data protection authorities and consumer protection agencies, to address overlapping regulatory concerns and ensure a cohesive approach to AI governance.

The European AI Act's Guidelines for an Ethic by Design Approach: an Example for the Education Sector

Imagine an AI-driven personalised learning platform is being developed to tailor educational content to individual students' needs and learning styles. The European AI Act highlights the importance of incorporating ethical considerations into the design and deployment of such high-risk AI system to ensure that it respects fundamental rights, promotes fairness, transparency, and accountability, and fosters public trust from the very beginning of its realisation:

1. **Identify Ethical Principles**:
   - Ensure transparency in how the platform recommends content and monitors student progress.
   - Assign accountability to educators and developers for the platform's recommendations and outcomes.
   - Strive for fairness by ensuring the platform does not favor certain groups of students over others.
   - Protect students' privacy by securely managing personal and educational data.
   - Ensure the platform is safe and supports positive educational outcomes.
2. **Stakeholder Engagement**:
   - Involve teachers, students, parents, and education experts in the design process.
   - Conduct workshops to gather feedback on the platform's features and ethical implications.
3. **Ethical Impact Assessment**:
   - Assess the potential impacts of personalized recommendations on student learning and well-being.

- Identify risks of reinforcing existing biases or educational inequalities.

4. **Design for Transparency and Explainability**:
   - Provide students and teachers with clear explanations of why specific content is recommended.
   - Offer transparency reports that outline the platform's decision-making criteria and processes.
5. **Implement Accountability Mechanisms**:
   - Designate educators to oversee the AI system's recommendations and intervene when necessary.
   - Develop audit logs to track the AI system's decisions and actions.
6. **Bias Mitigation**:
   - Use diverse datasets to train the AI system to avoid cultural or socioeconomic biases.
   - Continuously monitor the platform for biased recommendations and adjust algorithms as needed.
7. **Privacy and Data Protection**:
   - Implement strong data encryption and access controls to protect student data.
   - Ensure data is anonymized where possible and that data retention policies comply with legal requirements.
8. **Continuous Monitoring and Improvement**:
   - Regularly update the platform based on user feedback and new ethical standards.
   - Establish a review board to oversee the platform's ethical considerations and provide recommendations for improvement.

Chapter 2 – The most vulnerable professional sectors in data protection and digital rights.

2.1 The Health Sector

2.1.1 Introduction: The Importance of Digital Rights in the Health Sector

The digital transformation of healthcare has revolutionised how medical services are delivered and accessed, making healthcare more efficient, accessible, and patient-centric. However, with these advancements come significant concerns about digital rights, particularly regarding the privacy, security, and accessibility of personal health information. The importance of digital rights in the health sector cannot be overstated, as it directly impacts patient trust, safety, and the overall quality of care.

- **Privacy and Data Protection**

Health data is among the most sensitive types of personal information. It includes medical histories, diagnostic information, treatment records, and genetic data. Protecting this data from unauthorised access and breaches is crucial to maintaining patient confidentiality and trust. The GDPR sets stringent standards for handling personal health information, emphasising the need for explicit consent, transparency, and secure data storage and processing practices.

Heath Data Processing Notifications	
Bad Practices	**Good Practice**
The following expressions are ***not*** **sufficiently clear regarding the processing purposes**: • "*Your personal data may be used for the development of new services*" – It is not clear what "*services*" are involved and how this data will aid in their development; • "*Your personal data may be used to provide personalised services*" – It is not clear what this "*personalisation*" entails; • "*Your personal data may be used for research purposes*" – It is not clear which "*research*" it refers to	• "*Data about your previous purchases is stored, and details about the products you previously purchased are used so that we can suggest other products we believe you might also be interested in*" – The advertisement **purposes** and what **types of processed data** are clear; • "*We keep records of the articles you have accessed on our websites and use this information for targeted advertising on these websites that matches your interests, which we have determined based on the articles you have read*" – Both the **kind of personalisation** involved and **how data subjects' interests are determined** are clear

- **Patient Rights and Autonomy**

Digital rights in healthcare also encompass patient autonomy and the right to control one's own health information. This includes the right to access medical records, request corrections, and understand how data is used and shared. Ensuring that patients have these rights empowers them to make informed decisions about their health and fosters a collaborative healthcare environment where patients are active participants in their care.

- **Access and Equity:**

Digital health technologies should be accessible to all patients, regardless of their socioeconomic status, geographic location, or disability. This includes making health information systems and online services compliant with

accessibility standards. Bridging the digital divide in healthcare ensures that vulnerable populations receive equitable care and that health disparities are minimised.

Key Digital Health Initiatives: the Case of the Croatian CEZIH

Initiated in 2002, the **Central Health Information System of the Republic of Croatia** (**CEZIH**) aims to digitise and transform healthcare processes in Croatia, making the healthcare system more accessible to patients. It serves as a national integration platform for various information systems and applications within the healthcare sector. By centralising health data, CEZIH facilitates better coordination of care, reduces administrative burdens, and enhances the accuracy and availability of patient information.

However, **interoperability challenges** and **inconsistent data entry** practices hindered the implementation of CEZIH across the country. This resulted in **fragmented patient data** and **inefficiencies in healthcare delivery**. This case suggests that standardised data entry protocols and improved system integration strategies are crucial in ensuring a fair and efficient digital healthcare system.

2.1.3 Digital Rights Vulnerabilities in the Health Sector

Despite the advancements in digital health infrastructures, several vulnerabilities threaten the digital rights and freedoms of users and consumers in the healthcare sector.

- **Data Privacy and Security Breaches**

Health data is highly sensitive and valuable, making it a prime target for cybercriminals. This is why the healthcare sector faces significant risks related to data breaches and unauthorised access to personal health information.

For example, the centralisation of health data, while beneficial for care coordination, also presents a single point of vulnerability so that a **data breach** in such a system could expose the personal health of millions of patients. It is therefore crucial that robust cybersecurity measures and regular audits are in place.

Similarly, as healthcare workers need access to patient data to provide care, improper access controls can lead to **unauthorised access to and potential misuse of sensitive information**. Implementing strict access controls and monitoring systems can mitigate this risk.

- **Inadequate Patient Awareness and Education**

While privacy and data protection must be ensured at the institutional level, it is also important that users and consumers are able to directly safeguard their personal information. **Many patients, however, are unaware of their digital rights** concerning their health information, such as the right to access their medical records, request corrections, and understand how their data is being used. This can prevent them from taking necessary actions to protect their data.

At the same time, patients need to adequately understand how to securely access and manage their health information online, recognise phishing attempts, and use legal mechanisms for redress. It is therefore essential to enhance **digital skills** and **digital rights literacy** among them, especially older adults and those less familiar with technology.

- **Technological and Infrastructure Vulnerabilities**

The digitalisation of the health sector is steadily transforming healthcare systems. However, as adapting to digital solutions requires time, some institutions may still rely on **outdated infrastructures, processes, and techniques**, making them more susceptible to cyber-attacks and less efficient in handling data securely.

Meanwhile, the rapid adoption of digital health technologies introduces new challenges and vulnerabilities that current regulations may not fully address. Different health information systems and applications must seamlessly communicate and exchange data to provide comprehensive and coordinated care. **Interoperability issues** and **lack of standardised protocols and systems** can lead to fragmented care, data silos, and inefficiencies. Ensuring that all systems comply with interoperability standards is crucial for effective data exchange and patient care. Furthermore, **emerging technologies** like AI and the Internet of Things (IoT), while offering significant benefits, also introduce new risks and impact privacy and security in ways that may not be fully addressed by current regulations.

- **Regulatory and Enforcement Challenges**

Despite the existence of robust digital health regulations, limitations in scope and inconsistent enforcement pose risks to patients' rights and freedoms.

The **effectiveness of data protection regulations** depends on consistent implementation by regulatory bodies. Limited resources and capacity of bodies national authorities in digital health matters can hinder their ability to monitor compliance, address violations effectively, and thus protect users' and consumers' rights.

Moreover, the international nature of healthcare, particularly in the context of patient mobility within the EU, presents challenges for data protection. However, ensuring that data protection standards are maintained during **cross-border data transfers** is particularly challenging as healthcare providers might have to navigate through varying national and international regulations and different healthcare systems' policies.

Data Breach in a Croatian Healthcare Institution: a Case Study

In 2021, a major hospital in Croatia experienced a data breach where sensitive patient information was accessed by unauthorised personnel. Insufficient cybersecurity measures, as well as outdated IT infrastructures, made it possible for many patients' data to be compromised. This eventually brought the hospital's representatives to court and resulted in a loss of trust in the institution by Croatian citizens.

This case highlights the importance of staff training on data protection, but also the need for regular security audits and the constant update of cybersecurity protocols.

2.1.4. Digital Regulations' Shortcomings: Gaps in Existing Laws Concerning Digital Rights in the Health Sector

While the healthcare sector has made significant strides in digitising its services and aligning with European standards, several gaps and shortcomings in existing laws still pose challenges to patients' digital rights. These flaws also affect the sector's ability to comply fully with digital rights regulations and protect its consumers.

- **Fragmentation and Complexity of Regulations**

One of the significant issues can be the fragmentation and complexity of the regulatory framework governing health data. The **existence of different regulatory bodies**, for example, may diminish the harmony between national sector-specific regulations and data protection laws or foster overlapping regulations, thus leading to confusion

and inconsistency in data protection practices. At the same time, a unified regulatory framework should also include **clear, cohesive guidelines** ensuring consistent implementation of digital rights measures among healthcare providers.

- **Insufficient Resources**

Healthcare providers, particularly smaller clinics and general practitioners, often lack the resources needed to implement digital solutions and fully comply with the related regulations. For instance, implementing robust data protection measures like advanced encryption and secure data storage solutions requires **technical expertise and a financial capacity** that are not necessarily met by smaller healthcare providers. Similarly, **continuous training programmes and resources** are needed to keep staff updated on best practices and regulatory changes, but this may be too much of a burden for certain institutions.

In sum, the existence of robust legal frameworks for data protection in the health sector is not enough to fully ensure patients' rights and freedoms Addressing these issues requires a multifaceted approach that includes harmonising regulations, providing resources for compliance, strengthening enforcement mechanisms, addressing technological vulnerabilities, enhancing patient awareness and digital literacy, and improving cross-border data transfer processes.

2.2 The Social Sector – The Case of Homeless and Refugees

There are approximately **2.8 million** social economy enterprises in the European Union, employing 13.6 million people and representing **10%** of all businesses and 8% of the EU's GDP (European Economic and Social Committee 2017). Working across sectors and through cooperatives, mutual societies, associations, and foundations, social economy professionals try to solve wicked societal challenges like unemployment, poverty, democratic participation, and protection of fundamental rights. Their work often revolves around marginalised and vulnerable communities, such as homeless people and refugees.

2.2.1 The European Approach to Homelessness and Refugees

It is estimated that there are around **700,000** homeless people in the European Union (Develtere 2022). The EU addresses homelessness as a **social exclusion problem** that negatively affects people's physical and mental health, well-being, life expectancy, and access to many economic and social services. It is in this perspective that European institutions, governments, and civil society signed the **Lisbon Declaration** in 2021. The Declaration defines an integrated, housing-led approach that seeks to end – and not simply manage – homelessness and launches the **European Platform on Combatting Homelessness** to reinforce cooperation among stakeholders around this vision (Lisbon Declaration 2021).

Similarly, the EU has been actively working to establish an **effective, humanitarian, and safe European migration policy**. Despite the EU experiencing a significant decrease in irregular arrivals since the peak of the migration crisis in 2015 (Council of the European Union 2024), new geopolitical developments like the Russian aggression of Ukraine have fostered a new wave of refugees seeking asylum in the European continent (European Commission 2024b). Seeking a balance between humanitarian considerations and effective management, the EU recently proposed the **Pact on Migration and Asylum** to strengthen the management of asylum applications within its borders and distribute the burden more equitably among Member States (European Commission 2024a).

2.2.2 The Digitalisation of the Social Sector

The **digitalisation of the social economy** benefits service providers and beneficiaries by overcoming geographical barriers, improving access to accurate and fast information, and fostering innovative business models. Social sector professionals can take advantage of this enabling role of ICT to improve the effectiveness and magnify the outcomes of their solutions (Dionisio et al. 2023). Additionally, digital technologies expand the outreach of social service providers, enabling them to connect with hard-to-reach beneficiaries and raise broader awareness of their work (FEANTSA 2021, p. 15).

However, addressing societal challenges by digital means has often amplified already-existing problems and can create new ones. Professionals and recipients in the social sector are among the most exposed to the **risks of digitalisation**. In the context of privacy and data protection, the GDPR provides a comprehensive framework for protecting personal data and privacy rights, but it may not be able to fully address the specific vulnerabilities and circumstances affecting them.

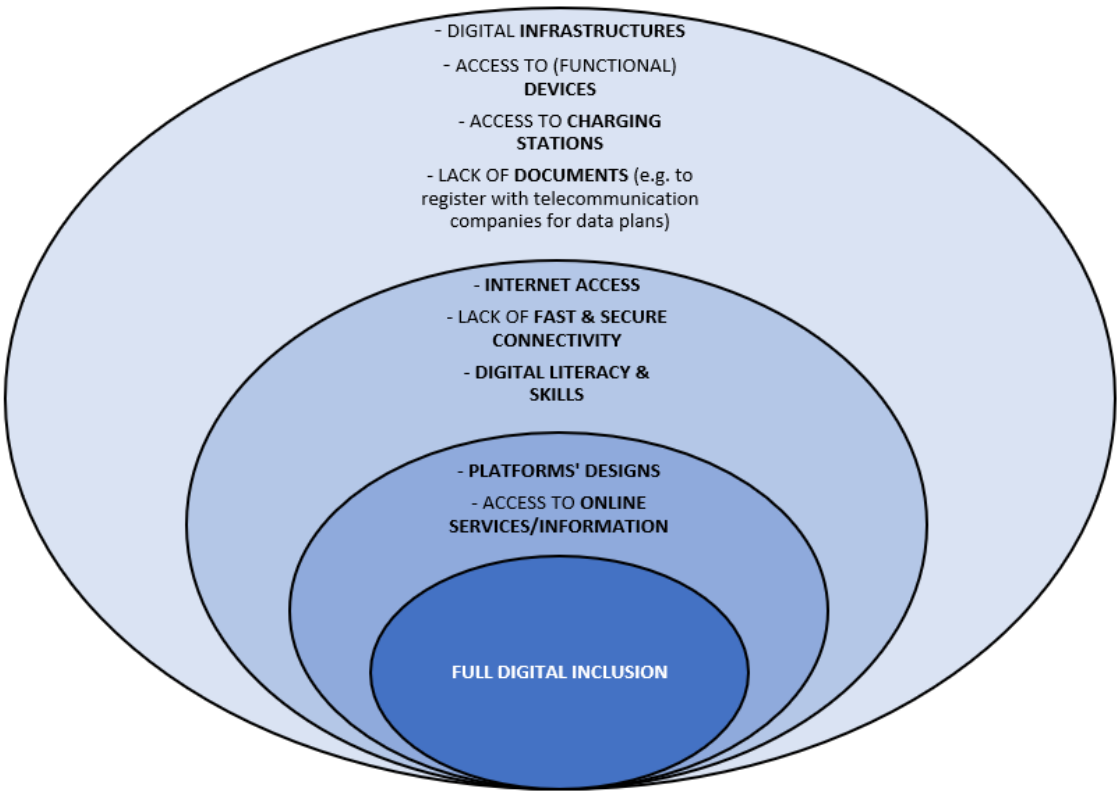
Due to their marginalised and often transient status, homeless people and refugees are particularly exposed to the unintended consequences and negative externalities of digitalisation. Embracing the digital transition in these contexts is a challenge for both humanitarian organisations and their beneficiaries.

2.2.3 Digital Exclusion

Marginalised groups have always been at the heart of debates about **digital inclusion and exclusion** – and the homeless and refugees are no different. 'Digital exclusion' can generically refer to situations where individuals or groups are unable or prevented from participating fully or partially in digital and online environments and/or practices (See also European Commission 2022).

Digital exclusion is usually associated with limited **access to the Internet**, lack of **fast and secure connectivity**, and lack of **digital literacy and skills**. Recognising these challenges, the EU strategic programme for the Digital Decade (**2030 Digital Compass**) and the **Action Plan for Digital Education 2021-2027** promote secure digital infrastructures to ensure universal connectivity and emphasise the importance of basic digital skills for all EU citizens (European Commission 2021), aiming to include socially excluded groups and criticising the lack of measures for lower-skilled adult learners and older people (European Commission 2020).

However, digital exclusion is a **multi-dimensional phenomenon**. While necessary, Internet access, connectivity, and digital skills only set the minimum threshold for digital inclusion. The marginalised groups' perspective clearly shows that other factors need to be accounted for to ensure real, meaningful digital inclusion.



Refugees and homeless people live in socio-economic conditions that make it difficult to afford **functioning devices** essential for digital connectivity. Even if they could obtain a suitable device, they would not have easy **access to charging stations**, due to their nomadic conditions. And even if these conditions were met, these groups would still face additional barriers, such as the **lack of necessary documents to sign a contract with telecommunications agencies**. Without these material bases, Internet access and connectivity remain extremely difficult. Moreover, access to online services and information can be further complicated by **platforms' unfriendly designs** – that is, platforms not designed to engage marginalised users (e.g., not adapted to certain devices, lacking alternative languages, or not suited to low digital skills).

Digital Exclusion: Special Case

Unlike refugees, homeless people are not subject to intense tracking and monitoring and may therefore experience another form of digital exclusion called "**data marginalisation**." Being excluded from the main data flows can mean invisibility in policy-making and greater difficulty in accessing online services.

In sum, **digital inclusion should not be focused solely on digital education and infrastructure**. Digital exclusion is not a polarized phenomenon (either present or absent) but is rather characterized by various nuances and levels of depth. Therefore, it is important to consider the factors contributing to digital exclusion as interconnected and interrelated.

Digital Exclusion of Homeless People: Data

A study conducted in **France in 2018** (Solinum 2019) found that:

- **91%** of homeless people had a mobile phone and **71%** had a smartphone;
- Only **55%** used the Internet daily;
- Up to **62%** never did administrative procedures online;
- **57%** had a personal email

2.2.4 GDPR Limitations

Entry barriers to the digital society represent just one of the struggles these communities endure concerning digital rights and risks. Unique life conditions expose homeless people and refugees to specific digital rights vulnerabilities that go beyond digital exclusion and may not be fully accounted for by existing laws.

First, **informing homeless individuals and raising their awareness** about data processing, consent, and their digital rights can be extremely difficult because of their transient life conditions as well as their anxiety and confusion about sharing information.

Informing Marginalised Pepole: Best Practices

The Connection at St. Martin-in-the-Field is a registered charity providing practical support to homeless people. In 2020, they conducted a study on their clients' main concerns relating to personal data aimed at identifying any misunderstandings that could threaten their trust and the most effective communication methods to address them (Connection at St. Martin 2020).

- **Key Messages tools**, **face-to-face information sessions**, and **Q&A opportunities** are valid alternatives to standard privacy notices;
- Ensuring frontline staff's competences through **role-based training** is crucial;
- **Conducting exercises** to assess the accessibility of privacy information materials and improve communication practices;
- **Simplified and tailored procedures to exercise data protection rights** should also be available

Moreover, marginalised groups often enjoy **precarious control over personal data** that is not considered in the GDPR:

- **Lack of Secure Storage**: These individuals are often compelled to share sensitive information such as health conditions, substance abuse histories, criminal records, refugee status, nationality, ethnicity, and traumatic experiences in order to benefit from service providers' assistance. However, data collection points like shelters, food banks, and social welfare programmes often lack robust and regulated data protection practices and do not always meet GDPR transparency requirements;
- **Cross-jurisdiction Data Transfers**: Refugees are especially vulnerable to undue data transfers across jurisdictions with different levels and standards of data protection.

All of this makes homeless people and refugees **more vulnerable to identity theft**, **discrimination, and unauthorised access** to personal data, exposing them to higher risks of data misuse or sharing with unauthorised parties.

Unique Risks of Data Misusage: Example

The digitalisation of the social economy faces challenges due to a global communications infrastructure that is susceptible to surveillance and infiltration by both state and non-state actors. Online requests for clients' sensitive information, especially from public entities, can be particularly dangerous. For example, between September 2016 and February 2017, the **UK Home Office** used data from charities in London to identify and deport European rough sleepers, while outreach workers were not aware of this misuse (The Guardian 2017)

The often complete dependence of the members of these on humanitarian assistance makes it **hard to balance out their data protection needs**. For instance, some individuals may be forced or compelled to share personal data even without meaningful choices or alternatives, problematising the idea of 'free consent' as exposed in the GDPR. That is probably why, at the beginning of GDPR's implementation period, obtaining informed consent from refugees for the collection and use of their data was rarely sought (D. Kaurin 2019). Similarly, the lack of official identification documents forces these people to rely on agencies, authorities, or complex networks of both, to register and process their personal data, exposing them to movement tracking and monitoring. Furthermore, when multiple, inter-agency data sharing is involved, it might be difficult to uphold GDPR's accountability standards (FEANTSA 2021).

While data controllers and processors may struggle to balance assistance and data protection needs, homeless people and refugees often experience **difficulties in directly exercising their digital rights**:

- the GDPR assumes **levels of digital literacy, access, and awareness that are not necessarily met** by people with limited resources and information concerning how their personal information is collected, processed, shared, and used;
- the **lack of a stable address** makes it difficult for homeless people and refugees to exercise their rights under the GDPR;
- the transient and marginalised status makes it harder for these people to **obtain the resources, support, or legal representation** necessary to access legal recourse or remedies for data protection violations.

2.2.4 Digital Surveillance

Since 2001, the so-called 'war on terrorism' has gone hand in hand with the global diffusion of new profiling technologies and the increase in access to digital data by public forces. The abuse of biometric profiling systems by national security and law enforcement agencies increases the **risks of unwarranted, unsafe, or undue data processing**. This is particularly troublesome as the GDPR primarily focuses on private-sector data controllers, often leaving public surveillance and data collection outside the provisions' scope.

Whether because of crossing borders or living in public spaces, refugees and homeless people are particularly exposed to **digital surveillance**. This can have significantly negative impacts on their ability to enjoy freedoms and rights:

- implicit prejudices against marginalised groups can lead to **biased data processing**, resulting in discriminatory algorithmic outputs that adversely affect their ability to receive help and support (United Nations 2022);
- the use of surveillance technologies can **exacerbate the marginalisation of homeless people and refugees**, making it harder for them to access essential services such as housing, healthcare, and employment opportunities;
- higher exposure to digital surveillance may **discourage homeless people and refugees from partaking in protests or public gatherings**, thus affecting their freedom of expression and assembly (D. Murray et al. 2024).

As Ben Hayes' article on *Migration and Data Protection* explains, data protection in the social sector was adopted late but also very rapidly. This led to a "*data-driven humanitarianism*" despite the organisations' vulnerability to state surveillance and lack of proper data protection mechanisms. In this context, social economy enterprises and humanitarian organisations hold a double role:

- **defenders of their beneficiaries' rights and best interests**;
- **users of the same interoperable technologies and partners of governments with multiple data interests**.

In the social sector, data protection often has a low priority, either because it is assumed that those needing assistance are happy to hand over their personal data to whoever requests it, or because it is supposed that 'privacy' and 'data protection' are essentially Western constructs with little appeal in other cultures or contexts. Without adequate protection of humanitarian data and with the growing adoption of interoperable technologies and partnerships with governments that use data for purposes beyond humanitarian aid, **social sector organisations risk inadvertently contributing to the surveillance of their beneficiaries** (B. Hayes 2017).

Digital Surveillance: the Case of the New EU Migration Pact

To provide a common political response and strike a balance between refugee protection and concerns over migratory pressures, the EU adopted the **Migration and Asylum Pact** on April 10, 2024. The Pact, however, encountered the resistance of more than 50 NGOs concerned about the **human rights risks** entailed by the new European tool (Picum 2023):

- The new screening and border procedures hold the potential for an increase in the arbitrary detention of migrants, racial profiling**,** and potentially discriminatory security checks on all individuals entering Europe irregularly.
- Additionally, the Pact will allow invasive technological practices at various stages of the asylum process, such as extracting data from mobile phones.
- Finally, the reform of the Schengen Borders Code will generali**s**e police checks for immigration enforcement, encouraging the use of surveillance, monitoring technologies, and 'crisis' procedures that can facilitate illegal pushbacks (Protection International 10 April 2024)

2.3 The E-commerce Sector

2.3.1. Introduction: The Importance of Digital Rights in the E-commerce Sector

In the modern digital economy, E-commerce has become a vital component of global trade, significantly impacting how businesses operate and how consumers interact with the marketplace. E-commerce, defined as **the buying and selling of goods and services over the Internet**, has grown exponentially in recent years. This growth is driven by technological advancements, increased Internet penetration, and the convenience of online shopping. As E-commerce continues to expand, the importance of digital rights within this sector becomes increasingly paramount.

- **Privacy, Data, and Consumer Protection**

E-commerce transactions involve the collection and processing of vast amounts of personal data, including names, addresses, payment information, and browsing habits. Protecting this data from unauthorised access, breaches, and misuse is essential to maintaining consumer trust and confidence. However, digital rights also include the protection of consumers from fraudulent activities, misleading advertisements, and unfair business practices. E-commerce platforms must ensure that consumers are informed about their rights, including the right to return goods, the right to refunds, and the right to receive accurate product information. Consumer protection laws at the national and European levels safeguard these rights by ensuring that E-commerce transactions are conducted fairly and transparently.

- **Freedom of Expression**

E-commerce platforms play a significant role in shaping online discourse, and their policies and practices can impact freedom of expression. For example, terms of service and community guidelines can restrict certain content, such as hate speech or controversial opinions, or algorithms used for content recommendations or search results can shape what information users see, potentially limiting diverse viewpoints. Moreover, differential pricing tiers and access levels can limit the diversity of content based on who can pay more and risk excluding marginalised voices (United Nations Human Rights Council 11 May 2016). This is why the digital marketplace should support the free exchange of ideas and information by allowing consumers to share reviews and feedback about products and services without fear of censorship or retaliation. At the same time, however, E-commerce platforms need to balance this freedom with the need to prevent harmful content, such as fake reviews or defamatory statements, which can mislead other consumers and harm businesses.

- **Access and Inclusion**

Ensuring that all individuals, regardless of their socio-economic status, location, or disability, have access to e-commerce platforms is a key aspect of digital rights. Not only excluding certain groups would perpetuate inequalities, but as people increasingly use E-commerce platforms as spaces for communication, expression, and exchange, denying access to anyone limits their ability to express opinions, share information, and engage in economic activities. It is thus important to strive for universal access to digital markets, including by making websites accessible to people with disabilities and ensuring that rural and underserved areas have reliable internet access. Inclusive e-commerce practices can help not only bridge the digital divide, providing equal opportunities for all consumers to benefit from the digital economy, but also encourage digital literacy and skills development, empowering users to navigate the digital landscape effectively.

The Significance of Digital Rights in E-Commerce: a Case Study

As E-commerce platforms collect vast amounts of user data, including browsing habits, purchase history, and preferences, the potential for misuse arises. In one study, the combination of data on the "likes" option on what used to be called “Facebook” with limited information from a survey allowed the scholars to accurately predict the sexual orientation of male users in 88% of cases, the ethnic background of users in 95% of cases, and the religious beliefs of users (Christian or Muslim) in 82% of cases. Researchers thus showed that **easily accessible digital records** of seemingly innocuous digital behavior can be used to **automatically and accurately predict intimate personal attributes**, raising important questions about personalised marketing and online privacy (Kosinski et al. 2013). Just like Facebook’s “likes”, E-commerce platforms use data analytics to create detailed user profiles and predictive algorithms to tailor recommendations, ads, and pricing, potentially revealing personal attributes and leading to **discriminatory practices**, the **perpetuation of biases**, or **invasion of privacy**.

In light of these considerations, it is clear that **a robust digital rights framework can have a profound economic and social impact in E-commerce**.

Digital rights are essential for a thriving e-commerce ecosystem, which drives economic growth. When consumers trust that their data is protected and their rights are respected, they engage more in online shopping, leading to increased sales and business expansion. This trust is built through transparent business practices, robust data protection measures, and responsive customer service, fostering long-term customer relationships and brand loyalty. Small and Medium-sized enterprises (SMEs) benefit particularly by reaching wider markets, enhancing their competitiveness, and innovating their business models.

Protecting digital rights also encourages innovation in the sector as businesses are motivated to develop new technologies and services that enhance privacy, security, and user experience. This drive for innovation propels the industry forward, creating new opportunities for growth and development. Secure payment systems, encryption, and user authentication methods are examples of innovations that have emerged to address digital rights concerns in E-commerce.

Finally, digital rights promote social equity by ensuring that all consumers have equal access to e-commerce benefits. This includes protecting vulnerable populations from exploitation and ensuring everyone can participate in the digital economy. Policies that promote digital literacy and provide resources for disadvantaged groups are essential for achieving social equity in e-commerce.

2.3.3. Digital Rights Vulnerabilities: Specific Threats to Users and Consumers

E-commerce users and consumers face several specific threats concerning their digital rights and freedoms. These vulnerabilities stem from various factors, including technological advancements, regulatory gaps, and evolving cyber threats.

- **Data Privacy and Security Breaches**

Despite stringent national and international regulations like the GDPR, E-commerce consumers are still vulnerable to data breaches and cyber-attacks. This is mainly due to the vast amounts of personal and financial information that are exchanged on E-commerce platforms, including payment details, addresses, and purchase histories, thus making them prime targets for cybercriminals seeking to steal data. High-profile **data breaches** can result in significant financial loss and identity theft for consumers, undermining trust in the platforms. Cybercriminals can

also use **phishing attacks**, such as fraudulent emails or websites that mimic legitimate e-commerce platforms, to deceive consumers into providing personal information or payment details. This puts to the fore the importance of increasing cybersecurity awareness and digital literacy among users, since those who fall victim to phishing can suffer financial and reputational losses and unauthorised transactions.

- **Misleading Information and Fraudulent Practices**

E-commerce consumers can also be susceptible to deceptive information and fraudulent activities. Some E-commerce platforms and sellers use **misleading advertisements**, such as false claims about product quality or exaggerated discounts, to attract consumers, but they may also include hidden costs: consumers thus make purchases based on incorrect or partial information, leading to dissatisfaction and financial loss. Moreover, the sale of **counterfeit products** pushes consumers to buy fake goods that are of inferior quality or unsafe without knowing, exposing them to financial and safety risks. Finally, some of the third-party sellers hosted by E-commerce platforms may engage in **fraudulent activities**, such as non-delivery of goods, incorrect or damaged items, and difficulties in obtaining refunds or returns.

Social Media Registration: an Example of Misleading Information

When registering for a social media platform via a desktop browser, users are encouraged to use the platform's mobile app. What appears to be another step in the sign-up process invites users to discover the app. However, when they click on the icon expecting to be directed to an app store, they are instead asked to provide their phone number to receive a download link via text message. **Explaining to users that they need to provide their phone number to receive a link to download the application is misleading**: there are multiple ways for users to access an app, such as scanning a QR code, using a direct link, or downloading it from the app store; these alternatives demonstrate that there is no mandatory reason for the social platform provider to request users' phone numbers.

- **Lack of Consumer Awareness and Digital Literacy**

While some efforts have been made to educate consumers about their rights under the GDPR and other relevant laws, these campaigns are often insufficient in scope and reach. Therefore, many consumers are not fully aware of their digital rights or how to protect themselves online. **Limited digital literacy** can make them more susceptible to online scams, phishing attacks, and other cyber threats. Similarly, a **lack of awareness** can prevent E-commerce consumers from taking action when their rights are violated, such as seeking refunds, returns, or compensation for data breaches. Educating consumers about safe online practices and their rights is thus crucial for mitigating these risks.

- **Technological Vulnerabilities**

The rapid advancement of technology introduces new vulnerabilities in the E-commerce sector. For example, the **security of online payment systems** relies on secure payment gateways in place and widespread consumer education about secure practices in order to protect their data. Moreover, with the increasing use of **mobile devices** for online shopping, consumers face additional risks like malware, unsecured Wi-Fi connections, and app-based vulnerabilities. Finally, **emerging technologies** introduce new challenges in the sector, such as Magecart and other AI-driven attacks targeting E-commerce storefronts, AI-powered bots taking over users' accounts, or AI models inadvertently leaking proprietary information and leading to breaches.

2.3.4. Digital Regulations' Shortcomings: Gaps in Existing Laws Concerning E-commerce

Despite the presence of robust legal frameworks at the national and European levels, several gaps and shortcomings still hinder the effective protection of digital rights and freedoms in the E-commerce sector.

- **Fragmentation and Overlap of Regulations**

While laws like the GDPR, consumer protection laws, and sector-specific regulations provide comprehensive protections, their coexistence can lead to **overlapping provisions**, confusion, and ambiguity in compliance requirements. In Croatia, for instance, the transparency of data processing and consumer rights is regulated by the GDPR and the Consumer Protection Act (Official Gazette of the Republic of Croatia 2022) respectively but their specific requirements and enforcement mechanisms can differ. When also responsibility over implementation is given to different authorities, as is the case for Croatia's AZOP for data protection and the State Inspectorate for consumer rights, overlapping laws can lead to **fragmented enforcement**, inconsistent application of the provisions, and creation of loopholes that can be exploited.

- **Inadequate Data Protection Measures**

Despite the stringent requirements of the GDPR, there are still gaps in the implementation of data protection measures.

Inadequate Data Protection Measures in E-commerce: an Example

Some mobile applications provide location services that allow users to find nearby restaurants offering discounts. However, the collected data is also used to create profiles of data subjects for marketing purposes to determine their preferences regarding food or general lifestyle. Data subjects expect their data to be used for finding restaurants, but not for receiving ads for pizza delivery just because the app determined they return home late. It is possible that this further use of location data is not consistent with the original purpose for which the data was collected, and therefore, the consent of the individual concerned may be required

In particular, SMEs often lack the resources and expertise needed to fully comply with GDPR requirements, such as conducting data protection impact assessments and implementing robust security measures. This can be particularly problematic in E-commerce because, while inadequate data protection undermines consumers' trust in and broadens public skepticism about the safety of small e-commerce enterprises, the **disparity in GDPR compliance** between large corporations and SMEs can create an uneven playing field, possibly stifling innovation and reducing the diversity of options available to consumers in the e-commerce market.

- **Gaps in Cross-Border Data Transfer Regulations**

The global nature of E-commerce often entails cross-border data transfers, which can complicate compliance with data protection regulations. While the GDPR provides mechanisms for cross-border data transfers, such as Standard Contractual Clauses (SCCs) and Binding Corporate Rules, the practical implementation of these mechanisms can be complex and burdensome for businesses. Moreover, differences in data protection regulations between countries can create challenges for businesses operating in multiple jurisdictions, leading to compliance difficulties and increased costs for ensuring that data protection measures meet varying international standards.

Gaps in Cross-Border Data Transfer Regulations: a Case Study

In July 2020, the EU Court of Justice (CJEU) delivered a landmark ruling in the so-called **Schrems II case**, which centered around the transfer of personal data from the EU to the United States by Facebook. The CJEU **invalidated the EU-US Privacy Shield framework**, which had allowed companies to transfer data between the EU and the US, citing concerns about US surveillance practices and lack of adequate protection of European citizens' data. While Standard Contractual Clauses (SCCs) were upheld as a valid transfer mechanism, the court emphasised that their use requires assessing the recipient country's legal framework. The Schrems II case **highlighted the global nature of data protection and the need for harmonised regulations**. The ruling disrupted data flows, affecting thousands of businesses relying on the Privacy Shield and pushing companies to conduct case-by-case assessments to ensure adequate protection when transferring data to non-EU countries and turn to alternative mechanisms (e.g. SCCs, Binding Corporate Rules) or localised data storage to comply with GDPR (Gabel and Hickman 2019)

)

- **Enforcement and Penalties**

Limited resources and enforcement capabilities of regulatory bodies lead to inconsistent enforcement of penalties for non-compliance, leaving some violations unpunished, diminishing the integrity of data protection laws, and possibly discouraging adherence to data protection standards in the E-commerce sector.

2.4 The Education Sector: Focus on Primary Schools

The European approach to education has undergone significant transformation over the past few decades, progressively recognising its critical role in fostering economic growth, social cohesion, and overall well-being of its citizens. In particular, the Union places significant emphasis on **primary education** and its relevance in laying the foundation for lifelong learning and personal development.

At the same time, the EU emphasises the **importance of understanding the links between education and social conditions**, as factors like socioeconomic status and social environment significantly impact educational outcomes and social mobility. To address these issues comprehensively, the EU has developed a framework supporting high educational standards and social services, ensuring equal opportunities and social inclusion for all citizens.

2.5.1 The European Approach to Education

The EU's approach to education reflects a commitment to fostering inclusive, equitable, and high-quality systems that support the well-being and development of all citizens. It is guided by principles set forth in various treaties and strategic frameworks, such as the Treaty on the Functioning of the European Union (TFEU) and the Europe 2020 strategy, and foresees a role for the EU that primarily involves supporting and complementing the actions of Member States through policy coordination, funding programs, and fostering cooperation and exchanges.

The strategic framework for **European cooperation in education and training** (**ET 2020**) serves as the cornerstone for EU educational policy. It establishes common objectives for Member States to enhance the quality and efficiency of education and training systems, promote equity and social cohesion, and ensure lifelong learning for all.

Key initiatives under this framework include:

- **Erasmus+**: Launched in 2014, Erasmus+ is the EU's flagship program for education, training, youth, and sport. It aims to enhance skills and employability through learning opportunities, promote cooperation between education institutions and businesses, and support social inclusion and equity. Erasmus+ has significantly expanded mobility opportunities, allowing millions of students, educators, and trainees to study or train abroad, thereby fostering intercultural understanding and professional development (European Commission 2020a).
- **European Education Area (EEA)**: By 2025, the EEA aims to create a space where learning, studying, and researching are not hindered by borders. It focuses on inclusivity, quality education, and the recognition of diplomas across Member States, thereby facilitating mobility and cooperation (European Commission 2021b).
- **Digital Education Action Plan**: Recognising the transformative impact of digital technologies on education, the EU has developed the Digital Education Action Plan (2021-2027) to support the use of technology in education, enhance digital skills and competencies, and promote high-quality digital learning content and infrastructure (European Commission 2020b).

In particular, to prepare children for primary school and addressing educational inequalities from a young age, the EU promotes policies that ensure access to **high-quality early childhood education and care**:

- **Pathways to School Success**: In 2022, the Council of the European Union recommended adopting a systemic approach with integrated and comprehensive strategies, paying attention to for groups at risk,

and improving data collection to address underachievement, promote well-being, prevent bullying and early school leaving, and foster a positive learning climate (Council of the European Union 2022).

By focusing on foundational learning, early intervention, digital competence, and teacher development, the EU aims to create a robust educational framework that supports lifelong learning and social inclusion.

Social Policies Contributing to EU Education

The 2017 **European Pillar of Social Rights** includes social policies sets out principles and rights that are essential in ensuring inclusive, equal and fair education for all students:

- **European Social Fund Plus (ESF+)**: As the EU's main financial instrument for investing in people, the ESF+ supports education and social inclusion, enhancing the quality of education and training, addressing disparities and promoting inclusive education, and funding projects that address skills mismatches, and support vulnerable groups (European Commission 2021a).
- **Youth Guarantee**: Launched in 2013, the Youth Guarantee seeks to ensure that all young people under 25 receive a good quality offer of employment, continued education, apprenticeship, or traineeship within four months of becoming unemployed or leaving formal education (European Commission 2020c).
- **European Child Guarantee**: Adopted in 2021, the European Child Guarantee aims to prevent and combat child poverty and social exclusion by ensuring that children in need have access to key services such as healthcare, education, childcare, housing, and adequate nutrition (European Commission 2021c).

2.5.2 Vulnerabilities of the Education Sector: an Overview

Despite significant progress, the EU Education sector still faces several challenges that can undermine their effectiveness and equity. As digital technologies become increasingly integrated into educational environments, these include digital rights vulnerabilities related to socio-economic disparities, digital divide and data privacy concerns that can impact students, teachers, and institutions.

2.5.2.1 Socio-Economic Disparities and Inclusion

Socio-economic disparities across and within Member States pose a significant challenge to achieving inclusive education. With the digitalisation of the Education sector, equitable access to quality educational opportunities and inclusiveness in education processes are finding new barriers.

- **Digital Divide**

While digital technologies have the potential to enhance learning and social inclusion, the digital divide represents a significant vulnerability in both education and social inclusion, exacerbating existing inequalities and especially creating educational obstacles for vulnerable groups, such as migrants, ethnic minorities, people with disabilities. In general, **inequitable digital access contributes to opportunity gaps** as students with better access have more opportunities for learning, research, and skill development.

In particular, ensuring **equitable access to digital tools, infrastructure, and skills** is critical. Students from underserved backgrounds and remote areas have fewer devices compared to their more advantaged peers and limited access to laptops, tablets, or smartphones hinders their ability to engage in the increasingly pervasive digital learning environments. Similarly, lower-quality internet connections are common among disadvantaged students and slow or unreliable Internet can affect their participation in online classes, research, and communication.

- **Cyberbullying**

Cyberbullying is the use of digital technologies to harass, threaten, or intimidate someone. It involves repeated aggressive behavior intended to cause harm or distress and can occur through various online platforms, including social media, messaging apps, emails, and websites.

Cyberbullying: Key Characteristics			
Anonymity	**Persistence**	**Public Exposure**	**Variety of Forms**
Perpetrators can often hide their identities, making it harder for victims to identify and confront them	Digital messages and posts can be shared widely and remain accessible for long periods	Cyberbullying can occur in public forums, leading to widespread humiliation and embarrassment for the victim	It can take many forms, such as spreading rumors, sending threatening messages, sharing private information or images without consent, and creating fake profiles to impersonate and defame the victim

Cyberbullying has significant impacts on education, affecting both students' well-being and their ability to learn. The **emotional toll** on young people can manifest as anxiety, depression, loneliness, sleep disturbances, and unhappiness, affecting their overall well-being, causing struggles in concentration and focus in class, leading to decreased motivation, engagement in learning, and academic performance. Moreover, persistent cyberbullying can lead to long-term, chronic stress, affecting cognitive functioning and memory, **impacting also students' future employment prospects** (Cowie 2018).

2.5.2.2 Data Privacy and Security

The increasing use of digital technologies in education raises concerns about data privacy and security, as they play a fundamental role in maintaining trust and protecting the rights and well-being of students, educators, and institutions.

- **Protecting Personal Information**

In the Education sector, the privacy and data protection requirements of regulations like the GDPR acquire great significance. To the extent that education is aimed at training the new generations in accordance with their aspirations and the values that inform today's societies, educational institutions have an **ethical obligation** to protect the privacy and security of the data they collect and manage more than other entities in different sectors. Education providers must therefore comply with existing regulations like the GDPR, ensuring transparency and accountability in their data processing activities.

Educational institutions collect and store a wide range of sensitive personal information, including student records, health information, financial details, and family data. Data breaches and cybersecurity threats can compromise this information, leading to **identity theft**, **financial fraud**, and other forms of exploitation, as well as **damage institutions' reputation**.

Secure digital environments allow educators and students can focus on learning without concerns about data breaches or misuse of information, and at the same time encourage the use of educational technologies and the development and implementation of innovative educational tools and methods.

- **Ensuring Safe Learning Environments**

Ensuring that users' information remains confidential is further challenged by specific **technical weaknesses and operational threats** within educational infrastructures. For example, outdated software, inadequate access controls, and insufficient cybersecurity measures can be exploited for unauthorised access, data theft, and other malicious activities.

Lack of adequate cybersecurity measures expose educational institutions to **hacking, phishing, malware, and other cyber threats** that can disrupt educational activities and compromise sensitive information.

Risk of Ransomware Attack: Example

In 2020, a major data breach occurred in the education sector. The University of California, San Francisco (UCSF) was targeted by a ransomware attack, resulting in the encryption of critical data and a ransom payment of $1.14 million to recover access. The breach exposed personal information of students, faculty, and staff, highlighting vulnerabilities in the educational institution's cybersecurity infrastructure (TechCrunch 2020). Such incidents not only **jeopardise the privacy of individuals** but also **cause financial and reputational damage to educational institutions**. This is only an example of several other similar cases that happen every year

To address these data privacy and security vulnerabilities, **a combination of advanced technological solutions and robust legislative measures is essential**. These tools not only help protect user data from unauthorised access and cyber threats but also ensure compliance with data protection regulations such as the GDPR. One such tool is the implementation of end-to-end encryption, which can secure data in transit and at rest, ensuring that intercepted data remains unreadable to unauthorised parties. Moreover, ensuring that digital learning platforms are secure helps protect students from online harassment and cyberbullying.

While educational institutions implement various measures to safeguard user information, however, teachers and students also play a crucial role in ensuring their own digital safety. Here are some practical tips to help users navigate the digital landscape safely and confidently:

Protecting Personal Information	Recognising Scams and Threats	Using Security Features
Avoid sharing sensitive information, such as passwords or financial details, over unsecured networks or public Wi-Fi	Be vigilant about phishing attempts, where attackers pose as legitimate entities to steal personal information. Warning signs include **unsolicited messages** asking for sensitive information, links to **unfamiliar websites**, and attachments from **unknown senders**	Activate the **security features offered by service providers**, such as regular updates of devices and software, enabling firewalls, and using encryption tools
Use strong, unique passwords for different accounts and change them regularly	**Verify the authenticity of emails and messages** before clicking on links or downloading attachments	Employ **multi-factor authentication** (**MFA**) to add an extra layer of security to accounts

Educate yourself about the latest cybersecurity threats and best practices for online safety	**Report** suspicious activities or potential security threats to relevant authorities or IT support	Utilise **secure communication platforms** that offer end-to-end encryption for sensitive information

2.5.2.3 Transparency

To ensure an overall privacy and data protection for students and educators, **transparency and accountability requirements** have been introduced in both the Education and Social inclusion sectors through various laws and regulations. Under the GDPR, Article 12 mandates that information intended for the public or data subjects is easily accessible and easy to understand, using clear and simple language. However, several factors can undermine transparency and accountability in these sectors:

1. **Complex and Ambiguous Policies**: Privacy policies and consent forms often use technical jargon and legal language, making them difficult for the average user, especially students and socially disadvantaged individuals, to understand.
2. **Regulatory Compliance Challenges**: Educational and social service providers must navigate different data protection regulations across countries and adapt to evolving legal landscapes, which can complicate compliance efforts.
3. **Entanglement with Government Affairs**: In many countries, educational institutions and social service providers may be required to cooperate with government authorities for various purposes, including national security and social welfare. Such cooperation, often conducted without proper supervision or user awareness, can lead to concerns about surveillance and data misuse.

Transparency & Social Media: a Case Study

These obstacles to transparency and accountability are especially worrying when the education sectors involves the **use of social media platforms**. In 2020, it was revealed that several universities in the United Kingdom had provided student data from social media platforms to government agencies monitoring protests. This included **tracking student activities and affiliations through their social media accounts**, raising significant privacy concerns and highlighting the need for greater transparency and accountability in how data is shared and used among education providers (The Guardian 2020)

2.5.2.4 Censorship in Social Media in the Education & Social Inclusion

Social media platforms play a critical role in education as a mean of promotion and communication and in social inclusion by providing a means for marginalised communities to access information, express their views, and connect with others. However, their functions in these sectors is undermined by several challenges related to censorship.

Social media censorship involves the suppression or regulation of content that is shared on social media platforms. This can be due to various reasons, including political pressure, legal requirements, or platform policies aimed at curbing misinformation and hate speech. While some level of content moderation is necessary to prevent harm, excessive or politically motivated censorship can have detrimental effects on education and social inclusion.

- **Political Censorship**

Governments may compel social media platforms to block or filter access to certain content or accounts deemed politically sensitive. This can limit access to critical information and restrict freedom of expression, especially for marginalised communities and human rights activists.

Political Censorship: a Case Study

During the 2020 protests in Belarus, **social media platforms were pressured by the government to remove content related to the protests**. This included posts, videos, and live streams documenting police violence and human rights abuses. Such actions significantly hampered the ability of protesters to organise and communicate, impacting their efforts to advocate for their rights (Human Rights Watch 2020)

- **Content Moderation Policies**

Social media companies have content moderation policies to prevent the spread of harmful content such as hate speech, misinformation, and violence. However, these policies can sometimes be inconsistently applied or overly broad, leading to the removal of legitimate content that is crucial for critical information, social inclusion, and advocacy.

Content Moderation Censorship: a Case Study

In 2021, **Facebook's automated moderation system mistakenly removed posts from indigenous activists** in Canada that were raising awareness about the discovery of unmarked graves at residential school sites. The removal of these posts hindered efforts to highlight historical injustices and mobilise community support for the affected families (CBC News 2021)

- **Economic Censorship**

Social media platforms may also engage in practices that favor certain types of content over others for economic reasons. For example, content from large, profitable accounts or advertisers may be prioritised over grassroots movements and non-profit organisations, limiting their visibility and outreach capacity.

Economic Censorship: a Case Study

In 2018, it was reported that changes in Facebook's algorithm resulted in **decreased visibility for non-profit organisations and community groups**, while content from major advertisers and popular influencers was given more prominence. This shift made it harder for smaller organisations to engage with their audiences and advocate for social causes (The Atlantic 2018)

By affecting the flow of information, social media censorship can undermine the educational potential of social media and impede efforts to foster a more inclusive society:

- **Restriction of Access to Information**: When social media platforms censor content, they reduce the diversity of opinions and information available online. This undermines users' right to access information and can create an information vacuum, limiting individuals' ability to form informed opinions. This is especially dangerous for children and young people, as social media often contribute to shaping the public opinion of the new generation of voters.

- **Suppression of Social Movements**: Censorship can stifle social movements by limiting their ability to communicate, organise, and mobilise support. This is particularly detrimental for marginalised communities that rely on social media to amplify their voices and advocate for their rights.
- **Loss of Skills**: Social media is a crucial part of modern communication and censorship prevents students from developing essential digital literacy and critical thinking skills, including evaluating sources, questioning and engaging with complex issues, understanding bias, and navigating online spaces.
- **Impact on Free Expression**: Excessive censorship can lead to chilling effects on expression, such as through self-censorship where individuals and organisations avoid discussing and sharing sensitive issues, controversial topics, or dissenting views for fear of being banned or having their content removed. This limits the public discourse, open dialogue, and intellectual growth and hinders progress towards social inclusion and justice.

2.5 The Telecommunications Sector

Concerned with exchanges of information over significant distances by electronic means, the modern **telecommunication sector** (also referred to as 'telecom') is at the heart of the digital transition. As such, an error, a mistake, or a threat in this sector can have profound consequences on the digital economy, its subjects, and their rights.

2.5.1 The European Approach to Telecommunications

The European regulatory framework for telecommunication services, networks, and technologies evolved significantly over the past 25 years. The **liberalisation** of the telecom markets in the early 1990s encouraged new market entrants, reduced barriers to investment and innovation, improved services, and enhanced consumer choice (Cave et al. 2019).

Cutting across the various aspects of the digital economy, the telecom sector became an integral part of the **Digital Single Market** (**DSM**) strategy of the European Commission. To create a fully integrated digital economy across the continent, the DSM sets forth specific objectives for telecommunications, including eliminating roaming charges for mobile phones across Europe, ensuring seamless access to services and content, and creating a level playing field for companies across the EU (European Commission 2015).

In this perspective, the European Commission launched a comprehensive **review of EU telecom rules** in 2015 to adapt them to the evolving digital landscape (European Commission 24 July 2015). As a result, the EU approach to the telecom sector now includes policies and rules addressing a wide range of topics, from cybersecurity and connectivity to competition and consumers' rights:

- The 2018 **European Electronic Communications Code (EECC)** is a revision of the entire EU regulatory framework for the telecommunications sector. It aims to facilitate the rollout of 5G networks and high-speed broadband by modernising the EU rules on electronic communications, including fixed and mobile networks, radio spectrum management and allocation, access to networks, and consumer rights. It also devises an Incident Reporting Framework for significant incidents affecting telecom services (European Parliament and Council of the European Union 2018b)
- The 2014 **Broadband Cost Reduction Directive** (**BCRD**) facilitates and incentivises the roll-out of high-speed electronic communications networks by promoting the joint use of existing physical infrastructure, enabling more efficient deployment of new infrastructure, and thus lowering deployment costs (European Parliament and Council of the European Union 2014).
- The 2015 **Telecommunications Single Market** (**TSM**) **Regulation** fosters the creation of a single European market for electronic communications by harmonising rules across Member States, promoting investment in high-speed networks, and improving consumer protection. The Regulation enshrines the **principle of Net Neutrality**, ensuring that internet service providers treat all data traffic equally without discrimination or interference, thus safeguarding consumers' access to an open Internet (European Parliament and Council of the European Union 2015)
- The 2022 **Roaming Regulation** requires domestic providers to allow customers to access regulated voice, SMS, and data roaming services from alternative roaming providers and ensures that consumers can use mobile services at domestic rates when travelling within the EU, reducing roaming charges and promoting connectivity across borders (European Parliament and Council of the European Union 2022).

In 2018, the **Body of European Regulators for Electronic Communications** (**BEREC**) was established as the entity responsible for assisting EU and national authorities in the implementation of EU telecom rules. It promotes consistent and cooperative regulatory approaches, provides advice and guidelines, and complements national regulatory tasks (European Parliament and Council of the European Union 2018a).

2.5.2 Vulnerabilities of the Telecom Sector

Within this strategic and institutional framework, the EU strives to balance the economic objectives of the telecom sector with the protection of citizens' and consumers' rights. Nevertheless, there are **policy, privacy, and human rights vulnerabilities** related to how telecom companies handle data, cooperate with governments, and impact societal and individual rights, including privacy, freedom of expression, and access to information.

2.5.2.1 Data Privacy & Security

Under the GDPR, telecom companies must ensure data transparency, obtain user consent, implement data protection measures, and notify authorities and affected individuals in case of data breaches. Despite these safeguards, however, data breaches, hacking, unauthorised access, and misuse in the telecom sector are particularly dangerous for individuals' privacy and confidentiality, trust in telecom services, and overall cybersecurity, because **telecom companies handle large volumes of personal data** (such as call records, text messages, internet usage logs, location data, etc.).

Heightened Risk of Data Breaches: Example

In 2021, a significant data breach occurred in the telecom sector. CloudSEK, a cybersecurity firm, discovered that the personal data of **750 million telecom users** in India was being sold on the dark web. The leaked data included personally identifiable information from all major telecom providers. Exposed data left individuals vulnerable to **cybercrimes** like identity theft and fraud, increasing the risks of **financial losses**, while telecom operators and government entities suffered **reputational damage** (Chakravarti 2024)

Ensuring that users' conversations, messages, and data remain confidential is further challenged by specific **technical weaknesses and operational threats** within the telecommunications infrastructure and services. For example, the so-called "**Signaling System Number 7**" (**SS7**) and "**Diameter**" are critical protocols used by fixed and mobile network operators for interconnection between networks. Unfortunately, both protocols have significant security weaknesses that can be exploited for wiretapping, intercepting phone calls and messages, tracking users' movements, and other fraudulent activities (Lyons 2024).

Therefore, to address the numerous data privacy and security vulnerabilities in the telecommunications sector, a **combination of advanced technological solutions and robust legislative measures** is essential. These tools not only help protect user data from unauthorised access and cyber threats but also ensure compliance with data protection regulations such as the GDPR. One such tool is the so-called "**end-to-end encryption**," a method to transform data on the sender's device into a secure format that can only be accessed with a decryption key on the recipient's device. In telecommunications, end-to-end encryption finds common application in instant messaging platforms, internet voice communications, and popular apps like WhatsApp, Signal, and Telegram. This ensures that data is not decrypted along the transmission path and that intercepted data remains unreadable to unauthorised parties.

The Security and Privacy Dilemma: the Case of End-to-end Encryption
How much of our personal information are we willing to give up for the promise of a safer online experience? **Sometimes, security and privacy are at odds with each other**. An article in *Politico* sheds light on how a proposal for a permanent law on fighting and preventing online child sexual abuse might inadvertently compromise existing privacy measures. Proposed in 2020 by the European Commission and recently adopted by the Parliament, this regulation would mandate internet platforms, including end-to-end encrypted messaging apps like Signal and WhatsApp, to detect, report, and remove images of child sexual abuse shared on their platforms. Yet, to achieve this, platforms would need to automatically scan every message, thus breaching end-to-end encryption and jeopardising users' privacy (Gregorová 2022)

While telecom companies implement various measures to safeguard user information, individuals also play a crucial role in ensuring their own digital safety. In the face of such challenges, telecom **users need to be proactive in protecting their data privacy and security**. The following practical tips can help empower users to navigate the digital landscape safely and confidently:

Protecting Personal Information	Recognising Scams and Threats	Using Security Features
Avoid sharing sensitive information, such as passwords or financial details, over **unsecured networks or public Wi-Fi**	Be vigilant about **phishing attempts**, where attackers pose as legitimate entities to steal personal information, and their warning signs: • unsolicited messages asking for sensitive information, • links to unfamiliar websites, • attachments from unknown senders	Activate the **security features** offered by telecom providers, such as • call blocking to prevent spam calls, • messaging apps with end-to-end encryption, • regular updates of devices and software

2.5.2.2 Transparency

Transparency and accountability requirements for the telecom sector have been introduced in many countries through different laws and regulations. Within the GDPR, Article 12 requires that information intended for the public or the data subject is easily accessible and easy to understand and that simple and clear language is used. However, there are at least three main factors that undermine the sector's capacity for transparency and accountability:

4. **complex and ambiguous privacy policies** might be difficult to understand for the average user, especially when using technical jargon;
5. **regulatory compliance** might be challenging for telecom companies operating across countries with different data protection regulations, or within evolving regulatory landscapes;
6. the telecom sector is often entangled with government affairs and, in many countries, companies are legally obliged to cooperate with government authorities for national security purposes, criminal investigations, and other reasons; however, **cooperation with governments** often takes place without proper supervision or user awareness and can contribute to mass surveillance.

Cooperation with Governments: a Case
In 2013, Amnesty International and other rights organisations brought a case against the **United Kingdom**'s intelligence agency GCHQ for secretly intercepting and processing the private communications of millions of people daily. On 25 May 2021, the **European Court of Human Rights** (ECHR) ruled that the UK government's bulk interception of communications powers violated the rights to privacy and freedom of expression under the European Convention on Human Rights. The ECHR reiterated that **mass interception must be subject to prior independent or judicial authorisation** to ensure adequate safeguards against abuse of power (Amnesty International 2021)

2.5.2.3 Net Neutrality and Censorship

Telecommunications companies provide the infrastructure needed to access the Internet, including wired and wireless networks, data centres and other data transmission technologies. These companies have the **power to influence how data is transmitted and received**, and thus can significantly shape users' online experience and impact their freedoms and rights.

The Principle of Net Neutrality: Definition	
Net neutrality ensures that Internet service providers (ISPs) **treat all online traffic equally and openly**, without discrimination, blocking, throttling, or prioritisation based on content, application, service, terminal, sender, or recipient. The EU upholds this principle by granting end-users the right to access and distribute *lawful* information, content, applications, and services of their choice, using any terminal equipment, regardless of the location or origin of the provider or service	
Exceptions	• compliance with legal obligations • network integrity • congestion management in exceptional and temporary situations

The Telecommunications Single Market (TSM) Regulation gave national authorities new regulatory, supervisory, and enforcement functions to ensure **users' right to an open Internet** (Art. 3). However, the net neutrality principle remains exposed to risks of violations due to:

- **Political Reasons**: telecommunications providers may be compelled by governments to block or filter access to specific websites, social media platforms, or content deemed objectionable or politically sensitive;
- **Economic Reasons**: ISPs and related stakeholders may monetise internet traffic through paid prioritisation and exclusive deals, gain competitive advantages by favouring their own services, or stifle market players' public outreach and innovation capacity.

Measures Breaching Net Neutrality: Examples		
Blocking Websites	**Social Media Filtering**	**Removal of Content**
Telecoms providers can block access to certain websites, including news sites, blogs, and independent media platforms	Social media platforms can be filtered for specific content or hashtags, limiting the dissemination of certain information. In the most extreme cases, entire platforms can be blocked	Providers may be required to remove specific content

Violations of net neutrality have several consequences:

- **Restriction of Access to Information:** When telecoms promote or demote certain content, they reduce the diversity of opinions and information available online, undermining users' right to access information. Censorship, content blocking, and other restrictions to diverse sources of information create an information vacuum, limiting individuals' ability to form informed opinions. When backed by governments, blocking and filtering for the suppression of dissent and political opposition are complemented by the possibility of surveillance and punitive actions, which can further dissuade individuals from freely expressing their opinions.

Content Blocking and Freedom of Expression: a Case

Net neutrality rests upon a delicate and ever-changing **equilibrium between legitimate security concerns and the preservation of fundamental human rights**.

The ECHR mandates that any state or private action to block, filter, or remove Internet content must comply with **Article** 10 of the **European Human Rights Convention**, ensuring freedom of expression. This involves a three-fold test to determine whether the interference is:

1. "prescribed by law" and clear enough for individuals to understand;
2. pursuing legitimate aims; and
3. "necessary in a democratic society."

In 2020, the ECHR ruled against a Russian court's order requiring a website owner to remove information on prohibited filter-bypassing tools to avoid site blocking. The ECHR found the order **arbitrary**, as it failed to consider the legitimate uses of such technologies, interfered with access to all content that might be accessed using those technologies, and lacked a specific legal basis (Safety of Journalists Platform 2022)

- **Discriminatory Economic Practices:** Violations of net neutrality can lead to discriminatory practices where **certain types of Internet traffic are prioritised over others**. For example, a service provider could accelerate traffic for video streaming services that pay a premium rate, while slowing down traffic for competitors who don't pay.
- **Impact on Competition and Innovation: Startups and small businesses** may not be able to pay for priority access, putting them at a **disadvantage** compared to large market players. This can stifle innovation and reduce competitiveness, as new ideas and services may not reach the public effectively.

Zero-rating Practices: a Case

Telecom companies engaging in zero-rating practices give unfair advantages to certain online services by making other data traffic more expensive and thus less attractive to consumers.

Telenor Hungary, a major national internet service provider, offered zero-tariff packages (bundles) to its customers, allowing unlimited access to specific applications. On 15 September **2020**, the **Court of Justice of the European Union** (**CJEU**) ruled against such practices as breaching net neutrality under the TSM Regulation (Ahava 2020)

Conclusions

The Digital Ethics Culture (DEC) project has laid a solid foundation for understanding and addressing digital rights issues within the EU, particularly in the context of Italy and Croatia. By examining critical regulations such as the GDPR, national data protection laws, and emerging frameworks like the AI Act, this Manual has highlighted the complex landscape of digital regulation and its implications for various professional sectors.

The insights into digital rights vulnerabilities across health, social services, e-commerce, education, and telecommunications sectors have underscored the importance of robust data protection measures. For Small and Medium-sized Enterprises (SMEs), which often struggle with limited resources and expertise, the challenges of complying with GDPR and other regulations are particularly pronounced. These challenges can lead to gaps in implementation, thereby risking the infringement of digital rights in the e-commerce sector and beyond.

This Manual not only aims to inform and educate but also to empower users to navigate and advocate for their digital rights effectively. As the digital landscape moves forward, it is crucial for stakeholders, including businesses, regulators, and consumers, to collaborate in fostering a culture of digital ethics. By doing so, the digital transformation will benefit all members of society while protecting fundamental rights. The DEC project and this Manual represent important steps toward achieving these goals, providing a comprehensive resource for understanding and addressing the digital rights challenges EU citizens face today.

Reference List

Chapter 1.1 – The Regulation (EU) 2016/679 of the European Parliament, or GDPR

Council of Europe. 28 July 1981. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. European Treaty Series 108. https://rm.coe.int/1680078b37 (Accessed on 24/06/2024)

Cour Européenne des Droits de l'Homme. 2022. Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence, pp. 49-65. https://www.echr.coe.int/documents/d/echr/Guide_Art_8_ENG (Accessed on 24/06/2024)

European Parliament and Council. 1995 Directive 95/46/EC "On the protection of individuals with regard to the processing of personal data and on the free movement of such data." In *Official Journal of the European Union L281*, pp. 31-50. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046 (Accessed on 24/06/2024)

European Parliament and Council. 2016. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)." In *Official Journal of the European Union L119*, pp. 1–88. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (Accessed on 24/06/2024)

Chapter 1.2 – Italian Privacy and Data Protection Regulations

Iaselli, M. 17 August 2019. "Diritto all'oblio può prevalere su vicende di cronaca passata". In *Altalex* https://www.altalex.com/documents/news/2019/08/17/diritto-oblio-puo-prevalere-vicende-cronaca-passata (Accessed on 24/06/2024)

Official Journal of the Italian Republic. 31 December 1996. Law No. 675 "Protection of Personal Data. (1996)." https://www.gazzettaufficiale.it/eli/id/1997/01/08/097G0004/sg (Accessed on 24/06/2024)

Official Journal of the Italian Republic. 30 June 2003. Legislative Decree No. 196 "Personal Data Protection Code. (2003)". https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2003-07-29&atto.codiceRedazionale=003G0218 (Accessed on 24/06/2024)

Olivi G. 2024. "Italy - Data protection overview". In *OneTrust Data Guidance*. https://www.dataguidance.com/notes/italy-data-protection-overview (Accessed on 24/06/2024)

Panetta R. 11 September 2018. "Un'analisi del quadro di responsabilità e del regime sanzionatorio derivante dal combinato disposto del GDPR, del decreto di armonizzazione delle leggi nazionali al Regolamento Ue e delle norme del Codice Privacy sopravvissute. Tutto quello che c'è da sapere". In *Agenda Digitale* https://www.agendadigitale.eu/sicurezza/privacy/gdpr-sanzioni-e-responsabilita-tutto-cio-che-ce-da-sapere (Accessed on 24/06/2024)

Saetta B. 2022. “Codice in materia di protezione dei dati personali”. In *Protezione Dati Personali* https://protezionedatipersonali.it/codice-protezione-dati-personali (Accessed on 24/06/2024)

Chapter 1.3 – Croatian Privacy and Data Protection Regulations

Central State Office for the Development of the Digital Society. 2022. Digital Croatia Strategy for the Period Until 2032. https://rdd.gov.hr/UserDocsImages/SDURDD-dokumenti/Strategija_Digitalne_Hrvatske_final_v1_EN.pdf (Accessed on 24/06/2024)

Čizmić, J. and Boban, M. 2018. "Učinak nove EU Uredbe 2016/679 (GDPR) na zaštitu osobnih podataka u Republici Hrvatskoj." In *Zbornik Pravnog fakulteta Sveučilišta u Rijeci, 39* (1), pp. 377-410. DOI: 10.30925/zpfsr.39.1.13. https://hrcak.srce.hr/199759 (Accessed on 24/06/2024)

Danko, B. 2019. Zaštita osobnih podataka s posebnim osvrtom na društvene mreže. https://repozitorij.unin.hr/islandora/object/unin%3A3053/datastream/PDF/view (Accessed on 24/06/2024)

Politiscope. 2021. Analiza rada Agencije za zaštitu osobnih podataka. https://acfcroatia.hr/wp-content/uploads/2021/04/Analiza_Azop.pdf (Accessed on 24/06/2024)

Wavestone. 2022. Digital Public Administration Factsheets – Croatia. https://joinup.ec.europa.eu/sites/default/files/inline-files/DPA_Factsheets_2022_Croatia_vFinal_0.pdf (Accessed on 24/06/2024)

Chapter 1.4 – The AI Act of the EU Commission

Council of the European Union. (2023). “Council adopts first-ever EU regulation on Artificial Intelligence.” https://www.consilium.europa.eu/en/press/press-releases/2023/12/15/council-adopts-first-ever-eu-regulation-on-artificial-intelligence (Accessed on 25/07/2024)

European Commission. 2018. “Artificial Intelligence for Europe.” https://ec.europa.eu/digital-strategy/our-policies/artificial-intelligence (Accessed on 25/07/2024)

European Commission. 2020. White Paper on Artificial Intelligence – A European approach to excellence and trust. https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (Accessed on 25/07/2024)

European Data Protection Board. 2022. “EDPB and EDPS Call for Ban on Use of AI for Automated Recognition of Human Features in Publicly Accessible Spaces.” https://edpb.europa.eu/news/news/2022/edpb-and-edps-call-ban-use-ai-automated-recognition-human-features-publicly_en (Accessed on 25/07/2024).

European Parliament. 2021. Draft Proposal for the Artificial Intelligence Act. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0401_EN.html (Accessed on 25/07/2024).

European Parliament. 2024. "European Parliament approves the AI Act." https://www.europarl.europa.eu/news/en/press-room/20240116IPR95010/european-parliament-approves-the-ai-act (Accessed on 25/07/2024).

High-Level Expert Group on Artificial Intelligence. 2019. Ethics Guidelines for Trustworthy AI. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (Accessed on 25/07/2024).

Chapter 2.1 – The Health Sector

Official Gazette of the Republic of Croatia. 2016. Healthcare Act (OG 150/08, 71/10, 139/10, 22/11, 84/11, 154/11, 12/12, 35/12 - OUSRH, 70/12, 144/12, 82/13, 159/13, 22/14 - O and RUSRH, 154/14 and 70/16). https://mvep.gov.hr/UserDocsImages/files/file/dokumenti/prevodenje/zakoni/26-Zakon-o-zdravstvenoj-za%C5%A1titi-NN-150-08,-71-10,-139-10...70-16-pro%C4%8Di%C5%A1%C4%87eni-tekst-ENG.pdf (Accessed on 24/06/2024)

Wavestone. 2022. Digital Public Administration Factsheets – Croatia. https://joinup.ec.europa.eu/sites/default/files/inline-files/DPA_Factsheets_2022_Croatia_vFinal_0.pdf (Accessed on 24/06/2024)

Chapter 2.2 – The Social Sector: the Case of Homeless and Refugees

Council of the European Union. 2024. EU migration and asylum policy. https://www.consilium.europa.eu/en/policies/eu-migration-policy/#0 (Accessed on 20/06/2024)

Develtere, P. 2022. Data Collection Systems and Homelessness in the EU – An Overview. DOI 10.2767/989826

Dionisio, M. et al. 2023. The role of digital social innovations to address SDGs: A systematic review. In Environment, Development and Sustainability. https://doi.org/10.1007/s10668-023-03038-x (Accessed on 20/06/2024)

European Commission. 2020. Digital education action plan 2021-2027: resetting education and training for the digital age. https://education.ec.europa.eu/sites/default/files/document-library-docs/deap-communication-sept2020_en.pdf

European Commission. 2021. 2030 digital compass – The European way for the digital decade. https://data.europa.eu/doi/10.2759/425691 (Accessed on 20/06/2024)

European Commission. 7 June 2022. Digital Inclusion. https://digital-strategy.ec.europa.eu/en/policies/digital-inclusion (Accessed on 20/06/2024)

European Commission. 2024. Pact on Migration and Asylum. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/migration-and-asylum/pact-migration-and-asylum_en (Accessed on 20/06/2024)

European Commission. 11 April 2024. Statistics on migration to Europe. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/statistics-migration-europe_en (Accessed on 20/06/2024)

European Economic and Social Committee. 2017. Recent Evolutions of Social Economy – Study. https://www.eesc.europa.eu/en/our-work/publications-other-work/publications/recent-evolutions-social-economy-study (Accessed on 20/06/2024)

European Federation of National Organisations Working with the Homeless (FEANTSA). 2021. Digital Inclusion for Homeless People and Homeless Service Providers: An analysis of benefits, challenges and solutions. https://www.feantsa.org/public/user/Digitalisation_Policy_Paper.pdf (Accessed on 20/06/2024)

Hayes, B. 2017. Migration and data protection: Doing no harm in an age of mass displacement, mass surveillance and "big data". International Review of the Red Cross 99(1), 179–209. doi:10.1017/S1816383117000637

Kaurin, D. 2019. Data Protection and Digital Agency for Refugees. In Center for International Governance Innovation, World Refugee Council Research Paper Series 12. https://www.cigionline.org/publications/data-protection-and-digital-agency-refugees/ (Accessed on 20/06/2024)

Lisbon Declaration on the European Platform on Combatting Homelessness. 2021. https://ec.europa.eu/social/BlobServlet?docId=24120&langId=en (Accessed on 20/06/2024)

Murray, D. et al. 2024. The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe. Journal of Human Rights Practice 16(1), 397–412. https://doi.org/10.1093/jhuman/huad020 (Accessed on 20/06/2024)

Picum. 18 December 2023. "Over 50 NGOs pen eleventh-hour open letter to EU on human rights risks in Migration Pact." https://picum.org/blog/open-letter-eu-human-rights-risks-migration-pact/ (Accessed on 11/06/2024)

Protection International. 10 April 2024. "The EU Migration Pact: a dangerous regime of migrant surveillance." https://privacyinternational.org/advocacy/5296/eu-migration-pact-dangerous-regime-migrant-surveillance (Accessed on 20/06/2024)

Solinum. 2019. Les sans-abri et le numérique: Équipement, usages et compétences numériques des personnes sans-abri en France en 2018. https://www.solinum.org/wp-content/uploads/2021/07/Rapport_annuel_2019.pdf (Accessed on 20/06/2024)

The Guardian, J. Henley. 19 August 2017. "Home Office used charity data map to deport rough sleepers." https://www.theguardian.com/uk-news/2017/aug/19/home-office-secret-emails-data-homeless-eu-nationals. (Accessed on 11/06/2024)

United Nations Human Rights Council. 2021. The right to privacy in the digital age Report of the Office of the United Nations High Commissioner for Human Rights.

https://documents.un.org/doc/undoc/gen/g21/249/21/pdf/g2124921.pdf?token=cuSvAjcLfWsykZAPRb&fe=true (Accessed on 20/06/2024)

Chapter 2.3 – The E-commerce Sector

Gabel, D. and Hickman, T. 5 April 2019. Chapter 13: Cross-Border Data Transfers. In D. Gabel and T. Hickman. 2019. *Unlocking the EU General Data Protection Regulation*. https://www.whitecase.com/insight-our-thinking/chapter-13-cross-border-data-transfers-unlocking-eu-general-data-protection (Accessed on 20/06/2024)

Kosinski, M. et al. 2013. Private traits and attributes are predictable from digital records of human behavior. In *PNAS 110* (15), pp. 5802-5805. https://www.pnas.org/doi/pdf/10.1073/pnas.1218772110 (Accessed on 20/06/2024)

Official Gazette of the Republic of Croatia. 2019. The Electronic Commerce Act (OG 173/03, 67/08, 36/09, 130/11, 30/14). https://www.zakon.hr/z/199/Zakon-o-elektroni%C4%8Dkoj-trgovini (Accessed on 20/06/2024)

Official Gazette of the Republic of Croatia. 2022. Consumer Protection Act (OG 19/2022). https://www.zakon.hr/z/193/Zakon-o-za%C5%A1titi-potro%C5%A1a%C4%8Da (Accessed on 20/06/2024)

United Nations Human Rights Council. 11 May 2016. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/32/38). https://documents.un.org/doc/undoc/gen/g16/095/12/pdf/g1609512.pdf?token=DUNkxZpJrJZITez1tm&fe=true (Accessed on 20/06/2024)

Chapter 2.4 – The Education Sector: Focus on Primary Schools

Council of the European Union. 2022. "*Council Recommendation of 28 November 2022 on Pathways to School Success and replacing the Council Recommendation of 28 June 2011 on policies to reduce early school leaving*." In Official Jounral of the European Union C 469, pp. 1-15. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022H1209(01)

Cowie, H. 2018. "*Cyberbullying and its impact on young people's emotional health and well-being*." In The Psychiatrist 37 (5), pp. pp. 167-170. https://doi.org/10.1192/pb.bp.112.040840

European Commission. 2020a. "Erasmus+ Programme Guide." https://ec.europa.eu/programmes/erasmus-plus/resources/documents/erasmus-programme-guide-2020_en (Accessed on 28/06/2024).

European Commission. 2020b. "Digital Education Action Plan (2021-2027)." https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en (Accessed on 30/06/2024).

European Commission. (2020c). "Youth Guarantee." https://ec.europa.eu/social/main.jsp?catId=1079&langId=en (Accessed on 28/06/2024).

European Commission. 2021a. "European Pillar of Social Rights Action Plan." https://ec.europa.eu/social/main.jsp?catId=1226&langId=en (Accessed on 27/06/2024).

European Commission. 2021b. "European Education Area." https://ec.europa.eu/education/education-in-the-eu/european-education-area_en (Accessed on 27/06/2024).

European Commission. 2021c. "European Child Guarantee." https://ec.europa.eu/social/main.jsp?catId=1428&langId=en (Accessed on 27/06/2024).

Gregorová, M. (2022). "The Commission's gross violation of privacy — endangering encryption." https://www.politico.eu/article/eu-commission-violation-privacy-endangering-encryption/ (Accessed on 18/06/2024).

TechCrunch. (2020). "University of California pays $1.14M ransom to recover data." https://techcrunch.com/2020/07/01/university-of-california-pays-ransom-to-recover-data (Accessed on 20/06/2024).

The Guardian. (2020). "Universities share student data with immigration authorities." https://www.theguardian.com/education/2020/jan/16/universities-share-student-data-with-immigration-authorities (Accessed on 20/06/2024).

CBC News. (2021). "Facebook apologises for removing posts about residential schools." https://www.cbc.ca/news/canada/facebook-residential-schools-posts-removed-1.6074095 (Accessed on 20/06/2024).

Human Rights Watch. (2020). "Belarus: Internet Shutdowns During Protests." https://www.hrw.org/news/2020/08/10/belarus-internet-shutdowns-during-protests (Accessed on 28/06/2024).

The Atlantic. (2018). "The Cost of Facebook's Algorithm Changes on Non-profits." https://www.theatlantic.com/technology/archive/2018/01/facebooks-algorithm-changes-will-hurt-non-profits/551015/ (Accessed on 27/06/2024).

Chapter 2.5 – The Telecommunications Sector

Ahava, A. 30 September 2020. "In Landmark Ruling CJEU Closes Loophole in EU Net Neutrality Regulation." Berggren. https://www.berggren.eu/en/blog/in-landmark-ruling-cjeu-closes-loophole-in-eu-net-neutrality-regulation (Accessed on 20/06/2024)

Amnesty International. 25 October 2021. "UK: Europe's top court rules UK mass surveillance regime violated human rights." https://www.amnesty.org/en/latest/news/2021/05/uk-surveillance-gchq-ecthr-ruling-2/#:~:text=In%20a%20landmark%20judgment%2C%20the%20Grand%20Chamber%20of,the%20rights%20to%20privacy%20and%20freedom%20of%20expression (Accessed on 20/06/2024)

Cave, M. et al. 2019. The European Framework for Regulating Telecommunications: A 25-year Appraisal. In Review of Industrial Organisation 55, pp. 47-62. https://doi.org/10.1007/s11151-019-09686-6

Chakravarti, A. 31 January 2024. "Data of 750 million telecom users in India being sold on dark web, cyber experts claim." India Today. https://www.indiatoday.in/technology/news/story/data-of-750-million-telecom-users-in-india-being-sold-on-dark-web-cyber-experts-claim-2495752-2024-01-31

European Commission. 2015. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A digital single market strategy for Europe. eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192

European Commission. 24 July 2015. "What next for EU telecom rules?" https://digital-strategy.ec.europa.eu/en/news/what-next-eu-telecom-rules

European Parliament and Council of the European Union. 2014. Directive 2014/61/EU of the European Parliament and of the Council of 15 May 2014 on measures to reduce the cost of deploying high-speed electronic communications networks. Official Journal of the European Union L155, 1-14. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0061

European Parliament and Council of the European Union. 2015. Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union. Official Journal of the European Union L310, 1-18. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2120

European Parliament and Council of the European Union. 2018a. Regulation (EU) 2018/1971 of the European Parliament and of the Council of 11 December 2018 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Agency for Support for BEREC (BEREC Office), amending Regulation (EU) 2015/2120 and repealing Regulation (EC) No 1211/2009. Official Journal of the European Union L321, 1-35. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1971

European Parliament and Council of the European Union. 2018b. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code. Official Journal of the European Union L321, 36-214. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2018:321:FULL

European Parliament and Council of the European Union. 2022. Regulation (EU) 2022/612 of the European Parliament and of the Council of 6 April 2022 on roaming on public mobile communications networks within

the Union. Official Journal of the European Union L115, 11-37. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0612

European Union Agency for Cybersecurity (ENISA). 2022. Telecom Security Incidents. Annual Report. https://www.enisa.europa.eu/publications/telecom-security-incidents-2021/@@download/fullReport

Gregorová, M. 25 October 2022. "The Commission's gross violation of privacy — endangering encryption." *Politico*. https://www.politico.eu/article/eu-commission-violation-privacy-endangering-encryption/ (Accessed 18/06/2024)

Lyons, J. 2 April 2024. "Feds finally decide to do something about years-old SS7 spy holes in phone networks." *The Register*. https://www.theregister.com/AMP/2024/04/02/fcc_ss7_security/ (Accessed 18/06/2024)

Safety of Journalists Platform. 2022. Thematic Factsheet: Blocking, Filtering, and Take Down of Online Content. https://rm.coe.int/factsheet-blocking-filtering-and-take-down-of-online-content-17june202/1680a6f693