



A Comparative Study of the Online Privacy and Data Protection of Children in the European Union and the United States

**Doctoral (Ph.D.) Thesis
Aslı Alkış Tümtürk**

**Supervisors:
Dr. Zsolt Nagy
Dr. Szilvia Váradi Dr. Kertészné**

**University of Szeged
Doctoral School of Law Szeged**

**Szeged
2023**

Table of Contents

Abbreviations.....	4
Tables and Charts.....	6
1. Introduction	7
1.1 Problem Statement	9
1.2 Objective and significance of the research	12
1.3 Research Design	14
1.4 Research Methodology	22
1.5 Research Structure	24
2. GDPR Article 8 and COPPA: The historical context and evolution of the current standards, definitions, and issues pertaining to the protection of children's data and privacy	26
2.1 Short Summary.....	38
3. Concept of parental consent in the GDPR and COPPA	40
3.1 Concept of consent in the GDPR	40
3.2 Children and parental consent in the GDPR comparing with the COPPA.....	42
3.3 Threshold age for parental consent under the GDPR and the COPPA	47
3.4 Online age verification methods	61
3.5 Short summary	69
4. Main rights of the children and their parents under the GDPR and COPPA ..	71
4.1 Short summary	77
5. Main obligations imposed on data controllers.....	79
5.1 Short Summary.....	90
6. Trans-Atlantic data transfers involving child data in the EU.....	92
6.1 Safe Harbour	99
6.2 Privacy Shield.....	101
6.3 The “essentially equivalent” level of data protection	104
6.3.1 Content Principles	105
6.3.2 Additional Content Principles	107
6.3.3 Procedural and Enforcement Mechanisms	107
6.3.4 .Essential conditions for public authorities to use surveillance and get access to personal data of individuals in third countries.....	108
6.4Existing methods for transferring personal data from the EU to the US in the absence of an adequacy decision	109
6.5 Transfer of children's personal data from the EU to third countries.....	114
6.6 Impacts of the fact that Privacy Shield is no longer applicable, and SCCs are being utilised instead: Is Data Localization the best solution?	121
6.7 The new Transatlantic Data Privacy Framework: Is the Schrems III coming?.....	124
6.8 Short Summary	133
7. Examples from the practice - Social networking services, privacy policies, child influencers and parental sharing	135

7.1 Short Summary	169
8. Conclusions	171
Bibliography.....	186

Abbreviations

AI	Artificial Intelligence
APPI	Act on the Protection of Personal Information (Japan's Data Protection Law)
BCRs	Binding Corporate Rules
BIPA	Biometric Information Privacy Act
BND	Bundesnachrichtendienst
CA	Court of Appeal
CCPA	California Consumer Privacy Act
CDC	Centres for Disease Control and Prevention
CFR	Charter of Fundamental Rights of the European Union
CJEU	European Court of Justice
CLPO	Civil Liberties Protection Officer in the Office of the Director of National Intelligence
COPPA	Children's Online Privacy Protection Act
DPIA	Data Protection Impact Assessment
DPRC	Data Protection Review Courts
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
eID	European Digital Identities
EU	European Union
GDPR	General Data Protection Regulation

FERPA	Family Educational Rights and Privacy Act
FRA	European Union Agency for Fundamental Rights
FTC	Federal Trade Commission
HIPPA	the Health Insurance Portability and Accountability Act
ISS	Information Society Services
ML	Machine Learning
NCMEC	National Centre for Missing and Exploited Children
NSA	National Security Agency
PIA	Privacy Impact Assessment
SCCs	Standard Contractual Clauses
TCPA	Telephone Consumer Protection Act
UK	United Kingdom
UNCRC	United Nations Convention on the Rights of the Child
US	United States
WP12	Article 29 Data Protection Working Party: Working Document. Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive
WP29	Article 29 Data Protection Working Party
WP254	Article 29 Data Protection Working Party: Working Document on Adequacy Referential

Tables and Charts

Table 1: Age of consent in the Member States

Table 2: Children's data and privacy literacy

Table 3: Children's views of how their data and privacy online should be addressed (entries paraphrased and summarized by the authors)

Chart 1: Children using social media sites by ages

Chart 2: Appropriate ages for children to begin using social media sites and playing video games according the parents

Chart 3: Visiting social media networks daily

Chart 4: Harm from online victimisation (at least a bit upset)

Chart 5: How much control teenagers have over their data

Chart 6: How much they worry about the control over their data

Chart 7: Slides from summary of Instagram's 2019 research

Chart 8: Global number of child nudity and sexual exploitation-related content items removed by Facebook from 2018 to 2022 (in millions)

Chart 9: Parents who share information about their children

Chart 10: Parents worry about their children being upset about the information they posted about them on social media

1. Introduction

“*Quid enim sanctius, quid omni religione munitius, quam domus unusquisque civium?* (What more sacred, what more strongly guarded by every holy feeling, than a man's own home?)” said *Cicero*, the famous lawyer, politician, orator and writer of the Roman era.¹ Moreover, the proverb “*Every man's home is his castle*” was first used in Roman law.² Family life and home are still foundational components of the concept of privacy.³

Even though historically and currently almost every country recognises privacy in their constitutions or other legislation,⁴ privacy does not have a universally agreed definition. Due to its dynamic character, it may adapt to the changing social, cultural, and economic circumstances of a given period and place.⁵ In light of several well-known examples of definitions, we may conclude the primary approaches to the notion of privacy in the European Union (the EU) and the United States (the US).

In 1890, *Louis Brandeis* and *Samuel Warren* published “*Right to Privacy*”, one of the most-cited renowned articles, which was a very significant step towards the development of the contemporary concept of privacy.⁶ They described privacy as “the right to be let alone” within this famous article.⁷ Moreover, the law professor *Alan Westin* contributed to the concept of privacy and data protection as “[...] *the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.*”⁸ These specifications affected privacy law in the US, and as a result, privacy has frequently been viewed as a component of liberty, the right to be free from governmental intrusions in the US.⁹

¹ William Blackstone and William Carey Jones (eds): *Commentaries on the Laws of England*, San Francisco, Bancroft-Whitney Co. (1916), 2430-2431.

² Samuel Dash: *The intruders: Unreasonable searches and seizures from King John to John Ashcroft*, Rutgers University Press (2004), 9.

³ Charter of Fundamental Rights of the European Union, OJ C 326, 26.12.2012, p. 391-407, Article 7: “*Everyone has the right to respect for his or her private and family life, home and communications.*”

⁴ European Data Protection Supervisor (EDPS), *Data Protection: Privacy- a fundamental right*, https://edps.europa.eu/data-protection/data-protection_en (last visited 22 January 2023).

⁵ Adrienn Lukács: *What is privacy? The history and definition of privacy*, In: Keresztes, Gábor (ed.): *Tavaszi Szél 2016 Tanulmánykötet I.*, Budapest, Doktoranduszok Országos Szövetsége (2016), 258 <https://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf> (last visited 22 January 2023).

⁶ Samuel D. Warren and Louis D. Brandeis: *Right to Privacy*, *Harvard Law Review* 4, no. 5 (1890), 193-220.

⁷ Samuel D. Warren and Louis D. Brandeis: *Right to Privacy*, *Harvard Law Review* 4, no. 5 (1890), 205.

⁸ Alan F. Westin: *Privacy and Freedom*, Atheneum New York (1967), 7.

⁹ European Data Protection Supervisor (EDPS), *Data Protection: What is privacy?*, https://edps.europa.eu/data-protection/data-protection_en (last visited 22 January 2023).

Following the aforementioned developments in the US, the EU created a new sort of protection. In the EU's approach to privacy, in addition to the right to be let alone, the right to private life, right to be autonomous, and have a control over one's own information play a crucial role.¹⁰ As technology and the Internet improved, the EU data subjects who provide their personal data became more aware of the limited control over their personal data.¹¹ Accordingly, the data protection stemming from the right to privacy covers specifically any information belonging to an identified or identifiable natural person in the EU.¹² Similarly, to the European perspective, the Hungarian jurist *Máté Dániel Szabó* claimed in 2005 that “*privacy is the right of the individual to decide about himself/herself.*”¹³

The historical evolution of the legal context of data protection and privacy will be explored in depth in the following chapter; therefore, we will not include it in the introductory chapter of this thesis. Rather, we would like to discuss when and why data protection became so crucial to our everyday lives, as well as why we selected children's privacy and data protection as the subject of our doctoral thesis. In addition, within this chapter, we will provide a list of our research questions as well as our methodology.

Today, we all live in a data-driven society, and it is essential and beneficial for us to share personal data in order to receive certain services. For instance, we share our health-related data with hospitals to receive health care services, our credit or debit card information to order food, and our personal information (at least username, email address, password, and most likely credit/debit card information to pay for the service if it is not gratis) to access online music or video platforms. This information will be used to provide products and services, but it should not be used for reasons that the data subjects did not expect or intend when they consented to the sharing of their information.¹⁴

¹⁰ European Data Protection Supervisor (EDPS), Data Protection: What is privacy?, https://edps.europa.eu/data-protection/data-protection_en (last visited 22 January 2023).

¹¹ Bart Custers, Alan M. Sears, Francien Dechesne, Iliana Georgieva, Tommaso Tani, and Simone Van der Hof: EU personal data protection in policy and practice, Hague: TMC Asser Press, Springer (2019), 1.

¹² European Data Protection Supervisor (EDPS), Data Protection: What is data protection?, https://edps.europa.eu/data-protection/data-protection_en (last visited 22 January 2023).

¹³ Máté Dániel Szabó: Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival, *Információs Társadalom: társadalomtudományi folyóirat* 5, no. 2 (2005), 46.

¹⁴ Information Commissioner's Office (ICO), The benefits of data protection laws, <https://ico.org.uk/for-organisations/sme-web-hub/the-benefits-of-data-protection-laws/#:~:text=And%20you%20have%20to%20protect,discrimination%20or%20even%20physical%20harm> (last visited 23 January 2023).

Data protection, as a fundamental right, ensures the protection of natural persons with respect to the processing of personal data.¹⁵ The second objective of data protection is to govern the free flow of personal data among individuals, organisations, and countries as a result of the societal and economic benefits of data sharing.¹⁶ Whereas, data security assures the safety of personal data, is the practise of protecting digital information against unauthorised access, corruption, or theft throughout its entire lifecycle.¹⁷ Although data protection and privacy will be the primary focus of this thesis, we will also cover data security using instances (e.g., cyber-attacks, identity theft). It is a crucial aspect of the GDPR, and data controllers are responsible for securing personal data via the implementation of appropriate technological and organisational measures.¹⁸ Furthermore, personal data that gets into the wrong hands may be highly dangerous, especially when the data subjects are children.¹⁹

1.1 Problem Statement

Long-standing issues concerning privacy and personal data have become much more interesting as a result of the increasing internet use of not just adults but also children around the world. Especially with the introduction of social media networks including YouTube, Facebook, and Instagram, the privacy and data protection of children have become significant concerns, since parents may now share their children's photo albums and videos with the entire online community. Therefore, being a minor celebrity or child influencer is now remarkably easy for any child.

This thesis, thus, will focus on a subset of the much broader issue of privacy and data protection, namely the privacy and data protection of children. However, this does not indicate that the topic of children's privacy and data protection is narrow; on the contrary,

¹⁵ What is ensured by data protection is stated in the GDPR's title: 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), OJ 2016 L 119, 04.05.2016, pp. 1-88.

¹⁶ The second aim of data protection is highlighted by the GDPR's title: 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), OJ 2016 L 119, 04.05.2016, pp. 1-88.

¹⁷ GDPR, Article 32-34.

¹⁸ GDPR, Article 32(1).

¹⁹ GDPR, Recital 75.

when we delved further, we discovered several insufficiencies and gaps between the law in text and law in practise.

The first problem we have observed is that one in three internet users worldwide are children²⁰ and that 80% of children in developed western countries have digital footprints before the age of two, largely due to the actions of their families.²¹ However, lawmakers are not taking this issue seriously, because they prioritize more economically attractive concerns, such as data transfers and profiling, over protecting vulnerable data subjects who may not contribute as much to the Digital Single Market economically.²² Similarly, websites, particularly social media networks, ignore the existence of children on their platforms and turn a blind eye to the fact that children under the age of consent are utilising their services.²³

Second problem we have noticed is that there are few academics who are interested in children's online activities and accordingly. Therefore, there are few academic literatures on this topic. Limited academic literature was one of the challenges we faced while doing research for our thesis. Hence, we believe that this doctoral thesis would be novel and beneficial to the academic world and the doctrine.

Thirdly, the real-life example of *Amanda Todd*, a young girl who committed suicide, because her data was not protected properly, convinced us that children are naiver and more vulnerable than adults and thus require more specialised protections.²⁴ This was a milestone factor that prompted us to conduct extensive study on this issue.

²⁰ UNICEF, More than 175,000 children go online for the first time every day, tapping into great opportunities, but facing grave risks (6 February 2018), <https://www.unicef.org/press-releases/more-175000-children-go-online-first-time-every-day-tapping-great-opportunities> (last visited 23 January 2023).

²¹ United Nations, Children's right to privacy in the digital age must be improved (15 July 2021) <https://www.ohchr.org/en/stories/2021/07/childrens-right-privacy-digital-age-must-be-improved> (last visited 23 January 2023).

²² Milda Macenaite and Eleni Kosta: Consent for processing children's personal data in the EU: following in US footsteps?, *Information & Communications Technology Law* 26, no. 2 (2017), 160.

²³ Brooke Auxier, Monica Anderson, Andrew Perrin and Erica Turner, Children's engagement with digital devices, screen time, Pew Research Center, (2020). 2. <https://www.pewresearch.org/internet/2020/07/28/childrens-engagement-with-digital-devices-screen-time/> (last visited 23 January 2023).

²⁴ My story: Struggling, bullying, suicide, self-harm, *Thesomebodytoknow* videos, available at: <https://www.youtube.com/watch?v=vOHXGNx-E7E> (last visited 23 January 2023).

The General Data Protection Regulation (GDPR) of the European Union²⁵ and the Children's Online Privacy Protection Act (COPPA) of the US²⁶ took vital measures since, rather than disregarding the internet presence of children, they created Articles mentioning them.²⁷ However, fourth problem we shall examine in our thesis is the overreliance on parental consent in both legislations. Especially, when parents are unaware of the risks or consequences of their children's online activities, relying on parental responsibility may be even more problematic to the well-being of children, since they are more likely to be victimised.

The fifth problem is that while the GDPR and the COPPA include data protection and privacy standards for children, these requirements are not comprehensive. For instance, neither the GDPR nor the COPPA regulate the transfer of children's personal data specifically, and there are no restrictions regarding parental sharing.

The difference between the legal text and its application in practice is the sixth problem we have identified. Because, for example, "*child*" is defined as "*an individual under the of 13*" under COPPA,²⁸ and COPPA applies to commercial websites or online services intended to children under the age of 13 that collect or *have actual knowledge* that they collect information from children.²⁹ To evade COPPA's requirements, the social media sites do not allow children under 13 to have accounts on their platforms. However, when their age verification procedures do not identify ages effectively, children may lie about their age and create profiles on such social networking platforms. Considering the surveys conducted related to children and profile images, and everyday online activities of children, it is inconceivable that social media sites are unaware of children's presence on their platforms. Even so, they are not yet deemed to be directly offered to children. Consequently, it seems that this broadened concept of *having actual knowledge* is not yet completely operational in practise.

²⁵ 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), OJ 2016 L 119, 04.05.2016, pp. 1-88.

²⁶ 16 CFR Part 312 Children's Online Privacy Protection Act; Final Rule, 15 U.S.C. §§ 6501–6506, Federal Register Vol. 64, No. 212, 03.11.1999, p. 59888-59915.

²⁷ 16 CFR Part 312 Children's Online Privacy Protection Act; Final Rule, 15 U.S.C. §§ 6501–6506, Federal Register Vol. 64, No. 212, 03.11.1999, p. 59888-59915 and 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), OJ 2016 L 119, 04.05.2016, pp. 1-88, Article 8.

²⁸ 16 CFR 312.2 "Child".

²⁹ 16 CFR 312.2 "Web site or online service directed to children".

Nonetheless, the fifth and sixth problems are not yet visible. The children of today who suffer/will suffer from their parents' and data controllers' online activities are not yet mature enough to comprehend the risks and consequences of excessive online sharing of their personal information and private lives. Consequently, Internet-victimized children now lack the maturity to take legal actions against their parents and/or the relevant data controllers. In the near future, however, we expect cases from today's children regarding violations of their privacy and data protection rights.

1.2 Objective and significance of the research

In this thesis, we intend to compare the COPPA and the GDPR and their practices regarding children's online data protection and privacy in the EU and the US in a number of areas, including the concept of consent and particularly the consent of the parents, the rights of children and parents and the obligations of data controllers as determined by the laws, the data transfer of children to third countries, the social media practises of children and parents, and the extent to which social media sites follow and apply the laws.

The reason why we chose the COPPA rule to compare it with the GDPR is that the US is where privacy discussions began in the world, and Article 8 of the GDPR partially adopted the COPPA's approach to children's data protection. It is evident that the two legislations share similarities since both the GDPR and COPPA hold parents accountable for their children's online actions, require parental consent for sharing children's personal data online, and establish a similar age of consent.³⁰

By making these comparisons, we will attempt to highlight both the weaknesses and the strengths, and in doing so, we will provide remedies for the flaws and seek the ideal solutions. With this thesis, our major objective is to call attention to the significance of safeguarding children's online data and privacy, as well as to contribute to the limited literature on this new and important issue.

Our long-term objective is to influence the viewpoints of lawmakers. Therefore, we expect that our research will help to the future creation of more child-friendly and child-centred policies, as well as more child-friendly social media rules and restrictions. In addition, we will emphasise that these laws and restrictions must always be implemented

³⁰ For more information see: Milda Macenaite and Eleni Kosta: Consent for processing children's personal data in the EU: following in US footsteps?, *Information & Communications Technology Law* 26, no. 2 (2017), 146-197.

with the best interests of children in mind. Last but not least, given the vulnerability of children, we would like to emphasise the significance of collaboration between parents, lawmakers and law enforcers, online service providers, and even schools.

1.3 Research Design

We will begin this thesis by analysing the background of the COPPA rule and Article 8 of the GDPR in Chapter 2. We will inquire as to the historical context and evolution of the definitions and standards related to the privacy and data protection of children in these legislations, as well as the emergence of the necessity to adopt such rules for children. Lastly, in Chapter 2, we will analyse how and in what manners the COPPA affected GDPR Article 8, and at which points these influences might be mainly observed, as well as what areas require improvement for both legislations.

Afterwards, the scope of the core concept of this research, which is consent and, more specifically, parental consent for underage children will be analysed in Chapter 3.³¹ Consent, as defined by the GDPR as the freely expressed, precise, informed, and clear wishes of the data subjects, indicates consent to the use of their personal data.³² Despite the fact that this definition emphasises the data subject's wishes, in the context of personal data processing, it is not possible to refer to a true will, but rather compliance with the necessary requirements in order to acquire certain services.

Indeed, *Frison-Roche*, a law professor, distinguishes between will and consent, and explains that consent is a kind of submission; consequently, the one who consents is the one who owes the other person anything. On the other hand, the will is the indication of domination, power, and autonomy, therefore it may request anything, whereas consent is limited to what is possible.³³ However, even if consent does not provide complete autonomy, it remains the only feasible means of exercising control over one's data under current conditions.

Regarding parental permission, GDPR stipulates that parental consent is required to make the processing of children's data lawful if the children are under the age of digital consent (could be 13 to 16 depending on the Member States).³⁴ Similarly, the COPPA defines parental consent as obtaining parental consent prior to the collection, use, and/or

³¹ According to Article 8(1) of the GDPR, under two circumstances, parental consent is necessary before an information society service may process a child's data: If a child is under 16 (can be 13 in some Member States) and an information society service is relying on consent as a lawful basis to process a child's personal data.

³² GDPR, Article 4(11).

³³ Marie-Anne Frison-Roche: *Remarques sur la distinction de la volonté et du consentement en droit des contrats*, RTD civ (1995), 574.

³⁴ GDPR, Article 8(1).

disclosure of their children's personal information if the children are under the age of thirteen.³⁵

In Chapter 3 regarding the concept of consent, we will also examine whether the COPPA and GDPR provide methods for obtaining parental consent. If so, what are they? If not, what are the potential methods to obtain parental consent in light of current technology, and if just one of the legislations uses such methods, is a legal transplant conceivable to incorporate them into the other?

After Chapter 3.1 and 3.2 related to the scope of the concept of consent and parental consent, we will examine in Chapter 3.3 how the threshold ages are implemented in practise and whether they are functional. In this chapter, we will attempt to address our first and second research questions:

Under the GDPR and COPPA, do the threshold ages for parental consent have any logical basis?

Do these threshold ages have any practical effects on children's internet activity habits and behaviours?

To answer the first question, we will compare the age of digital consent to other ages of consent in various contexts, such as entering the workforce, obtaining medical treatment, including diagnosis and surgery, and engaging in legal sexual activity with others. We shall investigate if there is coherence and sound rationale behind the varying ages of consent within the EU.

To address the second question, we will determine if there is any evidence that lowering the legal threshold age for accessing certain internet services has any practical effect. For instance, if a government passes a legislation with a higher threshold age, we will analyse if this actually raises the minimum age for using social networking platforms. Our viewpoints will be supported by surveys conducted by EU Kids Online³⁶ and the Pew Research Center in the US.³⁷

By answering these questions, we will determine whether the threshold ages for parental consent are implemented properly in real-world cases or if there is a gap between real-world

³⁵ 16 CFR 312.2 “Obtaining verifiable consent”.

³⁶ David Smahel, Hana Machackova, Giovanna Mascheroni, Lenka Dedkova, Elisabeth Staksrud, Kjartan Ólafsson, Sonia Livingstone, and Uwe Hasebrink, *EU Kids Online 2020: Survey results from 19 countries* (2020), EU Kids Online, 1-157.

³⁷ Brooke Auxier, Monica Anderson, Andrew Perrin and Erica Turner, *Children’s engagement with digital devices, screen time*, Pew Research Center, (2020) <https://www.pewresearch.org/internet/2020/07/28/childrens-engagement-with-digital-devices-screen-time/> (last visited 24 January 2023).

and legal requirements. If we will find out that there is a gap, we will debate if this disparity is a result of age verification procedures that might be easily deceived and/or whether parents are unconcerned and allow their children to have, for example, social media or Gmail accounts before the age of 13 (or in some EU countries this age would be up to 16).

As stated above, parents have the primary responsibility for their children's safety in accordance with the COPPA and GDPR. The parents of a child, however, cannot be expected to keep a close eye on them all the time. Because of this, there are internet technologies that make it easier to keep an eye on children while their parents are not available.³⁸ The purpose of these age verification systems is to use technology to ensure that only individuals of a specific age are allowed to see online content that is restricted by law or by the website's policy.³⁹ As a result, age verification might be useful in making the Internet safer for children.

We will investigate the age verification methods in Chapter 3.4 of this thesis and within this chapter, we will try to answer the third research question:

Could commonly deployed methods of age verification for preventing children's access to inappropriate online content be both trustworthy and respecting children's privacy and data protection rights?

Self-verification, peer-based verification, using a credit card, debit card, or other online payment systems as an age verification method, providing personal identification documents such as a passport or driver's licence, knowledge-based authentication, and the use of biologically unique identifiers will be compared in terms of their weaknesses and strengths in order to answer this question.⁴⁰ We will conclude by investigating whether a compromise exists to protect children from online dangers while simultaneously keeping their private data secured.

We will try to support our findings with data from an ongoing EU-funded project called euCONSENT, which is working to perfect the age verification methods. The 17th of February through the 3rd of March 2022 had seen the completion of the first large-scale trial

³⁸ Asli Alkis, Investigating the usefulness of online age verification methods, *Studia Iurisprudentiae Doctorandorum Miskolciensium*, (2021) vol.1, 8.

³⁹ Van der Maelen, Carl, *The Coming-of-Age of Technology: Using Emerging Tech for Online Age Verifications*, *Delphi 2* (2019), 115.

⁴⁰ Carl Van der Maelen: *The Coming-of-Age of Technology: Using Emerging Tech for Online Age Verifications*, *Delphi - Interdisciplinary Review of Emerging Technologies*, vol. 2, no. 3 (2019) 117-120.; Jules Polonetsky: *Online Age Verification for Our Children A Report on the Tools and Resources Available for Safeguarding the First Generation of Digital Natives*. 31st International Conference of Data Protection and Privacy Commissioners in Madrid, *Future of Privacy Forum*, (2009), 3-12.

of this project, and the results have just been made public. The study included around 2000 participants from five Europe countries: Greece, the United Kingdom, Germany, Cyprus, and Belgium.⁴¹ Finally, we intend finalise Chapter 3.4 with an analysis of the European Commission's proposal for European Digital Identities (eIDs).⁴² Using the eIDs for age verification purposes might raise concerns about privacy and security. Therefore, whether an eID solution can be both privacy-friendly and reliable, and how it may be differentiated from the usage of traditional personal IDs are all valid questions.

In Chapter 4, we will list the main rights of the children and the parents under the GDPR as well as COPPA. We will try to address the fourth research question in this chapter:

Taking into account the best interests of children, should data protection and privacy rights be provided directly to children by law, or should parents exercise them on their behalf?

To answer this question, we will attempt to determine which rights can be exercised by the children and which are too sophisticated for them to exercise, requiring the parents to do so on their behalf. We will examine the roles and responsibilities of data controllers or third-party service providers/suppliers (if any)⁴³ in making it feasible for children and their parents to exercise their rights. Besides, we shall inquire as to whether the children and their parents have any guidance on how to utilise their rights within these frameworks.

The GDPR provides children with the same data protection rights as adults. Whereas the COPPA only authorizes parents to exercise their children's rights to online privacy protection on behalf of them. To address our research question, we will examine whether the COPPA's current approach is appropriate or whether it should follow the GDPR's lead and extend at least some of the basic privacy rights to children directly. We will address which rights might be granted to children directly under the COPPA, if this is necessary, and why parental representation could not be sufficient in some instances.

Following the data subject's rights, we shall outline the obligations of data controllers and processors in Chapter 5, as they are interrelated. In this chapter, we will seek the answer to our fifth and sixth research questions:

⁴¹ euCONSENT, euCONSENT's first large scale pilot (18 March 2022) <https://euconsent.eu/euconsents-first-large-scale-pilot/> (last visited 24 January 2023).

⁴² European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, Brussels, 3.6.2021 COM (2021) 281 final 2021/0136 (COD).

⁴³ A service provider is an organisation that provides services to another organisation or entity. A cloud-based web hosting service, for instance, can be a third-party provider/supplier, and if it has access to the data stored in its cloud storage, also functions as a data controller.

Do the GDPR and the COPPA impose obligations specific to children on data controllers? If so, do these obligations enable direct communication between data controllers and children?

When and how could data controllers directly engage with children (instead of their parents) and offer them more control over their data?

Under the GDPR, it is the data controller's responsibility to make it possible and easy for data subjects to exercise their rights.⁴⁴ Moreover, data controllers specify the aims and means of processing personal data, and their most important task is to comply with the Regulation's norms and principles.⁴⁵ They must also preserve the privacy and data protection rights of children, and they must make all reasonable attempts, taking into consideration the state of technology, to get parental consent for processing children's data if the child is underage.⁴⁶ They have additional obligations originating from the concept of privacy by design and by default⁴⁷, as well as additional requirements connected to cooperating with the supervisory authority, particularly in the case of data breaches.⁴⁸ In addition, data controllers have a very significant responsibility to complete a data protection impact assessment where a type of processing, particularly one involving new technologies, and the purposes of the processing pose a high risk to the rights and freedoms of natural persons.⁴⁹

In this chapter devoted to the main obligations of data controllers, additional requirements under the GDPR will be listed and analysed in depth. Furthermore, we shall highlight the operators' obligations under the COPPA. Several COPPA obligations relate to making the exercise of parental rights easy and convenient.⁵⁰ Other obligations include protecting the confidentiality, security, and accuracy of the information collected from children.⁵¹

In order to answer our fifth and sixth research questions, we will perform a comparative analysis of both pieces of legislation to determine whether they should impose special obligations on data controllers regarding the protection of children's data. In addition, we

⁴⁴ GDPR Article 12(2): “The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.”

⁴⁵ GDPR, Article 24(1).

⁴⁶ GDPR, Article 8(2).

⁴⁷ GDPR, Article 25.

⁴⁸ GDPR, Article 31 and Article 33.

⁴⁹ GDPR, Article 35.

⁵⁰ 16 CFR 312.4(a)(b), 16 CFR 312.5(a)(2), 16 CFR 312.6(a) and 16 CFR 312.3(c).

⁵¹ 16 CFR 312.8.

will analyse the scenarios in which data controllers may actively involve children and offer them with more control over their personal data. Following that, we will explore data controllers' another important responsibility and one of the most significant aspects of the global digital economy, which is the free movement of data in Chapter 6. Personal data transfers to third countries can only occur if data controllers comply with the criteria outlined in Chapter 5 of the GDPR. The GDPR makes it abundantly obvious that the transfer of data between data controllers in EU countries and data controllers in third countries or international organisations is necessary for the expansion of international trade and cooperation.⁵² We shall seek a solution to our seventh and eighth research question in this chapter:

Given the historical and current challenges of transatlantic data transfers and the requirements of the GDPR, can the US ever achieve the "adequate level" of data protection?

Are there any child-specific data transfer requirements under the GDPR, and if not, how do the varying online consent ages for children across countries affect data transfers within the EU and to the US?

Due to fundamental differences in privacy and data protection between the EU and the US, there has not yet been a permanent and stable solution for data transfers from the US to the EU.⁵³ On one hand, in the US, personal data is viewed as a commodity,⁵⁴ and there is a sector-specific strategy that implements restricted regulation that only applies to specified goals. This gives US privacy regulations a tremendous deal of flexibility and freedom, as various sectors may interpret privacy and data protection quite differently. In this instance, though, some industries may be uncontrolled if there is no regulation protecting them.⁵⁵ On the other hand, privacy and data protection are seen as essential rights that must be respected by the EU.⁵⁶

When answering our seventh research question, we will emphasise that regardless of their personal data legislation and policies, neither the US nor the EU can afford to impede the flow of personal data across the Atlantic. Because the US remains the EU's largest

⁵² GDPR, Article 1 and Recital 101.

⁵³ Emily Linn: A Look into the Data Privacy Crystal Ball: A Survey of Possible Outcomes for the EU-US Privacy Shield Agreement, *Vand. J. Transnat'l L.* 50, (2017), 1312-1313.

⁵⁴ Paul M. Schwartz and Karl-Nikolaus Peifer: Transatlantic Data Privacy Law 106 *Geo. LJ.* (2017) 132-137 cited in Paul M. Schwartz: Global Data Privacy: The EU Way 94 *NYUL Rev.* (2019) 771-773.

⁵⁵ Emily A. Ivers: Using State-Based Adequacy Now, National Adequacy over Time to Anticipate and Defeat Schrems III, 62 *BC L Rev.* (2021) 2589-2591.

⁵⁶ Charter of Fundamental Rights of the European Union, OJ C 326, 26.12.2012, p. 391-407, Article 7-8.

commercial partner, and they have the most integrated economic relationship in the world.⁵⁷ Accordingly, for several years, they have been negotiating free data flow agreements. In Chapter 6, the previous partial adequacy decisions granted to the US by the European Commission will be examined. In the absence of adequacy decisions, we will investigate what methods are now being used and may be used to transfer data from the US to the EU in. We shall examine the circumstances and requirements of these current solutions in detail. We will attempt to determine how these strategies vary from adequacy decisions and why they are not optimal solutions. We will conduct a detailed analysis of the proposals by comparing this proposed solution to Japan's, which is another country deemed adequate by the European Commission,⁵⁸ and we will attempt to determine if this new agreement can achieve its objective or if it will result in an invitation to a possible Schrems III.

We will also debate the existing situation of the transfer of EU children's data to third countries to answer our eighth research question. We will investigate whether there are child-specific data transfer requirements. To demonstrate if online websites/applications make special mention of the transfer of children's data, we will provide specific examples from the practice. We will also investigate if varying digital platform-related consent ages for children would pose a concern for data transfer. If so, we will discuss the potential solutions to this issue. In the course of our research, we have not come across any academic sources directly related to the transfer of children's data, and we would like to draw attention to this issue.

In Chapter 7, we intend to address real life examples such as social networking sites, privacy policies, child influencers, and parental sharing. We intend to begin this chapter by discussing the sociological and cultural changes brought about by the rise of social media websites. On the grounds that in the past, sharing images and videos was limited to close family and friends via photo albums and videotapes. However, following the advent of the Internet and social media networks such as Facebook, Instagram, and YouTube, the situation has altered considerably. Because individuals now have the opportunity to share their material online with millions of random strangers, everyone has the potential to become

⁵⁷ European Commission, Trade, EU trade relationships by country/region, Countries and Regions, United States, https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/united-states_en#:~:text=The%20European%20Union%20and%20the,and%20investment%20partner%20by%20far (last visited 25 January 2023).

⁵⁸ Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/ 679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, OJ L 76, 19.3.2019, p. 1–58.

celebrities or, as the term has evolved, influencers.⁵⁹ Given the fact that the GDPR and the COPPA restrict children's online sharing of personal information without parental consent if they are under a certain age, social media platforms do not allow children under the age of consent to create accounts on their platform.⁶⁰ This chapter addresses our ninth and tenth research questions:

How do the requirements of the GDPR and the COPPA affect the practises of social media sites and the sharing activities of parents concerning their children?

Can excessive reliance on parental consent protect the personal data and privacy of children?

To answer the ninth question, we will examine the case law, surveys, statistics, and real-world examples from social media sites (e.g., a child influencer's photo on Instagram or Facebook, a family prank video on YouTube, etc.). By doing so, we will try to determine whether the prohibited content outlined in the data protection and privacy policies of these social media sites is reflected in practise.

Moreover, we will debate whether the sharing activities of adults falls within the realm of freedom of experience. If the answer is affirmative, we should investigate how to strike a balance between the parent's freedom of expression and right to informational self-determination (exercising on behalf of their children) and the children's right to privacy. We will provide some instances from the case law of the EU and the US and propose a method to strike a balance in favour of children, taking their best interests into account.⁶¹

Moreover, we will highlight the reasons why the sharing of children's personal information should be restricted by law and not left to parental consent. In addition to privacy violations, cyberbullying, identity theft, exposure to child pornography, discrimination and labelling, and kidnapping are among these reasons.⁶² In conjunction with the various

⁵⁹ Shannon Sorensen: Protecting Children's Right to Privacy in the Digital Age: Parents as Trustees of Children's Rights, *Children's Legal Rights Journal* 36, no. 3 (2016), 156-157.

⁶⁰ Instagram Help Center, How to Report Things, How do I report a child under the age of 13 on Instagram?: https://help.instagram.com/2922067214679225/?helpref=hc_fnav (last visited 26 January 2023); YouTube, Terms of Service, General Terms and Conditions: Who can use the service?, Age requirements <https://kids.youtube.com/t/terms> (last visited 26 January 2023).

Facebook Help Center, How to Report Things, How do I report a child under the age of 13 on Facebook?: https://www.facebook.com/help/157793540954833/?helpref=uf_share (last visited 26 January 2023).

⁶¹ Asli Alkis Tümtürk: Implications of Parental Sharing of Children's Personal Data Online, *ArsBoni Jogi Folyoirat*, X. evfolyam 2022/1-2 (2022), 11 available at https://arsboni.hu/wp-content/uploads/2022/09/Arsboni-foly%C3%B3irat_2022_1_2.pdf (last visited 26 January 2023).

⁶² For more information see: Stacey B. Steinberg: Sharenting: Children's Privacy in the Age of Social Media, *Emory Law Journal* 66, no. 4 (2017), 849-850 and Tehila Minkus, Kelvin Liu, and Keith W. Ross: Children seen but not heard: When parents compromise children's online privacy, In *Proceedings of the 24th international conference on World Wide Web* (2015), 777.

scenarios, these potential risks will be examined in detail. By doing so, we will try to answer the tenth and last research question of this thesis. Instead of completely prohibiting the sharing of child-related information, we will explore the optimal approach and restrictions that can be implemented.

1.4 Research Methodology

This thesis will be written using the comparative law method and to strengthen and deepen our research, we will employ this method focusing not only on the similarities, but also on the differences between the GDPR and the COPPA. In order to accomplish this, we will need to compare equivalent phrases and understand their variances in meaning. For instance, “operator” in the COPPA is nearly synonymous with “data controller” in the GDPR; however, there are some nuances, such as the fact that GDPR defines the “data controller” as the one who “determines the purposes and means of the processing of personal data”⁶³, whereas the COPPA defines “operator” as the one “who collects or maintains personal information”⁶⁴. Another difference between COPPA and GDPR terminology is that the former refers to any identifiable information related to an individual as “personal information,”⁶⁵ while the latter refers to the same as “personal data”.⁶⁶ The comparative method enables us to determine if two separate legal systems may reach roughly the same outcome without applying the same terminology, rule, or procedure.⁶⁷

The comparative law method enriches the research by analysing the importance of similarities and differences not only in light of the legal systems of both jurisdictions, but also considering their respective cultures. Likewise, this method enables us to identify the discrepancies between written legislation and actual law enforcement. Consequently, this methodology helped us in enhancing our research by allowing us to focus not only on the letter of the law but also on law in action by analysing the historical contexts of privacy and data protection, the case law, the works of scholars, conducted surveys and statistics in the

⁶³ GDPR, Article 4(7).

⁶⁴ 16 CFR 312.2 “Operator”.

⁶⁵ 16 CFR 312.2 “Personal information”.

⁶⁶ GDPR, Article 4(1).

⁶⁷ John C. Reitz: How to Do Comparative Law, *American Journal of Comparative Law* 46, no. 4 (Fall 1998), 621.

literature, and social media examples in order to better comprehend the implementation of legal text into practise.⁶⁸

It is important to highlight at this stage that one of the most challenging aspects of researching the doctrine and case law was the difficulty in locating appropriate sources. This is because the great majority of academics write about general topics and issues linked to the privacy and data protection of adults, rather than focusing on the privacy and data protection rights of children. In addition, there are not many cases involving children's online data protection and privacy, because online sharing of children's data and children's use of the Internet is such a recent topic that it will take time for today's child influencers to reach adulthood and, for instance, exercise their right to be forgotten before the courts.⁶⁹

The analytical method will also be fruitful for analysing the legal rules and concepts of these two different legal systems. It will not only enable us to detect the common parts and variations between these legal systems, but also to compare them to the “ideal type.”⁷⁰ Detecting and searching for the *ideal* will allow us to design solutions and make suggestions. For example, when we write on privacy and data protection rights under the COPPA and the GDPR, we will study the most effective ways of implementing these rights in addition to analysing these legislation as they currently stand. We will evaluate whether these privacy and data protection rights are granted to children or their parents, and moreover, if they should be exercised directly by children or on their behalf by parents. This would enable us to contribute to the development of child-friendly online privacy and data protection rules and enforcements.

Legal transplant is a highly significant and useful concept in the subject of comparative law, which will also be addressed in this thesis. Although *Alan Watson* created the term in 1974, this practise has been around for ages. We can describe legal transplanting as the mobility of rules from one legal system to another.⁷¹ Both *Watson* and *Legrand* recognize the concept of legal transplanting in a strict manner, as seen by their famous debate on this topic. According to *Watson*, a rule remains the same wherever it goes,⁷² while *Legrand*

⁶⁸ John C. Reitz: How to Do Comparative Law, *American Journal of Comparative Law* 46, no. 4 (Fall 1998), 626-631.

⁶⁹ The right to be forgotten of children will be analysed in depth in the Chapter 4 and Chapter 7.

⁷⁰ For more information about analytical method see: Mark Van Hoecke: *Methodology of comparative legal research*, *Law and method* (2015), 13-16.

⁷¹ Alan Watson: Introduction to Legal Transplants In *Legal Transplants: An Approach to Comparative Law* (1974), 21.

⁷² Alan Watson: Introduction to Legal Transplants In *Legal Transplants: An Approach to Comparative Law* (1974), 21.

contends that the application of a legal transplant is impossible due to the historical and cultural diversity of each society and legal system.⁷³ We, however, believe that the transfer of rules from one legal system to another is possible and they will be formed and developed by each system's particular historical and sociological processes and will result in the enrichment of both legal systems. In our paper published in *The Journal of Comparative Law* on this topic, we summed up our position on this concept as follows:

“Legal transplantation is necessary because it not only serves the host culture, but also serves the parent culture. By doing so it not only changes the rules and laws, but also changes the social dynamics and has a greater impact on the future.”⁷⁴

Accordingly, in this thesis, we will discuss a legal transplant case adopted from the COPPA to the GDPR in the digital era related to our topic which is the online age threshold for obtaining parental consent. We will also propose a new legal transplant from the COPPA to the GDPR addressing the methods of verifying parental consent, since it would guide data controllers on how to determine if the given consent is from a parent or not.

1.5 Research Structure

In Chapter 2, we analyse the historical context of both the GDPR and the COPPA, as well as the reasons and movements behind the privacy and data protection of children in both legal systems. In Chapter 3, the concept of parental consent to make the processing of underage children's data lawful and verifying the parental consents will be examined in detail. In Chapter 4, main rights of children and parents will be outlined and analysed in both legislations. In Chapter 5, main obligations of data controllers under the GDPR and the COPPA will be discussed. In Chapter 6, we determine the significance of transatlantic data flows as well as if the US will ever attain an "adequate level" of data protection and if so, how it will affect the flow of children's data from the EU to the US. In Chapter 7, we will compare and evaluate the privacy policies and terms of service of three social media platforms (YouTube, Facebook, and Instagram), as well as the use of these social media sites

⁷³ Pierre Legrand: The impossibility of 'legal transplants, *Maastricht journal of European and comparative law* 4, no. 2 (1997), 111.

⁷⁴ Asli Alkis Tümtürk: The Threshold Age for Children's Online Consent in Light of the Watson/Legrand Debate: Is Legal Transplant Possible in the Digital Era?, *The Journal of Comparative Law* vol. 17/1 (2022), 243.

by parents and children, in order to determine how legal texts manifest themselves in online practise.

2. GDPR Article 8 and COPPA: The historical context and evolution of the current standards, definitions, and issues pertaining to the protection of children's data and privacy

Even though privacy became a widely recognised right in the nineteenth and twentieth centuries, its origins date back much further. In the *Code of Hammurabi*, for instance, domestic life was protected against invasions by the provision, “*If a man makes a breach into a house, one shall kill him in front of the breach, and bury him in it.*” And this specific protection of the house is strongly supported by religion at the time. The concept that the house is sacred was also prevalent in ancient Greece and Roman law. In fact, Roman law originally expressed this in the proverb “*Every man's home is his castle.*”⁷⁵

The distinction between the private and public gives birth to the notion of privacy. This separation essentially stems from his/her goods versus theirs and himself/herself versus the others. Nevertheless, the concept and understanding of privacy evolve with time.⁷⁶ In the Roman era, even though the house was a private area, there were no toilets within the homes. One or two out of every five people may have had toilets at home, but the majority used the public toilets, where seats are adjacent to one another and there are no signs of dividers between the seats.⁷⁷ Even researchers have questions such as whether or not public restrooms were socializing places where people sat half-naked close to one another, had a chat and made friends which is quite the contrary of the modern sense of privacy.⁷⁸

We may infer that as society and the economy evolve, so does the concept of privacy. As a result of the economic and social changes of the 19th century and urbanisation, for instance, people began to live in crowded cities, resulting in a loss of physical space and privacy. Notwithstanding, in contrast to the village life, they were able to experience a new type of mental privacy and freedom, in the sense that who they were living with, where they were working, and what they were doing were no longer concerns of their neighbours. The development of newspapers and photojournalism, however, has resulted in the emergence

⁷⁵ Samuel Dash: *The intruders: Unreasonable searches and seizures from King John to John Ashcroft*, Rutgers University Press (2004), 9.

⁷⁶ Adrienn Lukács: What is privacy? The history and definition of privacy, In: Gábor Keresztes (ed.): *Tavaszi Szél 2016 Tanulmánykötet I.*, Budapest, Doktoranduszok Országos Szövetsége (2016), 257 <https://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf> (last visited 4 January 2023).

⁷⁷ Chelsea Wald: The secret history of ancient toilets, *Nature* 533, no. 7604 (2016), 457.

⁷⁸ Chelsea Wald: The secret history of ancient toilets, *Nature* 533, no. 7604 (2016), 458.

of a new form of surveillance, which has a particularly negative impact on famous persons and families.⁷⁹

In 1890, the “most influential law review article of all”⁸⁰ titled “Right to Privacy”,⁸¹ was written by *Samuel Warren* and *Louis Brandeis* in response to these sociological and technological advancements and new forms of privacy loss. With these famous lines below, the article describes how the press disregards and violates the boundaries of individuals' private lives, and how these violations of privacy impair the well-being of individuals:

“[...] The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers. To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle. The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury [...]”⁸²

There is a precise theory among scholars that Warren was prompted to write this article because he was particularly bothered by a specific item about his private family matters in a Boston newspaper.⁸³ Nonetheless, it is widely accepted that Warren's dislike of Boston's print media in general and his perception of its invasion of social privacy inspired this article

⁷⁹ Adrienn Lukács: What is privacy? The history and definition of privacy, In: Gábor Keresztes (ed.): *Tavaszi Szél 2016 Tanulmánykötet I.*, Budapest, Doktoranduszok Országos Szövetsége (2016), 257 <https://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf> (last visited 4 January 2023).

⁸⁰ Harry Kalven Jr.: Privacy in Tort Law--Were Warren and Brandeis Wrong, *Law and Contemporary Problems* 31, no. 2 (1966), 327.

⁸¹ Samuel D. Warren and Louis D. Brandeis: Right to Privacy, *Harvard Law Review* 4, no. 5 (1890), 193-220.

⁸² Samuel D. Warren and Louis D. Brandeis: Right to Privacy, *Harvard Law Review* 4, no. 5 (1890), 196.

⁸³ “Warren's perception of the press may have been influenced by his sensitive nature. What may have further distorted this perception, however, was an unwillingness to concede that he, and others like him, were in many ways “public figures,” in that they regularly engaged in a variety of political and community activities.” in James H. Barron: Warren and Brandies, the Right to Privacy, 4 *Harv. L. Rev.* 193 (1890): Demystifying a Landmark Citation, *Suffolk University Law Review* 13, no. 4 (1979), 910.; For additional information regarding the historical review of possible invasions into Warren's private life that inspired the famous article “Right to Privacy”: James H. Barron: Warren and Brandies, the Right to Privacy, 4 *Harv. L. Rev.* 193 (1890): Demystifying a Landmark Citation, *Suffolk University Law Review* 13, no. 4 (1979), 895-922 cited in Ben Bratman: Brandeis and Warren's the Right to Privacy and the Birth of the Right to Privacy, *Tennessee Law Review* 69, no. 3 (2002), 629.

and with Brandeis's sophisticated and “eloquent” contribution resulted in a landmark paper. In any case, the idea of developing this article, the article's poignant focus on human sensitivities, and its definition of privacy as the “right to be let alone” all contributed to the establishment of the modern fundamental right to privacy.⁸⁴

With the increased use of computers in the 1960s, particularly in large industries and the US security, military and space services,⁸⁵ it was questioned whether the right to privacy was sufficient to cover the protection of private life, and technological advances resulted in the development of a new right which is called the right to data protection and its subject is also the protection of private life.⁸⁶

Consequently, Alan Westin's publication titled *Privacy and Freedom* in 1967 contributed to define the global field of privacy and data protection as: “Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”⁸⁷ *Jeffrey Rosen*, a law professor at George Washington University and the legal affairs editor of *The New Republic*, said “He was the most important scholar of privacy since Louis Brandeis,” and added, “He transformed the privacy debate by defining privacy as the ability to control how much about ourselves we reveal to others.”⁸⁸ Moreover, *Marc Rotenberg*, the executive director of the Electronic Privacy Information Centre in Washington, remarked, “This concept⁸⁹ became the cornerstone of our modern right to privacy.”⁹⁰ Hence, *Privacy and Freedom* became the reference book for the upcoming informational privacy, and it was believed that this article was the first which examined the coming issues regarding data privacy and data protection.⁹¹

⁸⁴ Ben Bratman: Brandeis and Warren's the Right to Privacy and the Birth of the Right to Privacy, *Tennessee Law Review* 69, no. 3 (2002), 629.; James H. Barron: Warren and Brandies, the Right to Privacy, 4 *Harv. L. Rev.* 193 (1890): Demystifying a Landmark Citation, *Suffolk University Law Review* 13, no. 4 (1979), 876.; Vernon Valentine Palmer: Three Milestones in the History of Privacy in the United States, *Tulane European and Civil Law Forum* 26 (2011), 71.

⁸⁵ For more information: Computer History Museum: Timeline of Computer History, <https://www.computerhistory.org/timeline/1960/#1960s> (last visited 7 January 2023).

⁸⁶ Adrienn Lukács: What is privacy? The history and definition of privacy, In: Gábor Keresztes (ed.): *Tavaszi Szél 2016 Tanulmánykötet I.*, Budapest, Doktoranduszok Országos Szövetsége (2016), 259 <https://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf> (last visited 4 January 2023).

⁸⁷ Alan F. Westin: *Privacy and Freedom*, Atheneum New York (1967), 1-487.

⁸⁸ The New York Times, Alan F. Westin, Who Transformed Privacy Debate Before the Web Era, Dies at 83 (22 February 2013) <https://www.nytimes.com/2013/02/23/us/alan-f-westin-scholar-who-defined-right-to-privacy-dies-at-83.html> (last visited 7 January 2023).

⁸⁹ Marc Rotenberg uses “this concept” to refer to Alan Westin's definition of privacy.

⁹⁰ The New York Times, Alan F. Westin, Who Transformed Privacy Debate Before the Web Era, Dies at 83 (22 February 2013) <https://www.nytimes.com/2013/02/23/us/alan-f-westin-scholar-who-defined-right-to-privacy-dies-at-83.html> (last visited 7 January 2023).

⁹¹ Andrew Clearwater and J. Trevor Hughes: In the Beginning - An Early History of the Privacy Profession, *Ohio State Law Journal* 74, no. 6 (2013), 899.

The aforementioned improvements to the right to privacy and data protection first arise in the United States, followed by the European Union, which developed a new type of protection.⁹² Privacy rights first appeared in common law torts in the US, where criminal and civil remedies existed for the exploitation of an individual's personal name and image for advertising purposes. It initially appears in a New York legislation classifying the use of the name, portrait, or image of any person for “advertising purposes or for the purposes of trade” without obtaining their written consent as both a misdemeanour and a tort.⁹³ In the amended version of this statute, it is still stated, without omitting the children's privacy rights, that

“A person, firm, or corporation that uses the name, portrait, or picture of a living person for advertising or commercial purposes without first obtaining the written consent of that person, or if a minor, of his or her parent or guardian, is guilty of a misdemeanour.”⁹⁴

Afterwards, in *Griswold v. Connecticut*, the Supreme Court has recognised privacy rights as constitutional rights. A Connecticut statute prohibited the use of any substance or medication to prevent conception. Therefore, the plaintiffs in that case argued that the enacted Connecticut statute violated the Fourteenth Amendment. The ruling was sustained by an intermediate court of appeal and the state's highest court. Because the Fourteenth Amendment states that “[...] No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States [...]”⁹⁵ the Supreme Court ruled that the Connecticut law in question violated the fundamental right to privacy surrounding marriage and for the first time recognised marital privacy as a constitutional right.⁹⁶

⁹² Máté Dániel Szabó: Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival, *Információs Társadalom: társadalomtudományi folyóirat* 5, no. 2 (2005), 44.

⁹³ N.Y. Sess. Laws 1903, ch. 132, §§ 1-2, amended by N.Y. Civ. Rights Law, §§ 50-51 (McKinney 1909) cited in W. Page Keeton (et al.): *Prosser and Keeton on the Law of Torts*, West Publishing Co. St. Paul Minn. 5th ed. (1984), 850-851.

⁹⁴ N.Y. Civ. Rights Law, §§ 50 (McKinney 1909).

⁹⁵ U.S. Const. amend. XIV section 1.1: “All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.”

⁹⁶ *Griswold v. State of Connecticut*, 381 U.S. 479 (1965) 484-86. <https://tile.loc.gov/storage-services/service/l/usrep/usrep381/usrep381479/usrep381479.pdf> (last visited 9 January 2023). See also: Haeji Hong: Dismantling the Private Enforcement of the Privacy Act of 1974: *Doe v. Chao*, *Akron Law Review* 38, no. 1 (2005), 76-77 and Virginia A. M. Talley: Major Flaws in Minor Laws: Improving Data Privacy Rights and Protections for Children under the GDPR, *Indiana International & Comparative Law Review* 30, no. 1 (2019), 143.

As previously noted, the increasing use of computers and technological developments have resulted in the establishment of a new right known as the right to data protection, and individuals are most concerned about the government's power to access, use, analyse, and store personal information. In response to these concerns, the United States Congress adopted the Privacy Act of 1974.⁹⁷ The Privacy Act of 1974 aims to restrict government violations of citizens' personal information while maintaining the government's legitimate efficiency goals. This statute prohibits the collection, use, and storage of personally identifiable information without the individual's consent. There are, however, numerous government-beneficial exceptions to this restriction.⁹⁸

However, the Privacy Act of 1974 is not the same as the GDPR, the EU's overarching regulation, because it only applies to the processing of personal information by the federal government. Therefore, after the Privacy Act of 1974, several laws targeting different sectors and data subject groups were enacted, including the Health Insurance Portability and Accountability Act (HIPPA),⁹⁹ the Family Educational Rights and Privacy Act (FERPA),¹⁰⁰ Telephone Consumer Protection Act of 1991 (TCPA)¹⁰¹ and most significantly for our research, the Children's Online Privacy and Protection Act (COPPA)^{102, 103}

Following advancements in the right to privacy in the US, two critical international treaties developed at the regional level in Europe: the European Convention on Human Rights (ECHR) was established by the Council of Europe in 1950,¹⁰⁴ and the Charter of Fundamental Rights of the European Union was officially declared by the European Parliament, the European Council, and the European Commission in 2000.¹⁰⁵ According to

⁹⁷ Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896, as amended 5 U.S.C. § 552a. See also: Virginia A. M. Talley: Major Flaws in Minor Laws: Improving Data Privacy Rights and Protections for Children under the GDPR, *Indiana International & Comparative Law Review* 30, no. 1 (2019), 143.

⁹⁸ 5 U.S.C. § 552a(b)-(f). For detailed Overview of the Privacy Act of 1974: Haeji Hong: Dismantling the Private Enforcement of the Privacy Act of 1974: *Doe v. Chao*, *Akron Law Review* 38, no. 1 (2005), 81-85.

⁹⁹ Health Insurance Portability and Accountability Act. Pub. L. No. 104-191, 110 Stat. 1936 (1996).

¹⁰⁰ Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (1974).

¹⁰¹ Telephone Consumer Protection Act of 1991, 47 U.S. Code § 227 (1991).

¹⁰² 16 CFR Part 312 Children's Online Privacy Protection Act; Final Rule, 15 U.S.C. §§ 6501–6506, *Federal Register* Vol. 64, No. 212, 03.11.1999, p. 59888-59915.

¹⁰³ Holly Kathleen Hall: Oversharenting; Is It Really Your Story to Tell, *John Marshall Journal of Information Technology and Privacy Law* 33, no. 3 (2018), 132 cited in Virginia A. M. Talley: Major Flaws in Minor Laws: Improving Data Privacy Rights and Protections for Children under the GDPR, *Indiana International & Comparative Law Review* 30, no. 1 (2019), 143-144.

¹⁰⁴ Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, https://www.echr.coe.int/documents/convention_eng.pdf (last visited 10 January 2023).

¹⁰⁵ Charter of Fundamental Rights of The European Union, OJ C 364, 18.12.2000, pp. 1-22. It became legally binding as EU primary law with the Lisbon Treaty(*) in 1 January 2009.

Article 8 of the ECHR, “Everyone has the right to respect for his private and family life, his home and his correspondence.”¹⁰⁶ Later the same right appeared in the CFR almost identically as “Everyone has the right to respect for his or her private and family life, home and communications”.¹⁰⁷ However, because these articles are not very thorough and do not define what is privacy or how it should be legally guaranteed, the decisions of European Court of Human Rights (ECtHR) could offer these answers.¹⁰⁸

Nonetheless, the ECtHR has stated in its case law that there is no exhaustive concept of privacy since the ECHR's reach is so expansive and technological progress necessitates constant changes to the terms and definitions of privacy.¹⁰⁹ Even though the list is not exhaustive, we may still enumerate some of the examples that the European Court of Human Rights has deemed to be an intrusion of private life under Article 8 of ECHR, such as the protection of personal data,¹¹⁰ wiretapping,¹¹¹ sexual life,¹¹² profession or domicile,¹¹³ and the protection against the environmental nuisances (e.g., noise nuisance).¹¹⁴ It is ideal to develop a flexible approach to privacy since, as stated previously, the concept of privacy is changing as technology improves and society evolves.¹¹⁵

Case law from the European Court of Human Rights (ECtHR) had a significant effect on the European Union's Court of Justice (CJEU). This significant effect can be explained in a few ways: as we mentioned above, Article 7 of the CFR is substantially identical to Article 8 of the European Convention on Human Rights.¹¹⁶ Besides, according to Article 52

(*) Treaty of Lisbon, Amending the Treaty on European Union and the Treaty establishing the European Community, OJ C 306, 17.12.2007, p. 1–271.

¹⁰⁶ Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, Article 8(1) https://www.echr.coe.int/documents/convention_eng.pdf (last visited 10 January 2023).

¹⁰⁷ Charter of Fundamental Rights of The European Union, OJ C 364, 18.12.2000, pp. 1-22, Article 7.

¹⁰⁸ Raphael Gellert and Serge Gutwirth: The legal construction of privacy and data protection, *Computer Law & Security Review* 29, no. 5 (2013), 524.

¹⁰⁹ *Niemietz v. Germany* judgment on 16 December 1992, no. 13710/88 para. 29: “The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of “private life”[...]”

¹¹⁰ *Leander v. Sweden* judgment of 26 March 1987, no. 9248/81 para. 46-48.

¹¹¹ *Klass and Others v. Germany* judgment on 6 September 1978, no. 5029/71 para. 41.

¹¹² *Dudgeon v. the United Kingdom* judgment on 22 October 1981, no. 7525/76 para. 40-41.

¹¹³ *Niemietz v. Germany* judgment on 16 December 1992, no. 13710/88 par. 28-33.

¹¹⁴ *Powell and Rayner v. the United Kingdom* judgment of 21 February 1990, no. 9310/81, para. 41.

¹¹⁵ For further information regarding the cases and the interpretation: Adrienn Lukács: What is privacy? The history and definition of privacy, In: Gábor Keresztes (ed.): *Tavaszi Szél 2016 Tanulmánykötet I.*, Budapest, Doktoranduszok Országos Szövetsége (2016), 260 <https://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf> (last visited 10 January 2023) and Raphael Gellert and Serge Gutwirth: The legal construction of privacy and data protection, *Computer Law & Security Review* 29, no. 5 (2013), 524-527.

¹¹⁶ Case C-450/06 *Varec* [2008] ECR I-581, EU:C:2008:91, para. 48: “One of the fundamental rights capable of being protected in this way is the right to respect for private life, enshrined in Article 8 of the ECHR, which flows from the common constitutional traditions of the Member States and which is restated in Article

of the CFR, the extent and meaning of the rights included in the CFR that were inspired by the ECHR are the same as those secured by the ECHR:

“[...] In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.”¹¹⁷

As technology improved and the impacts of the digitalisation became abundantly apparent, the EU acknowledged the need for data protection.¹¹⁸ Although the right to data protection derives from the right to privacy, it is more specific in ensuring the fair collection, use, and storage of personal information by both the private and public sectors. The data protection encompasses all personally identifiable information, including names, birth dates, photographs, videos, postal addresses, email addresses, telephone numbers, and biometric data (e.g., fingerprints). IP addresses, cookies, and location data are also considered personal information, as they enable the identification of individuals through their devices.¹¹⁹ The data protection extends beyond the concept of privacy in that it protects individuals through their personal data even if it is not a violation of privacy, but a violation of other fundamental rights, such as if the data subject is threatened with discrimination.¹²⁰

7 of the Charter of fundamental rights of the European Union, proclaimed in Nice on 7 December 2000 (OJ 2000 C 364, p. 1) (see, in particular, Case C-62/90 Commission v Germany [1992] ECR I-2575, paragraph 23, and Case C-404/92 P X v Commission [1994] ECR I-4737, paragraph 17). It follows from the case-law of the European Court of Human Rights that the notion of ‘private life’ cannot be taken to mean that the professional or commercial activities of either natural or legal persons are excluded (see Niemietz v Germany, judgment of 16 December 1992, Series A No 251-B, §29; Société Colas Est and Others v France, No 37971/97, §41, ECHR 2002-III; and also Peck v The United Kingdom No 44647/98, §57, ECHR 2003-D). Those activities can include participation in a contract award procedure.”

¹¹⁷ CFR, Article 52(3).

¹¹⁸ Graham Pearce and Nicholas Platten: Achieving personal data protection in the European Union, *JCMS: Journal of Common Market Studies* 36, no. 4 (1998), 531.

¹¹⁹ European Data Protection Supervisor (EDPS), Data Protection, https://edps.europa.eu/data-protection/data-protection_en (last visited 13 January 2023).

¹²⁰ CFR, Article 21: “1. Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited. 2. Within the scope of application of the Treaties and without prejudice to any of their specific provisions, any discrimination on grounds of nationality shall be prohibited.”

ECHR, Article 14: “The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.”

See also: Raphael Gellert and Serge Gutwirth: The legal construction of privacy and data protection, *Computer Law & Security Review* 29, no. 5 (2013), 526.

Besides the right to respect for private and family life (Article 7)¹²¹, the CFR recognises the right to the protection of personal data (Article 8)¹²² and the related core concepts. It specifies that the processing must be lawful, fair, and limited to the stated purposes (either consent or other legitimate interests laid down by the law). Moreover, Article 8 of the CFR stipulates that individuals have the right to access and rectify their personal data.¹²³ The CFR elevates the right to data protection to the status of a fundamental right under EU law. Article 8 of the CFR, which was drafted some years after Convention 108 and the Directive 95/46/EC,¹²⁴ shall be interpreted as a continuation of pre-existing EU data protection legislation.¹²⁵

Initially, ECtHR case law issued data protection within Article 8 of the ECHR,¹²⁶ but in 1981, the Council of Europe established the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). Convention 108 was the first international treaty with legal force in the field of data protection. Under the terms of this convention, the parties have agreed to alter their domestic legislation to conform to the requirements and principles, and they will guarantee that the fundamental rights of all individuals relating to the processing of personal data are protected by their domestic laws.¹²⁷

With the Convention 108, the Council of Europe was successful in raising the concept of data protection and defining the main principles of data protection; however, it was not successful in harmonising the legal framework across the Member States, as the entry into force dates were not consistent.¹²⁸ Besides, the Member States' data protection approach was

¹²¹ CFR, Article 7.

¹²² CFR, Article 8.

¹²³ CFR, Article 8(2).

¹²⁴ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50.

¹²⁵ European Union Agency for Fundamental Rights, Council of Europe, European Court of Human Rights, European Data Protection Supervisor: Handbook on European data protection law (2018), 28.

https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf (last visited 17 February 2023).

¹²⁶ Leander v. Sweden judgment of 26 March 1987, no. 9248/81 para. 46-48.

¹²⁷ Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 28.01.1981, ETS No. 108 amended as Council of Europe, Convention 108+ Convention for the protection of individuals with regard to the processing of personal data, ETS No. 108 (2018)

<https://www.coe.int/en/web/data-protection/convention108-and-protocol> (last visited 16 February 2023).

¹²⁸ Council of Europe, Chart of signatures and ratifications of Treaty 108,

<https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108> (last visited 13 January 2023).

not uniformed. In terms of data protection, some Member States had very strict legislation while others had almost none at all.¹²⁹

The EU's Member States also had different data protection standards, which had restricted free data flow within the EU and hindered trade among the Member States. The European Commission proposed an EC regulation in 1992 to address the need for data protection rules to be harmonised across Member States in order to create a fully united market.¹³⁰ Afterwards, in October 1995, the European Union's Directive 95/46/EC was enacted¹³¹ with the stated goal of harmonising data protection legislation at the national level within the European Union.¹³²

Nevertheless, according to Article 288 of the Treaty on the Functioning of the European Union (TFEU), directives are not directly applicable in the Member States once they come into force at the Union level, since they need EU Member States to incorporate them into national law in order to accomplish the directive's intended results. As stated in the TFEU, directives are legally binding on Member States, but it is up to national authorities to choose the form and means of attaining the intended results.¹³³ With respect to this, the European Court of Justice has determined that directives do not have direct effect unless its "clear, precise, and unconditional provision[s]" are implemented sufficiently at the national level.¹³⁴

¹²⁹ "France and Germany have possibly the strictest laws in this area, while Greece, Belgium, and Italy have almost none." Peter Mei: The EC Proposed Data Protection Law, *Law and Policy in International Business* 25, no. 1 (1993), 305.

¹³⁰ European Commission, Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Preamble, COM(92) 422 final - SYN 287, OJ C 311/30, 27.11.1992, pp. 30-61.; See also: Peter Mei: The EC Proposed Data Protection Law, *Law and Policy in International Business* 25, no. 1 (1993), 305.

¹³¹ "Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest at the end of a period of three years from the date of its adoption." Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31-50, Article 32(1).

¹³² Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31-50, Article 1: "1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. 2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1."

¹³³ Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, p. 47-390, Article 288.

¹³⁴ "[...] according to settled case-law, a directive cannot of itself impose obligations on an individual and cannot therefore be relied upon as such against an individual. It follows that even a clear, precise and unconditional provision of a directive seeking to confer rights or impose obligations on individuals cannot of itself apply in proceedings exclusively between private parties."

Case C-80/06, *Carp v. Electricité de France (EDF)* [2007] ECR I-4473, EU:C:2007:327, para. 20 cited in Paul Craig: *The Evolution of EU Law*, 2nd ed. Oxford: Oxford University Press (2011), 335.

Therefore, adopting the directives into domestic legislation does not result in completely uniform national laws across the Member States.

In the meantime, the technology had developed since the Directive 95/46/EC was adopted, as well as technological advancements such as cloud computing, personalised advertising, and social networking platforms, geo-location apps created several privacy and data protection challenges. In addition, because of globalisation, cross-border data flows and data processing have expanded. Besides, Article 16 of the TFEU's¹³⁵ coming into effect ushered in a new era for data protection and established a sound legal foundation for a comprehensive data protection legislation in the EU.¹³⁶

Accordingly, the European Data Protection Supervisor published an opinion on the European Commission's Communication in June 2011 regarding a need for “a comprehensive approach on personal data protection in EU”.¹³⁷ This need was met by enacting a regulation rather than a directive, which are legal actions that apply directly and entirely to all EU Member States as soon as they enter into force, without the need for transposition into national law.¹³⁸

Following its adoption by the European Parliament and the Council of the European Union, the General Data Protection Regulation (GDPR) went into effect in 2016. As of May 25, 2018, compliance is required for any controller or processor that processes personal data and established in the EU, regardless of whether the processing occurs in the EU or not.¹³⁹ In addition, it applies if data subjects are EU residents/citizens and the data controller or processor is based outside the EU, but the providing of goods and services to such data subjects in the EU or monitoring of their behaviour occurs within the EU.¹⁴⁰ Consequently, we may infer that the GDPR created a wide territorial scope.

Additionally, the GDPR strengthened data protection and privacy rights. At this moment, we only discuss a few of the most significant amendments, but in the following chapters, we will examine in depth the provisions relevant to our topic. For instance, data

¹³⁵ TFEU, Article 16.

¹³⁶ TFEU, General Part, Context, para. 13-16.

¹³⁷ Opinion on the Communication from the Commission on "A comprehensive approach on personal data protection in the European Union", OJ C 181/01, 22.06.2011, p.1 https://edps.europa.eu/data-protection/our-work/publications/opinions/comprehensive-approach-personal-data-protection_en (last visited 18 February 2023).

¹³⁸ Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, p. 47–390, Article 288.

¹³⁹ GDPR, Article 3(1).

¹⁴⁰ GDPR, Article 3(2).

portability is a new right introduced by the GDPR.¹⁴¹ Besides, the right to be forgotten, initially articulated by the CJEU,¹⁴² is incorporated into the GDPR as a separate data subject right.¹⁴³ Moreover, the concept of consent is defined under the GDPR as:

“any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.¹⁴⁴

On one hand, the core concept of consent is quite similar to that of Directive 95/46/EC,¹⁴⁵ and it remains one of the lawful bases for processing personal data.¹⁴⁶ On the other hand, the GDPR gives further guidance on how the data controller should comply with the consent's main components (e.g., demonstrating the given consent, to ensure that consent is freely given and there is no imbalance of power between the data subject and the data controller).¹⁴⁷ It also includes instructions on how the data subject may exercise more control over their data, such as by withdrawing their consent at any time, which must be as simple as giving consent in the first place.¹⁴⁸

Furthermore, fines for GDPR violations increased to a maximum of €20 million, or 4% of the company's global turnover of the preceding financial year.¹⁴⁹ Likewise, the controller or processor shall compensate any individual who has suffered material or non-material harm as a direct result of the controller's or processor's violation of the GDPR.¹⁵⁰ Overall, the GDPR merged twenty-eight different data protection laws emanating from the Directive 95/46/EC into one single legislation that is stricter and more effective with enhanced data protection rights, concepts, and remedies in the case of a data breach.¹⁵¹

¹⁴¹ GDPR, Article 20.

¹⁴² Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González EU:C:2014:317 and Case C-507/17 Google LLC v Commission nationale de l'informatique et des libertés (CNIL) EU:C:2019:772.

¹⁴³ GDPR, Article 17 and Recital 66.

¹⁴⁴ GDPR, Article 4(11).

¹⁴⁵ Directive 95/46/EC defines the consent as: “any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.” Article 7 further states that personal data shall be processed only if: “data subject has unambiguously given his consent”.

¹⁴⁶ GDPR, Article 6(1)(a) and Directive 95/46/EC, Article 7(a).

¹⁴⁷ GDPR, Article 7 and Recitals 32, 33, 42, 43.

¹⁴⁸ Article 29 Working Party, Guidelines on consent under Regulation 2016/679 17/EN WP 259 rev.01, 10 April 2018, 4-5.

¹⁴⁹ GDPR, Article 83(6).

¹⁵⁰ GDPR, Article 82(1).

¹⁵¹ Manu J. Sebastian: The European Union's General Data Protection Regulation: How Will It Affect Non-EU Enterprises, *Syracuse Journal of Science and Technology Law* 31 (2014-2015), 222-223.

There were no particular requirements for the protection of children's personal data in Directive 95/46/EC. The GDPR, however, did not turn a blind eye to children's online activities and Article 8 of the GDPR provided special protection for the processing of children's personal data.¹⁵² However, the history of Article 8 did not reveal well-reasoned and well-justified requirements, as the majority of debates focused on articles with direct economic impact (e.g., articles related to data transfers, profiling) rather than the vulnerable data subjects who will not contribute economically to the Digital Single Market.¹⁵³ For instance, it is not well-reasoned why the age of consent barrier may be lowered to 13, and as if that were not enough, the Commission stated that for commercial purposes they adopted the US age of consent, which is 13.¹⁵⁴ Nonetheless, Member States might raise the age of consent to 16, which could lead to a lack of uniformity and validity issues when data is transferred to another country even within the EU. In that scenario, the opposite would occur when we consider the original objective of the EU about the free flow of personal data.¹⁵⁵

Besides, the GDPR does not indicate any methods for obtaining parental consent; however, for data controllers to have legal certainty, there must be guidance on how to verify such parental consent. The COPPA's following methods could serve as a model for the GPDR:¹⁵⁶

“(i) Providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or electronic scan;(ii) Requiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder; (iii) Having a parent call a toll-free telephone number staffed by trained personnel; (iv) Having a parent connect to trained personnel via video-conference; (v) Verifying a parent's identity by checking a form of government-issued identification against databases of such information, where the parent's identification is deleted by the operator from its records promptly after

¹⁵² GDPR, Article 8.

¹⁵³ Milda Macenaite and Eleni Kosta: Consent for processing children's personal data in the EU: following in US footsteps?, *Information & Communications Technology Law* 26, no. 2 (2017), 160.

¹⁵⁴ “[...] The specific rules on consent in the online environment for children below 13 years – for which parental authorisation is required – take inspiration for the age limit from the current US Children Online Data Protection Act of 1998 and are not expected to impose undue and unrealistic burden upon providers of online services and other controllers. [...]” Commission Staff Working Paper, Impact Assessment, SEC (2012) 72 final, p. 68, https://www.europarl.europa.eu/cmsdata/59702/att_20130508ATT65856-1873079025799224642.pdf (last visited 19 January 2023).

¹⁵⁵ GDPR, Article 1(3): “The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.”

¹⁵⁶ Eva Lievens and Valerie Verdood: Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation, *Computer Law & Security Review* 34, no. 2 (2018), 274.

such verification is complete; or (vi) Provided that, an operator that does not “disclose” (as defined by [§ 312.2](#)) children's personal information, may use an email coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: Sending a confirmatory email to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. An operator that uses this method must provide notice that the parent can revoke any consent given in response to the earlier email.”¹⁵⁷

Nonetheless, since the GDPR does not specify any particular procedure, the burden lies on the data controllers by obliging them to make reasonable efforts, taking into account the available technology, to determine if the consent is granted by the authorised parents.¹⁵⁸ It is unclear, however, how much work would be considered reasonable and how this should be proven and confirmed.¹⁵⁹

Both COPPA and GDPR rely on the self-determination of users for age verification; however, given the present state of technology, alternative approaches should be investigated because self-verification is an easy-to-implement but also easy-to-evade method.¹⁶⁰ In the next chapter on the notion of parental consent, we will analyse in depth all of the aforementioned topics, including the general concept of consent, parental consent under the GDPR and COPPA, the minimum age for parental consent, and online age verification methods.

2.1 Short Summary

In the previous chapter, we examined the history of privacy and data protection in the US and the EU, as well as how the concepts of privacy and data protection have developed through time as a result of economic and social changes. Later, we argued that technological advances and computer innovations gave rise to a new right, data protection, which was derived from the protection of private life.

¹⁵⁷ 16 CFR COPPA 312.5(b)(2).

¹⁵⁸ GDPR, Article 8(2).

¹⁵⁹ GDPR Article 8(2) and Milda Macenaite and Eleni Kosta: Consent for processing children’s personal data in the EU: following in US footsteps?, *Information & Communications Technology Law* 26, no. 2 (2017), 177.

¹⁶⁰ Milda Macenaite and Eleni Kosta: Consent for processing children’s personal data in the EU: following in US footsteps?, *Information & Communications Technology Law* 26, no. 2 (2017), 191.

Most importantly for our thesis, we have explained the background of the GDPR and the COPPA and we concluded this chapter by mentioning the parts that should be improved, such as the consent age threshold (which should be uniform and well-justified across all EU Member States) and the introduction of effective and innovative methods for obtaining parental consent (some of the methods for verifying parental consent of the COPPA might be transplanted into the GDPR Article 8) as well as methods for verifying children's age when accessing websites, particularly websites that contain age-restricted content.

This chapter contributes to the literature by providing a deductive comparison of the historical roots of the COPPA and Article 8 of the GDPR. In addition, it was an important chapter for us to analyse the flaws and strengths of both pieces of legislation since it led us to the upcoming chapters in which we would examine them in further detail.

3. Concept of parental consent in the GDPR and COPPA

3.1 Concept of consent in the GDPR

Article 8 of the Charter of Fundamental Rights of the EU (CFR) highlights the importance of consent as a lawful basis for processing personal data and stipulates that everyone should have control over their data.¹⁶¹ In accordance with the CFR, consent is one of the six legal grounds for processing personal data under the GDPR¹⁶² and is defined as:

“ [...] any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her” under the GDPR.¹⁶³

According to the Preamble of the GDPR, it is one of the main goals of the GDPR to ensure the data subjects' control, which is why data controllers must ensure that they collect personal data based on consent obtained in complete accordance with the CFR and the GDPR. Because otherwise, the processing of the collected personal information would be unlawful.¹⁶⁴

First and foremost, consent should be freely given, which implies that the data subject should have a genuine choice. For example, if online content cannot be accessible without consent, there is no real choice, and hence the consent-obtaining process would be unlawful.¹⁶⁵

Second, consent should be granted for one or more specific purposes. Therefore, the necessity for specific consent should be considered in light of the purpose limitation principle, which states that personal data must be “collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes”¹⁶⁶. For example, if the data subject consented to YouTube collecting their data in order to show them similar content videos, but YouTube decides to allow third parties to

¹⁶¹ CFR, Article 8.

¹⁶² GDPR, Article 6(1).

¹⁶³ GDPR, Article 4 (11).

¹⁶⁴ Article 29 Working Party, Guidelines on consent under Regulation 2016/679 17/EN WP 259 rev.01, 10 April 2018, 1-31, 3.

¹⁶⁵ Article 29 Working Party, Guidelines on consent under Regulation 2016/679 17/EN WP 259 rev.01, 10 April 2018, 1-31, 5-6.

¹⁶⁶ GDPR, Article 5(1)(b).

send advertisements linked to the material they are watching, it should obtain a new consent for this new purpose.¹⁶⁷

In light of the GDPR's transparency principle, consent should be informed.¹⁶⁸ The data controller must inform the data subject of their identity, contact information, the purpose for collecting personal data, the type of data collected and used, the data subject's right to withdraw consent, and the appropriate safeguards in the event of data transfers to a third country or international organisation.¹⁶⁹ These details should be written in a clear and simple manner that everyone can comprehend, not only lawyers. If children are the intended audience, privacy policies should be age appropriate. For example, it might be illustrated with simple and fun animated movies or vivid drawings.¹⁷⁰

Consent should be unambiguous and given by the data subject in the form of a clear statement or affirmative action. As a result, pre-ticked or opt-out consent options are not allowed by the GDPR since consent must be obtained prior to the collection of personal data. Consent can be granted by signing a document, writing a clear statement, expressing orally by phone or video call, or actively ticking an optional box declaring “I agree”, “I consent”, and so on. For example, if consent is obtained by ticking boxes, the boxes should have the same size, shape, and colour. If the “I consent” button is overly eye-catching, it would confuse the data subject and mislead them. Thus, that deceived consent cannot be regarded as clear and unambiguous.¹⁷¹

Other lawful bases for processing data include performance of a contract, compliance with a legal obligation, protection of the vital interests of the data subject or other natural persons, processing by public authorities, and the data controller's or a third party's legitimate interest.¹⁷² Nonetheless, if the data subject is a child, the processing might pose a high risk to the data subject's interests or fundamental rights and freedoms, even if the processing is based on a lawful basis. For this reason, the GDPR requires a Data Protection Impact Assessment (DPIA) where data subjects are vulnerable natural persons, especially children.¹⁷³

¹⁶⁷ Article 29 Working Party, Guidelines on consent under Regulation 2016/679 17/EN WP 259 rev.01, 10 April 2018, 1-31, 11-12.

¹⁶⁸ GDPR, Article 5(1)(a).

¹⁶⁹ GDPR, Article 15.

¹⁷⁰ Article 29 Working Party, Guidelines on consent under Regulation 2016/679 17/EN WP 259 rev.01, 10 April 2018, 1-31, 13-15.

¹⁷¹ Article 29 Working Party, Guidelines on consent under Regulation 2016/679 17/EN WP 259 rev.01, 10 April 2018, 1-31, 15-18.

¹⁷² GDPR, Article 6(1) b)-f).

¹⁷³ GDPR, Article 35 and Recital 75.

Before collecting data, the data controller should determine the legal basis that would be relied on at the time of collection. Other legitimate basis cannot be substituted by the data controller if there is an issue with the data subject's consent, for as if the data subject withdraws his/her consent.¹⁷⁴

3.2 Children and parental consent in the GDPR comparing with the COPPA

According to Article 8 of the GDPR

“[...] in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.”¹⁷⁵

As a result, because children are vulnerable, GDPR necessitates an additional measure of protection. The rationale for this additional protection is indicated in Recital (38), which emphasizes their vulnerability by stating that “[...] they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data [...]”.¹⁷⁶

Hence, there are two conditions that must be met in order to apply Article 8 of the GDPR: first, this provision is “*in relation [only] to the offer of information society services directly to a child*”¹⁷⁷; and second, the processing should be based on consent.¹⁷⁸ Contracts

¹⁷⁴ Article 29 Working Party, Guidelines on consent under Regulation 2016/679 17/EN WP 259 rev.01, 10 April 2018, 1-31, 23.

¹⁷⁵ GDPR, Article 8(1).

¹⁷⁶ GDPR, Recital 38.

¹⁷⁷ GDPR, Article 8(1).

¹⁷⁸ According to Article 4(25) of the GDPR the Information Society Service means a service as defined in point (b) of Article 1(1) of Directive 2015/1535: “[...]any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition: (i) ‘at a distance’ means that the service is provided without the parties being simultaneously present; (ii) ‘by electronic means’ means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (iii) ‘at the individual request of a recipient of services’ means that the service is provided through the transmission of data on individual request. [...]”

and other services concluded or delivered online, such as applications, search engines, social media platforms, online streaming services, online games, news, and educational services, are examples of information society services.¹⁷⁹ Furthermore, the phrase “offered directly to a child” means that Article 8 does not apply to service providers who explicitly state that they are offering their services to adults, unless it is proven otherwise (for example, while the service provider states that it does not provide services for children, its content includes cartoons, toys, and online children games).¹⁸⁰

Whereas COPPA covers commercial websites or online services directed to children under the age of 13 that collect information from children or have actual knowledge that they collect information from children, as well as a website or online service that has actual knowledge that it is collecting personal information directly from users of another website or online service directed to children.¹⁸¹

Thus, the COPPA broadens the definition of “services offered directly to a child” by including the phrase *having actual knowledge* that children's personal information is being gathered. However, having actual knowledge is such a broad concept that it is not specified how the operators might demonstrate their knowledge. However, while considering everyday life occurrences, it should be clear that the social media network operators (e.g., Facebook, Instagram) have actual knowledge that children under the age of 13 have accounts by simply lying about their age. It is clear from their profile photos, activities, and interactions with other users. Even so, their services are not considered to be provided directly to children. Accordingly, we claim that this enhanced definition is not yet fully functional in practice.

The COPPA also requires website and online service operators to obtain parental consent before collecting, using, or disclosing their children's personal information, as GDPR Article 8 does. Furthermore, the COPPA requires operators to make reasonable

Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services OJ L 241, 17.9.2015, p. 1, Article 1(b).

¹⁷⁹ Article 29 Working Party, Guidelines on consent under Regulation 2016/679 17/EN WP 259 rev.01, 10 April 2018, 1-31, 24.

¹⁸⁰ Article 29 Working Party, Guidelines on consent under Regulation 2016/679 17/EN WP 259 rev.01, 10 April 2018, 1-31, 25.; The GDPR does not define a child, but Convention on the Rights of the Child does: “For the purposes of the present Convention, a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier.” Assembly, UN General, Convention on the Rights of the Child, United Nations, Treaty Series 1577, no. 3 (1989), pp. 1-23.

¹⁸¹ 16 CFR Part 312 Children’s Online Privacy Protection Act; Final Rule, 15 U.S.C. §§ 6501–6506, Federal Register Vol. 64, No. 212, 03.11.1999, p. 59888—59915, at part §312.2.

efforts to obtain parental consent, taking into account the available technology. Unlike GDPR Article 8, the COPPA provides some examples of methods for verifying parental consent. These include providing parental consent through e-mail or electronic scan; if there is a monetary transaction using a credit card that provides notification, having a parent phone or video-conference with authorised personnel, and verifying the parent's identification by checking their government-issued ID.¹⁸²

These methods are not exhaustive; there may be more methods developed by the operators and approved by the Federal Trade Commission (FTC) in light of the currently available technology. To employ an alternative method, operators do not need FTC approval. However, some operators desire FTC approval to guarantee that their process complies with the COPPA regulation. For example, the FTC has approved a novel method of asking knowledge-based challenge questions that only the children's parents can correctly answer.¹⁸³ There is also the *email plus* approach, which is solely appropriate for the operators' internal use without disclosing the collected data. These consist of three steps: The operator first requests consent from the parent by e-mail, and the parent responds by giving consent. Finally, the operator confirms that they have received the parental consent, which is the so-called *plus* factor of this method.¹⁸⁴

The COPPA's non-exhaustive methods are appropriate examples of how data controllers might get parental consent in order to comply with the rule. If the methods had been exhaustive, they would have been restricted given how quickly technology advances, and they would have fallen behind the developments. However, it is beneficial that the FTC may constantly update its list by adding new methods, and also that providers of online services have the option of not obtaining FTC approval and still using their own method.¹⁸⁵

As stated above, unlike the COPPA, GDPR does not define any method and instead leaves that solution to data controllers, requiring them to do all reasonable measures to verify the given consent was granted legitimately by those who have parental responsibility, considering the available technology. We suggest that providing some instances for

¹⁸² 16 CFR COPPA 312.5(b)(2).

¹⁸³ FTC, Complying with COPPA: Frequently Asked Questions, QI.4., [Complying with COPPA: Frequently Asked Questions | Federal Trade Commission \(ftc.gov\)](https://www.ftc.gov/business-guidance/privacy-security/verifiable-parental-consent-childrens-online-privacy-rule) (last visited 10 March 2023) and FTC, Verifiable Parental Consent and the Children's Online Privacy Rule, <https://www.ftc.gov/business-guidance/privacy-security/verifiable-parental-consent-childrens-online-privacy-rule> (last visited 10 March 2023).

¹⁸⁴ 16 CFR COPPA 312.5(b)(2)(vi).

¹⁸⁵ FTC, Verifiable Parental Consent and the Children's Online Privacy Rule, <https://www.ftc.gov/business-guidance/privacy-security/verifiable-parental-consent-childrens-online-privacy-rule> (last visited 10 March 2023)

verifying parental consent would be good for both parents and data controllers as guidance. Nonetheless, there is still the possibility to adjust and adopt COPPA's methods in compliance with the EU's legal system. This might pave the path for a useful example of legal transplanting in the digital era.

There are exceptions to prior parental consent under the COPPA. For instance, a one-time response to a child's request could be an example if the operator not using any personal information and immediately deleting the collected information after replying to the request. Another example would be replying to a child's request multiple times (e.g., monthly newsletters), in which case the operator should notify the parents and guarantee that they have the choice to unsubscribe from the website/online service. Moreover, such information may be collected in order to protect children's safety, public safety, or the security or integrity of a website/online service.¹⁸⁶

Whereas the only exception to the necessity of parental consent indicated in GDPR Article 8 is the preventive or counselling services offered directly to children, because they seek to protect the best interests of the child.¹⁸⁷ For example, if a child goes to his/her school's counselling service to discuss problems with his/her classmates and bullying, and the counsellor collects and records the student's personal information for further research and performance to help the student, this processing does not require parental consent. Then again, this exception does not exclude contacting parents in order to gain their cooperation in the best interests of the child.

Comparing the two legislation in terms of these exceptions, we argue that legitimate interests of online services should not be served as an excuse for not obtaining parental consent before processing children's personal data, since Article 6 states that when the data subject is a child, such interests might well be overridden by the children's best interests.¹⁸⁸ However, if a child's vital interests or a public task are involved, processing without parental consent may be lawful, as mentioned in the same article.¹⁸⁹

Furthermore, the COPPA exemption allowing operators to collect children's personal information without parental consent is not an exception under the GDPR. To avoid any

¹⁸⁶ For more information about the exceptions see: 16 CFR 312.5(c).

¹⁸⁷ GDPR, Recital (38).

¹⁸⁸ GDPR, Article 6(1)(f).

¹⁸⁹ GDPR, Article 6(1)(d) and (e).

confusion, it is important to note that GDPR Article 8 does not use the term collection as COPPA does.¹⁹⁰ COPPA defines the collection as:

“[t]he gathering of any personal information from a child by any means, including but not limited to:

- (1) Requesting, prompting, or encouraging a child to submit personal information online;
- (2) Enabling a child to make personal information publicly available in identifiable form;
- (3) Passive tracking of a child online.”

Therefore, *collection* under the COPPA is similar to the concept of *processing* under the GDPR, since processing also involves the collection of personal information.¹⁹¹ Yet, one may argue that processing is more comprehensive than collection. Since, for example, processing includes the deletion or restriction of data, but collection under COPPA does not cover deletion if the operator takes reasonable measures to delete them prior to their public availability.¹⁹²

The COPPA does not include the preventive or counselling service exception, as the GDPR does, and the reason for this would be that the legislators did not consider the importance of these services, or the legislators assumed that these services could not behave in the best interests of the children more than parents do. However, in some cases, qualified counsellors may be more knowledgeable about pedagogy, digital literacy, and privacy education than average-educated parents. For example, with the increasing use of social media networks, parents now have more opportunities to share their children's intimate moments in public, and they typically do not obtain their children's approval before revealing their privacy. Most of cases it is because of these parents' lack of education and risk-analysis abilities. According to a survey, teens find their parents' sharing embarrassing and useless.¹⁹³ Consequently, parental sharing might result in (cyber)bullying among the teens' classmates.

¹⁹⁰ Instead GDPR uses the term “processing” and it is defined under the Article 4(2) as “[a]ny operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.”

¹⁹¹ GDPR, Article 4(2). “‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.”

¹⁹² 16 CFR COPPA 312.2(2).

¹⁹³ Karen Verswijvel, Michel Walrave, Kris Hardies, Wannes Heirman: Sharenting, is it a good or a bad thing? Understanding how adolescents think and feel about sharenting on social network sites. Children and youth services review 104 (2019) 104401, 7.

Therefore, we assert that it would be beneficial for children if the COPPA contained an exception for obtaining prior parental consent when offering preventative or counselling services directly to children. Because there could be occasions in which children report their parents' inappropriate behaviour towards them to school counselling services. Thus, this exception would allow children to express themselves and seek assistance from school counsellors/teachers.

In this chapter, we analysed the concept of parental consent, the methods for verifying parental consent prior to processing, and the exceptions to this verification, comparing the GDPR and the COPPA. In the next chapter, we will analyse the threshold age at which parental consent must be obtained in accordance with the GDPR and COPPA. We will analyse the relevance of the concept of a threshold age and whether or not it is necessary for protecting the personal data and privacy of children.

3.3 Threshold age for parental consent under the GDPR and the COPPA

According to COPPA, a child is defined as an individual under the age of 13.¹⁹⁴ Because, according to the FTC, children under the age of 13 are more vulnerable to the hazards and consequences of their online behaviours and interactions.¹⁹⁵ But who can argue that a twelve-year-old child is vulnerable, but a thirteen-year-old child is not? In everyday life, twelve and thirteen-year-old children frequently have similar abilities.¹⁹⁶

Moreover, would not it be better if the rule cover at least the adolescent years of the children? Senator *Edward Markey* of the US revealed that in his initial draft. He classified a child as anyone under the age of sixteen, but they changed it to thirteen for some economic reasons. Some e-commerce companies did not want to lose this attractive adolescent market. He now admits that the thirteen-year-old age threshold was too low, but he claims that it was the best he could do, because not only e-commerce companies, but also civil liberties groups, were opposed to the sixteen-year-old age threshold.¹⁹⁷

¹⁹⁴ 16 CFR COPPA 312.2 “Child: means an individual under the age of 13.”

¹⁹⁵ Complying with COPPA: Frequently Asked Questions, Why does COPPA apply only to children under 13? What about protecting the online privacy of teens? <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions> (last visited 10 March 2023)

¹⁹⁶ Virginia A. M. Talley, Major Flaws in Minor Laws: Improving Data Privacy Rights and Protections for Children under the GDPR, 30 Ind. Int'l & Comp. L. Rev. 127 (2019), 145.

¹⁹⁷ The Wall Street Journal, Julie Jargon, How 13 Became the Internet's Age of Adulthood? (18 June 2019), <https://www.wsj.com/articles/how-13-became-the-internets-age-of-adulthood-11560850201> (last visited 10 March 2023).

However, for similar economic reasons, the EU has followed in the footsteps of the US and implemented a remarkably similar age threshold with its partial legal transplanting. We suggest it is partly because, while the EU raised the age to 16 in order to protect teenagers, it also allows the Member States to lower it till the age of 13. Furthermore, the age of 13 was chosen as the standard age based on the COPPA since it would otherwise be a burden on websites and online service providers, as stated directly by the European Council.¹⁹⁸ According to this reasoning, we claim that economic considerations appear to be more important than adolescents' online data protection and privacy.

The table below compares the ages of consent of the Member States in different scenarios: accessing the realm of digital platforms, entering the labour market and receiving medical care, including diagnosis and surgery, engaging in sexual activities with others lawfully.

	Digital platforms ¹⁹⁹	Part-time work ²⁰⁰	Medical treatments ²⁰¹	Sexual activity ²⁰²

¹⁹⁸ European Commission, Commission Staff Working Paper, Impact Assessment, Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, SEC (2012) 72 final, p. 68, https://www.europarl.europa.eu/cmsdata/59702/att_20130508ATT65856-1873079025799224642.pdf (last visited 20 February 2023). For more information regarding the mentioned legal transplantation: Asli Alkis Tümtürk: The Threshold Age for Children's Online Consent in Light of the Watson/Legrand Debate: Is Legal Transplant Possible in the Digital Era?, *The Journal of Comparative Law* vol. 17/1 (2022), 243.

¹⁹⁹ EuConsent, Digital Age of Consent under the GDPR, <https://euconsent.eu/digital-age-of-consent-under-the-gdpr/#:~:text=As%20per%20Article%208%20of,at%20least%2016%20years%20old>. (last visited 10 March 2023).

²⁰⁰ FRA (European Union Agency for Fundamental Rights), Minimum age requirements related to rights of the child in the EU, Social rights; Employment; Education; Alternative care; LGBTI and Mobility, https://fra.europa.eu/en/publications-and-resources/data-and-maps/minag?dataSource=MINAG_en_62756&media=png&width=740&topic=group05&question=MINAG_HE01&plot=MAP&subset=NONE&subsetValue=NONE&answer=MINAG_HE01&year=2017 (last visited 10 March 2023).

²⁰¹ FRA, Consenting to medical treatment without parental consent, <https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements-concerning-rights-child-eu/consenting-medical-treatment-without-parental-consent#:~:text=However%2C%20where%20a%20medical%20intervention,is%20set%20at%2015%20years>. (last visited 10 March 2023).

²⁰² FRA, Minimum age requirements related to rights of the child in the EU, Marriage and sexual consent; Citizenship; Political Participation; Religion; Health, https://fra.europa.eu/en/publications-and-resources/data-and-maps/minag?dataSource=MINAG_en_62756&media=png&width=740&topic=group05&question=MINAG_HE01&plot=MAP&subset=NONE&subsetValue=NONE&answer=MINAG_HE01&year=2017 (last visited 10 March 2023).

Austria	14	15	Depends on maturity	14
Belgium	13	15	Depends on maturity	16
Bulgaria	14	15	18	14
Croatia	16	15	16	15
Cyprus	14	14	18	17
Czech Republic	15	15	Depends on maturity	15
Denmark	13	13	15	15
Estonia	13	13	Depends on maturity	14
Finland	13	14	18	16
France	15	14	18	15
Germany	16	15	Depends on maturity	14
Greece	15	15	18	15
Hungary	16	16	18	14
Ireland	16	14	16	17
Italy	14	16	18	14
Latvia	13	13	14	16

Lithuania	14	14	16	16
Luxembourg	16	15	Depends on maturity	16
Malta	13	16	18	18
Netherlands	16	13	16	16
Poland	16	16	16	15
Portugal	13	16	16	14
Romania	16	16	18	15
Slovakia	16	15	18	15
Slovenia	15	15	15	15
Spain	14	16	16	16
Sweden	13	13	Depends on maturity	15

Table 1: Age of consent in the Member States²⁰³

As seen in the table, the highest ages of consent thresholds are found in areas where children receive medical care. Getting a diagnosis or having surgery without parental consent is legal in ten of the EU Member States at the age of 18, and it is legal in seven of them depending on the child's maturity. The child maturity test indicates that doctors should make decisions on a case-by-case basis. This maturity test would not be achievable in the digital

²⁰³ This table created by the author using the abovementioned sources.

world, because even if some questions were asked to assess the children's maturity, such questions may be passed by coincidence.

Because according to Article 9 of the GDPR, health data falls into the special categories of personal data,²⁰⁴ it is reasonable to set higher thresholds for this. In the GDPR's Preamble, it is stated that processing personal data which are sensitive by their nature poses a high risk to the fundamental rights and freedoms of individuals.²⁰⁵ Therefore, they require specific protection and the Article 9 prohibits processing data with sensitive nature (e.g., health data) unless one of these conditions is met²⁰⁶: data subject provides explicit consent; data subject's data with sensitive nature is processed in the context of employment, social security and social protection (on the basis of law); vital interests of data subject is in place; processing is necessary for the legitimate activities of non-profit bodies; the data is made public by the data subject ; processing is necessary for the establishment of legal claims or judicial acts; processing is necessary for reasons of public interest (on the basis of law); processing is necessary for the purposes of health or social care (on the basis of law); processing is necessary for reasons of public health (on the basis of law); or processing is necessary for archiving, research and statistics purposes (on the basis of law).

Nevertheless, internet service providers profit from the processing of individuals' personal data; even if the personal data falls under the special categories,²⁰⁷ they choose to share it with interested organizations (such as advertising companies). The MyFitnessPal app, for example, indicates in its privacy policy that they process users' personal data for “internet-based and cross-app, cross-device advertising.” In terms of data with sensitive nature , users can choose not to provide them; however, in this case, they will be unable to access some of the services and features, meaning that the app would not function properly.²⁰⁸ Individuals under the age of eighteen are not permitted to register for the MyFitnessPal app; however, there are several health-related applications that enable children to register.

For example, the Happify that promises to improve well-being of users, measure their emotional happiness, and reduce their stress and anxiety levels. It allows children aged 16

²⁰⁴ GDPR, Article 9(1).

²⁰⁵ GDPR, Recital 51.

²⁰⁶ GDPR, Article 9(2) (a-j).

²⁰⁷ For more detailed information regarding the potential legal basis for processing of health data: Szilvia Váradi: Legal challenges of processing health data in the shadow of COVID-19 in the European Union, Forum: Acta Juridica Et Politica, Vol. 11. No. 4 (2021), 358-362.

²⁰⁸ MyFitnessPal Privacy Policy, <https://www.myfitnesspal.com/privacy-policy> (last visited 10 March 2023).

and older to register their app. They also state that they give opt-in or opt-out options for data with sensitive nature before sharing it with third parties.²⁰⁹ A 16-year-old child, though, may not be mature enough to understand the consequences of sharing sensitive information with third parties. Doctors, however, should keep their patients' personal information and diagnoses private, unlike internet service providers.²¹⁰

Interestingly, a 16-year-old child in Hungary, for example, cannot go to a doctor on his/her own, but he/she may download a health-related app (e.g., Happify) on his/her phone that collects and processes data with sensitive nature and might even share this data for profit. Even though, considering the risks associated with both options, the first scenario should be considerably more secure and confidential, given that doctors must adhere to the physician-patient privilege.

When it comes to another sensitive area of children's data, their sexual lives, the age of consent ranges between 14 to 16 in the Member States. So, the threshold ages are not as high as the medical treatments, and oddly, the maturity test for the age of consent for children's sexual activity is not required. Furthermore, some nations allow children to participate in sexual behaviours before they may engage in internet activities. For example, a 14-year-old child in Hungary or Germany can have sexual intercourse, but he or she cannot create a social media account without the consent of his or her parents.

On the one hand, there are these sensitive areas in individuals' lives, and on the other, there is the labour market, which people may participate in once they reach maturity. The legal age of consent for children to enter the labour market part-time may also be found in the table above, and the ages are quite similar among the Member States, ranging from 13 to 16. However, it might still be perplexing for a child at the age of 13, for example, in the Netherlands, where he or she can choose to work part-time after school and earn his or her own money but cannot obtain an e-mail account without the consent of his or her parents.

These differing consent ages for different matters do not appear to be well-reasoned or consistent. Thereby, this might cause confusion for a child's abilities between the physical

²⁰⁹ Happify, Legal, Happify™ Privacy Policy: Last Updated in July 2020, <https://www.happify.com/public/legal/#legal> (last visited 10 March 2023).

²¹⁰ European Council of Medical Orders, Principles of European medical ethics, Article 7. "The doctor is the patient's necessary confidant. He or she must guarantee the complete secrecy of all the information he or she has collected and the findings made during his or her contact with the patient. The patient's death does not exempt the doctor from medical confidentiality. The doctor must respect the patient's privacy and take all necessary measures to render impossible the disclosure of all the information he or she has acquired while exercising his or her profession. If exceptions to medical confidentiality are provided for by national law, the doctor may ask for the prior opinion of his association or the professional body of similar competence." <http://www.ceom-ecmo.eu/en/view/principles-of-european-medical-ethics> (last visited 10 March 2023).

world and the online realm. A child may easily assume that lying about his/her age is the best option to avoid these online restrictions that he/she does not have in real life or has less of in comparison to his/her online activities.

Furthermore, in most situations, the age verification process to register for an app or enter a website is too simple since the applications or websites merely ask children to type their ages themselves. For example, the MyFitnessPal app stated above just needs a child to input their age/birth date before proceeding with the registration procedure, and then they can create an account with the help of their e-mail address.²¹¹ It is also very simple for a child to get a Gmail account, because Google simply requires inputting your birth date as well and all a child should do is type an age that is acceptable in their country to open a Gmail account.²¹² This method makes it very easy for a child to lie. This issue will be covered in-depth in the next chapter.

Parents of an older child are more likely to say child uses social media sites

% of U.S. parents of a child age 11 or younger who say that, as far as they know, their child uses ...

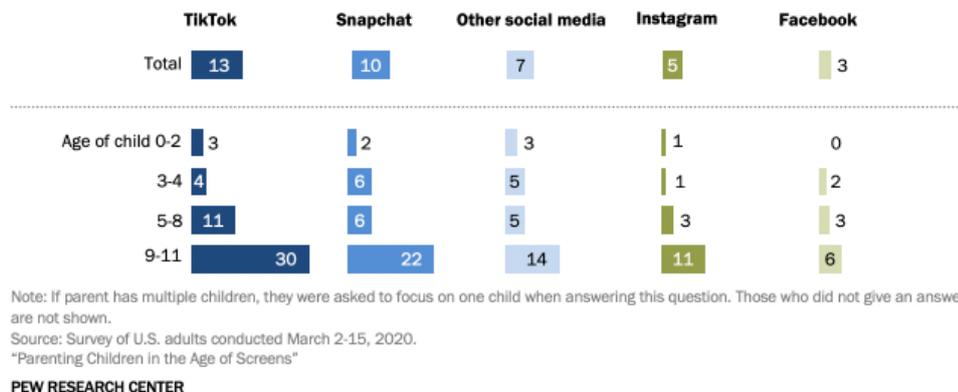


Chart 1: Children using social media sites by ages²¹³

²¹¹ MyFitnessPal, Sign Up, <https://www.myfitnesspal.com/account/create> (last visited 10 March 2023).

²¹² Google, Sign Up, <https://accounts.google.com/signup/v2/webcreateaccount?flowName=GlifWebSignIn&flowEntry=SignUp> (last visited 10 March 2023).

²¹³ Source: Brooke Auxier, Monica Anderson, Andrew Perrin and Erica Turner, Children’s engagement with digital devices, screen time, Pew Research Center, (2020), 2. <https://www.pewresearch.org/internet/2020/07/28/childrens-engagement-with-digital-devices-screen-time/> (last visited 10 March 2023).

Majority of parents think it is unacceptable for children to begin using social media before age 12

% of U.S. parents who say it is **acceptable** for children to begin ___ at age ...

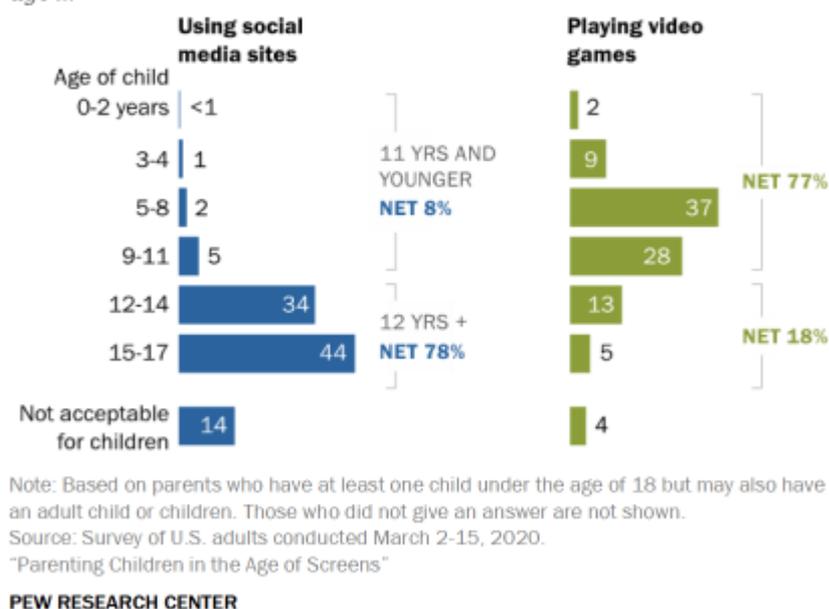


Chart 2: Appropriate ages for children to begin using social media sites and playing video games according to the parents²¹⁴

Considering children under the age of 13 (or in some jurisdictions up to 16) cannot legally register for certain social media networks (e.g., Facebook²¹⁵, Instagram²¹⁶), they appear to be lying about their ages in order to register for those platforms, as seen above in the Pew Research Center's 2020 surveys conducted in the US. The ages of children who access social networking sites are decreasing till they are less than two years old. Among the younger children, those aged 9 to 11 had the highest rate. It appears that some parents in the US are still allowing their children to have social media accounts even though the vast majority of them agree that children under the age of 12 should avoid using such sites due to the risks they pose (including exposure to sexual content, violent content, cyberbullying, and harassment).

²¹⁴ Brooke Auxier, Monica Anderson, Andrew Perrin and Erica Turner, Children's engagement with digital devices, screen time, Pew Research Center, (2020). 4.
<https://www.pewresearch.org/internet/2020/07/28/childrens-engagement-with-digital-devices-screen-time/> (last visited 10 March 2023).

²¹⁵ Facebook Help Center, How to Report Things, How do I report a child under the age of 13 on Facebook?, https://www.facebook.com/help/157793540954833/?helpref=uf_share (last visited 10 March 2023).

²¹⁶ Instagram Help Center, How to Report Things, How do I report a child under the age of 13 on Instagram?, https://help.instagram.com/2922067214679225/?helpref=hc_fnav (last visited 10 March 2023).

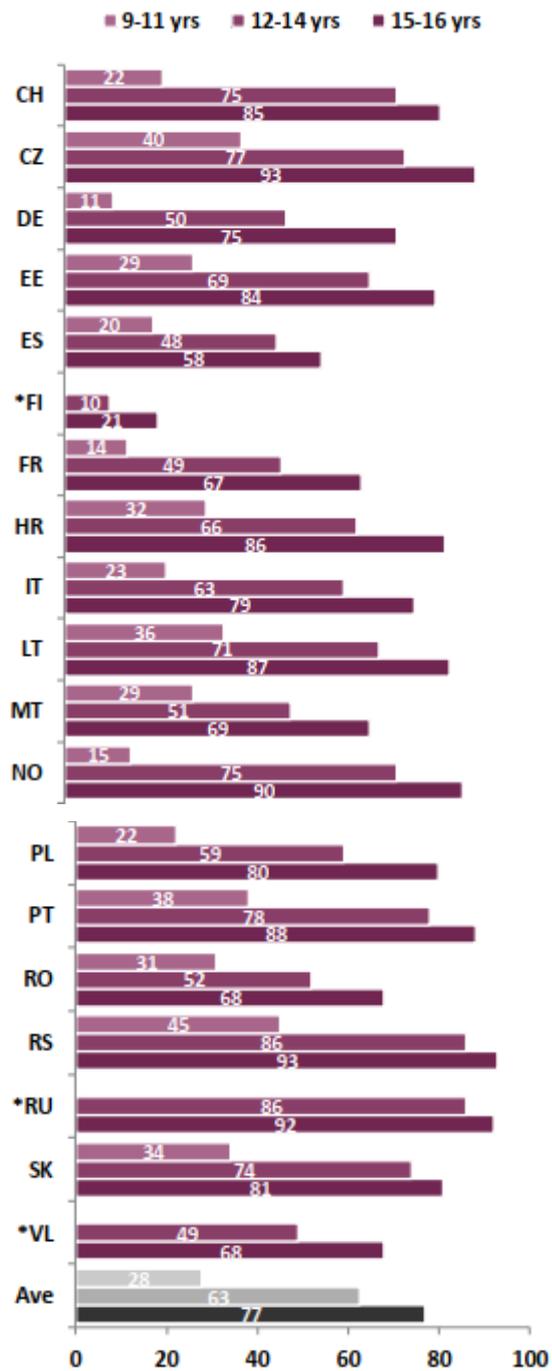


Chart 3: Visiting social media networks daily²¹⁷

²¹⁷ David Smahel, Hana Machackova, Giovanna Mascheroni, Lenka Dedkova, Elisabeth Staksrud, Kjartan Ólafsson, Sonia Livingstone, and Uwe Hasebrink: EU Kids Online 2020: Survey results from 19 countries (2020), EU Kids Online, 30.

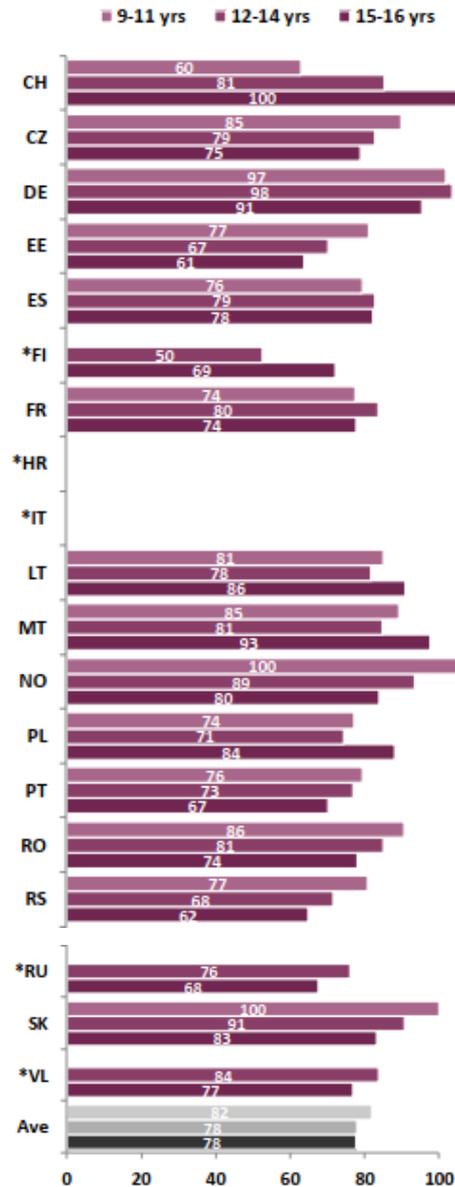


Chart 4: Harm from online victimisation (at least a bit upset)²¹⁸

As observed in the above surveys conducted in EU countries, and similar to the findings obtained in the US, children who use social media networks include not only legally permitted children but also children who are “under-age.”

We advocate that considering Table 1 above, the varying digital ages of consent in different European countries have no significant effect on children's access to social media

²¹⁸ David Smahel, Hana Machackova, Giovanna Mascheroni, Lenka Dedkova, Elisabeth Staksrud, Kjartan Ólafsson, Sonia Livingstone, and Uwe Hasebrink, EU Kids Online 2020: Survey results from 19 countries (2020), EU Kids Online, 58.

networks. According to a research (2019) conducted by Better Internet for Kids (BIK)²¹⁹ about children's age of consent for data processing across the Europe, the selected countries' justifications for decreasing/increasing the online age of consent (as permitted by the GDPR) are often based on two factors: First, those that do not lower the age of consent online argue that they do so for the safety of children.²²⁰ Second, those who reduce the internet age of consent (to as low as 13) justify their actions by claiming that they respect children's right to freedom of speech and press.²²¹

Yet, based on the above instances shown by the Chart 3 and 4, we may conclude that raising the legal age of consent does not give further protection and that decreasing it has no direct influence on children's online behaviour. According to mentioned report of BIK, Spain asserted that age-based restrictions on access to the Internet and its services might reduce the changes of the children to have sufficient Internet skills and cope with the difficulties of the digital life. Hence, Spain's data protection legislation sets the age of consent for the processing of a child's personal information at 14.²²² Nonetheless, based on the data shown in Chart 3 above, daily visits to social media networks by children aged 9 to 16 in Spain are below average. It seems that decreasing the age requirement has no immediate effect on children's motivation to participate in online activities.

²¹⁹ Ingrida Milkaite and Eva Lievens: The GDPR child's age of consent for data processing across the EU—one year later (July 2019), Better Internet for Kids (2019), 1-7.

²²⁰ See these examples: “[i]n the end of April 2018, news emerged suggesting that the main opposition parties in Ireland are trying to raise the age of digital consent for children to 16 years in an attempt to strengthen children's online safety. Politicians stated that they are planning to prepare “an amendment to the Data Protection Bill at committee stage in order to amend the age of digital consent from 13 to 16 years”. Their reasoning is related to stronger protection of children's data, especially in the context of profiling and commercial targeting and decisions taken by other European countries, such as the Netherlands and Germany.” in Ingrida Milkaite and Eva Lievens: The GDPR child's age of consent for data processing across the EU—one year later (July 2019), Better Internet for Kids (2019), 4. and “The Explanatory Statement accompanying the Draft Law (Dôvodová Správa) explains that children deserve special protection of their personal data as they are less aware of the risks and consequences associated with the processing of their personal data, especially when their data is obtained through a publicly accessible internet network.” in Ingrida Milkaite and Eva Lievens: The GDPR child's age of consent for data processing across the EU—one year later (July 2019), Better Internet for Kids (2019), 5-6.

²²¹ See the examples: “Section 13.4.2 [of the draft of which was initially proposed by the Norwegian Ministry of Justice and Public security] provides the insights by different consultation bodies, some of them arguing that setting the age of consent at 13 would not protect children enough, while other bodies stressed the need for respect for the child's right to self-determination, child's right to information and freedom of expression.” in The GDPR child's age of consent for data processing across the EU—one year later (July 2019), Better Internet for Kids (2019), 6. and “On 13 June 2018 the draft law was withdrawn due to the discussion surrounding the provisions which could possibly restrict the freedom of the press.” in The GDPR child's age of consent for data processing across the EU—one year later (July 2019), Better Internet for Kids (2019), 3.

²²² The GDPR child's age of consent for data processing across the EU—one year later (July 2019), Better Internet for Kids (2019), 5.

In Spain, where the threshold age for parental consent is 14, children use social media networks at a lower rate than in Germany, where the threshold age is 16. Additionally, according to Chart 4 above, children aged 9 to 16 in Germany experience higher online victimisation than children in Spain. Furthermore, if we compare Finland (where the threshold age for parental consent is 13) and Norway examples (where the threshold age for parental consent is 16), we can observe that Finland has the lowest rates, while Norway has one of the highest rates of online victimisation, particularly among children aged 9 to 11. These findings suggest that variances in the digital age of consent have no direct effect on use or online safety in practise.

Another noteworthy observation is that the age of children who claim to be harmed by online victimization is unrelated to their age. In other words, encountering harm is not exactly proportional to the age of children. In Switzerland, for example, children aged 15 to 16 were the most affected by online victimization as compared to younger children. However, as observed in the Slovak Republic, the youngest children, aged 9 to 11, are the most harmed.²²³

In order to make comparative conclusions about the age of digital consent, some Member States, according to the findings of the same report of BIK, referred to various legal disciplines and articles in their draft laws on personal data protection. For instance, explanatory part of the Draft Law of the Slovenian Personal Data Protection Act asserts that the age of 15 was chosen in accordance with the Slovenian Family Law Code, which allows a 15-year-old child to take legal action alone.²²⁴ Similarly, as shown in Table 1 above, the minimum age for beginning part-time employment, receiving medical care, or engaging in sexual activity is 15 in Slovenia.

A similar example is provided by the Polish draft law on the protection of personal data, which explains that the age of 13 was selected due to the similar age threshold provided by the Polish Civil Code, which states that a person who has reached the age of 13 has limited legal capacity and can therefore enter into "minor contracts of daily life." Nevertheless,

²²³ David Smahel, Hana Machackova, Giovanna Mascheroni, Lenka Dedkova, Elisabeth Staksrud, Kjartan Ólafsson, Sonia Livingstone, and Uwe Hasebrink, *EU Kids Online 2020: Survey results from 19 countries* (2020), *EU Kids Online*, 132.

²²⁴ "The explanatory part of the Draft Law makes a reference (on page 90) to the US COPPA and specifies that the age of 15 was chosen with regard to the systematic guidance of the Slovenian Family Code, according to which a 15-year-old child can take legal action on his or her own, unless the law provides otherwise." Ingrida Milkaite and Eva Lievens: *The GDPR child's age of consent for data processing across the EU—one year later* (July 2019), *Better Internet for Kids* (2019), 5.

unlike the draft law, the final law does not mention children and the age was set at 16 years.²²⁵

Another interesting example stated by the Czech Republic in their explanatory note on the draft law (*Důvodová Správa*) is that teens may get driving licences (types of motorcycles) at the age of 15, despite the riskier and more difficult nature of these vehicles. Hence, this note claims that it may be improper to restrict email services, social networks, and other comparable forms of online communication. It is recommended that education should be used to address the risks of online activities. Ergo, the age of 15 was chosen as the digital consent age.²²⁶ In the Czech Republic, the minimum age for beginning a part-time work or engaging in sexual behaviour is similarly 15, as shown in Table 1 above.

The practice of comparing the age of digital consent to that of other law fields is, in our view, appropriate. It clarifies the legislative intention and gives relative consistency, as shown by Slovenia and the Czech Republic. Hence, we may suggest that all Member States adopt a uniform age of digital consent and provide appropriate justifications for their choice. A uniform age threshold for digital consent online would offer clarity, consistency, and simplicity of compliance inside the EU for both individuals and companies. They may utilise the comparative method to determine the age threshold considering European legal culture and customs. Establishing a uniform age is crucial for transferring data not only to third countries but also inside the Union. This topic will be discussed in depth in Chapter 6.

Moreover, setting age restrictions, we believe, can direct and guide parents, but in the digital era and with growing technology, it appears hard to keep children away from these

²²⁵ “An introduction to the draft law on the protection of personal data which is published together with the draft law, explains that the age of 13 was chosen due to similar age threshold provided by the Polish Civil Code (article 15) which states that a person who has reached the age of 13 has limited legal capacity and can therefore conclude ‘minor contracts of daily life’. In this context, the document explains that it is also justified to accept the age of 13 for the effective expression of consent by the child for the processing of personal data relating to him or her as there is no reason to assume that a person who can manage his or her earnings and conclude minor contracts is not entitled to consent to the processing of his or her personal data in accordance with the provisions of the GDPR also bearing in mind that consent may be withdrawn at any time.” Ingrida Milkaite and Eva Lievens: *The GDPR child's age of consent for data processing across the EU—one year later* (July 2019), *Better Internet for Kids* (2019), 5.

²²⁶ “The Czech law regarding driving licences is provided as an example which concerns teenagers of 15, 16 or 17 years. It is stated that driving a motor vehicle is an activity that the driver typically carries out independently and personally, which cannot be interfered with, and which is more difficult and risky in nature. Crucially, the document also explains that the reality of minors commonly using mobile phones and sending text messages should not be ignored. Therefore, limiting, for example, email services, social networks, or similar methods of communication, may be inappropriate. According to the document, a better way of addressing the risks associated with the use of information and communication technologies by children may be education and regular interest of educated parents.” Ingrida Milkaite and Eva Lievens: *The GDPR child's age of consent for data processing across the EU—one year later* (July 2019), *Better Internet for Kids* (2019), 2.

digital platforms. Furthermore, there are certain advantages to participating in online activities such as online libraries, opportunity to learn different cultures and languages, instructive documentaries, and brain-boosting games. As previously indicated, the countries participated in BIK's research also emphasised the significance of children using the Internet to enhance their digital skills and exercise their right to information²²⁷ and freedom of expression.²²⁸

On one hand, parents cannot and should not keep their children away from these beneficial internet activities. On the other hand, according to the GDPR and the COPPA, parents have the responsibility to protect their children's privacy and online safety.²²⁹ We suggest that policymakers should review whether imposing age limits is useful or whether there would be other solutions.²³⁰

An alternative and optimal method would be to achieve a good balance with the aid of digital education and literacy. Other alternatives would include the combination of parental supervision with the use of a software solution that limits inappropriate content and websites²³¹ and ethical design principles of online platforms with more child-friendly content that considers the online needs of children.

However, currently, we should implement legal age restrictions on the Internet since these are the existing reality of the GDPR and the COPPA. In the next chapter, we will examine age-verification solutions that are designed to comply with the legal age of consent for using digital platforms.

²²⁷ Article 17 of the UNCRC guarantees the right to information of children.

UN Commission on Human Rights, Convention on the Rights of the Child, E/CN.4/RES/1990/74, 07.03.1990, Article 17.

²²⁸ Article 13 of the UNCRC protects the right of children to freedom of expression.

UN Commission on Human Rights, Convention on the Rights of the Child, E/CN.4/RES/1990/74, 07.03.1990, Article 13.

²²⁹ GDPR, Article 8 and 16 CFR COPPA 312.5.

²³⁰ David Smahel, Hana Machackova, Giovanna Mascheroni, Lenka Dedkova, Elisabeth Staksrud, Kjartan Ólafsson, Sonia Livingstone, and Uwe Hasebrink, *EU Kids Online 2020: Survey results from 19 countries* (2020), *EU Kids Online*, 132.

²³¹ For more information regarding the software solutions for parental control: Asli Alkis, *Investigating the usefulness of online age verification methods*, *Studia Iurisprudentiae Doctorandorum Miskolciensium*, (2021) vol.1, 17.

3.4 Online age verification methods

According to the COPPA and GDPR, as indicated above, parents are primarily responsible for their children's safety. However, in the natural course of events, parents cannot be expected to constantly monitor and supervise their children. Thus, attempts are being undertaken to develop internet tools that would make it simpler to monitor children when the parents are physically absent.²³²

Thereby, age verification has the potential to be a beneficial method for making the Internet safer for children. The goal of age verification systems is to impose a technological instrument that checks if the internet user is of legal age to access age-restricted content.²³³ However, online age verification systems may present significant challenges and concerns that policymakers, data controllers, and parents should be aware of and work to address in order to improve them. It is important to remember that there is no such thing as a flawless age verification mechanism. The assumption that the age verification method would keep children safe from any harmful content may cause a false feeling of security.²³⁴

When it comes to existing age verification methods, none of them are perfect but there are some features that make some of them preferred. First, there is the self-verification method, which is the most often employed by websites and applications and is based on the internet user writing their birth date (e.g., Facebook)²³⁵ or clicking a yes or no box (e.g., mralkohol.hu)²³⁶ as proof that they are of legal age. That is extremely affordable and simple to require for the operators; yet it is very easy for a child to lie in order to gain access to or create an account for certain websites, applications, or social media networks.²³⁷

The second method is the peer-based verification, which is based on the peers' ratings of internet users who intend to attend a website. However, these ratings should be based on offline interactions with these Internet users, rather than their online profiles. This strategy can be effective in social media networks since it is simple to rate peers based on their profile

²³² Asli Alkis, Investigating the usefulness of online age verification methods, *Studia Iurisprudentiae Doctorandorum Miskolciensium*, (2021) vol.1, 8.

²³³ Van der Maelen, Carl, *The Coming-of-Age of Technology: Using Emerging Tech for Online Age Verifications*, *Delphi 2* (2019), 115.

²³⁴ Thierer, Adam D., *Social networking and age verification: Many hard questions; no easy solutions*, *Progress & Freedom Foundation Progress on Point Paper 14.5* (2007), 3.

²³⁵ Facebook, Sign Up: <https://www.facebook.com/signup> (last visited 10 March 2023).

²³⁶ Mr.Alkohol (Coctails&Drinks): <https://mralkohol.hu/> (last visited 10 March 2023).

²³⁷ Jules Polonetsky: *Online Age Verification for Our Children A Report on the Tools and Resources Available for Safeguarding the First Generation of Digital Natives*. 31st International Conference of Data Protection and Privacy Commissioners in Madrid, Future of Privacy Forum, (2009), 3-4.

pictures and it is also cost-effective for operators. However, there is the potential of creating fake accounts and verifying them with each other, which may render the verification technique ineffective. This method is relatively more reliable than self-verification, although there is still the possibility of fraud without much effort.²³⁸

Third, there is the use of a credit card, debit card, or other online payment systems as an age verification method.²³⁹ Moreover, under the COPPA, this is also a verification system for obtaining parental consent, but it is only allowed in connection with a monetary transaction.²⁴⁰ We agree that this should be the case, because providing credit card information for other purposes, such as creating a social network account is not reasonable. Besides, children may also have bank accounts and as a result, distinguishing a child from an adult could be difficult.²⁴¹ Even if it is feasible to detect that it is a child bank account, the question remains as to how we can determine the precise age from the bank account or credit card number.

Moreover, some children steal or borrow credit cards from their parents and use them online without their parents' knowledge.²⁴² Furthermore, while not all adults or children use credit or debit cards, requiring them and assuming that everyone has or should have one might be discriminatory to those who do not prefer to use credit cards or cannot afford them at all.²⁴³ Even if they have one, some people may be reluctant to provide their credit card information due to some reasonable security concerns.

Fourth, providing personal IDs such as a passport or driver's license might be an option for age verification, and it would be relatively easy to distinguish a child from an adult. However, this could lead to plenty of privacy issues because, on the Internet today, if you

²³⁸ Jules Polonetsky, Online Age Verification for Our Children A Report on the Tools and Resources Available for Safeguarding the First Generation of Digital Natives. 31st International Conference of Data Protection and Privacy Commissioners in Madrid, Future of Privacy Forum, (2009), 4.

²³⁹ Jules Polonetsky, Online Age Verification for Our Children A Report on the Tools and Resources Available for Safeguarding the First Generation of Digital Natives. 31st International Conference of Data Protection and Privacy Commissioners in Madrid, Future of Privacy Forum, (2009), 5.

²⁴⁰ 16 CFR COPPA 312.5(b)(2)(ii).

²⁴¹ Children may also have bank accounts with the consent of their parents or guardians. For instance: HSBC, Children's Bank Accounts, <https://www.hsbc.co.uk/current-accounts/products/children/> (last visited 10 March 2023).

²⁴² The Guardian, Boy, 12, Steals Credit Card and Goes on Bali Holiday after Fight with Mother (23 April 2018) <https://www.theguardian.com/australia-news/2018/apr/23/boy-12-steals-credit-card-and-goes-on-bali-holiday-after-fight-with-mother> (last visited 10 March 2023) cited in Carl Van der Maelen, The Coming-of-Age of Technology: Using Emerging Tech for Online Age Verifications, Delphi - Interdisciplinary Review of Emerging Technologies, vol. 2, no. 3, 2019, p.117.

²⁴³ Carl Van der Maelen, The Coming-of-Age of Technology: Using Emerging Tech for Online Age Verifications, Delphi - Interdisciplinary Review of Emerging Technologies, vol. 2, no. 3, 2019, p.117-118.

share a piece of information, it could be shared with untrustworthy third parties in a fraction of a second, either voluntarily because the parties have some economic interest in doing so or through malicious cyber-attacks. It might be reliable as an age verification tool, but it could easily go beyond its purpose and generate some data protection difficulties. As a result, personal IDs should not be used unless there are very secure and trustworthy government websites such as systems that enable access to public services from a single website (e.g., Ügyfélkapu²⁴⁴ in Hungary).²⁴⁵

Fifth, as previously stated, there is a knowledge-based authentication method for verifying parental consent that has been approved by the FTC. It can, in fact, be used as an age verification method since it can distinguish between children and adults. Nevertheless, some of the EU Member States, including Hungary, require data controllers to get parental consent if the children are under the age of 16. In this case, a 16-year-old child and an 18-year-old adult cannot always be distinguished by knowledge-based questions since 16-year-olds often have the similar levels of maturity as 17/18-year-olds.²⁴⁶

Sixth, fingerprints, bone density, characteristic markings on the surface of the eye, or other biologically unique identifiers may now be used to determine the age of users. There are not just physical biometrics, but also behavioural biometrics that may be used to determine a user's age, such as typing style.²⁴⁷ Biometric data, however, is classified as sensitive information about an individual under the GDPR, and “...the processing of genetic data, biometric data for the aim of uniquely identifying a natural person...”²⁴⁸ is prohibited. This means that biometric data cannot be used for any purpose if there is no explicit consent or other legal bases (e.g., “processing is necessary to protect the vital interests of the data subject or another natural person”²⁴⁹). Therefore, data controllers should ensure that their data policy explains the risks and consequences of collecting and processing biometric data clearly, and they should get the explicit consent of underage children's parents for lawfully processing their biometric data.

²⁴⁴ Ügyfélkapu, <https://ugyfelkapu.gov.hu/>, (last visited 10 March 2023).

²⁴⁵ Jules Polonetsky, Online Age Verification for Our Children A Report on the Tools and Resources Available for Safeguarding the First Generation of Digital Natives. 31st International Conference of Data Protection and Privacy Commissioners in Madrid, Future of Privacy Forum, (2009), 7.

²⁴⁶ Carl Van der Maelen, The Coming-of-Age of Technology: Using Emerging Tech for Online Age Verifications, Delphi - Interdisciplinary Review of Emerging Technologies, vol. 2, no. 3, 2019, p.119-120.

²⁴⁷ Jules Polonetsky: Online Age Verification for Our Children A Report on the Tools and Resources Available for Safeguarding the First Generation of Digital Natives. 31st International Conference of Data Protection and Privacy Commissioners in Madrid, Future of Privacy Forum, (2009), 11.

²⁴⁸ GDPR, Article 9(1).

²⁴⁹ GDPR, Article 6(1)(d).

Even if parents trust the website, there is always the potential of cyber-attacks, and if a malicious third-party acquires a child's biometric data, such as his/her fingerprint, they may access any service that needs a fingerprint (e.g., verifying a passport, unlocking a phone's screen). Eventually, the consequences would be extremely dangerous, given that a fingerprint, like other biometric data, is a unique characteristic of an individual. Fake fingerprints may imitate real ones in today's technology.²⁵⁰ Biometrics provide a false sense of security since they are unique features, but that does not mean that current technology cannot reproduce them. According to a study presented at a security conference in Los Angeles, artificial fingerprints called "DeepMasterPrints" by New York University researchers may fool 77% of the subjects in the dataset with a 1% mismatch rate.²⁵¹ So, in today's digital age, unique does not imply secrets, and passwords can be changed if they are hacked, but what if fingerprints are stolen? As a result, before exposing biometric information in the cybersphere, one should proceed with caution.

A person's voice and facial features can be used as biometric data since these distinguishing characteristics can also be used to identify a person if they are processed using a specific technological measures.²⁵² There are voice recognition artificial intelligence (AI) solutions that might be used for verifying the age of individuals, such as Apple's Siri,²⁵³ which detects the users' voice and assists them with vocal instructions, or voice signatures,²⁵⁴ which are currently used to access one's own bank account via telephone banking. When it comes to face-matching AI solutions, one might consider the iPhone's Face ID tool, which

²⁵⁰ The Guardian, Fake fingerprints can imitate real ones in biometric systems – research, 15 November 2018, <https://www.theguardian.com/technology/2018/nov/15/fake-fingerprints-can-imitate-real-fingerprints-in-biometric-systems-research> (last visited 10 March 2023).

²⁵¹ Philip Bontrager, Aditi Roy, Julian Togelius, Nasir Memon, and Arun Ross: Deepmasterprints: Generating masterprints for dictionary attacks via latent variable evolution, 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), IEEE (2018), 2. cited in The Guardian, Fake fingerprints can imitate real ones in biometric systems – research, 15 November 2018, <https://www.theguardian.com/technology/2018/nov/15/fake-fingerprints-can-imitate-real-fingerprints-in-biometric-systems-research> (last visited 10 March 2023).

²⁵² GDPR, Recital 51: "The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person."

Carl Van der Maelen: The Coming-of-Age of Technology: Using Emerging Tech for Online Age Verifications, *Delphi - Interdisciplinary Review of Emerging Technologies*, vol. 2, no. 3 (2019), 119-120.

²⁵³ Apple, Siri, <https://www.apple.com/siri/> (last visited 10 March 2023).

²⁵⁴ For instance: HSBC Voice ID, <https://www.hsbc.com.hk/ways-to-bank/phone/voice-id/> (last visited 10 March 2023).

is used for unlocking the screen and accessing certain applications (e.g., Internet banking apps, e-wallet) on users' phones.²⁵⁵

However, many AI systems can only determine an age range rather than the specific age of a child. Because a 12-year-old child and a 13-year-old child may sound and look alike, an AI cannot determine a child's actual age.²⁵⁶ Therefore, we suggest that verifying the age via voice recognition tools is not an appropriate solution, and it can also cause the same problems with fingerprints as we mentioned above. If the Face IDs and voice signatures are matched with the individuals' personal IDs, there is always the risk of having those unique features stolen by malicious attackers, which can lead to dangerous situations because they may currently give access to a lot of personal information (e.g., bank accounts,²⁵⁷ phone access).

None of the aforementioned methods are flawless. On the one hand, there are pretty precise ways for estimating a child's age, but they are not privacy-friendly, such as personal ID or biometric characteristics (e.g., fingerprint) scanning. On the other hand, there are technologies that may breach data privacy but are ineffective for estimating an individual's precise age, such as voice recognition and facial ID tools. Moreover, there are methods that are privacy-friendly yet completely useless since they are so simple to deceive, such as self-verification and/or peer-verification. There is also a knowledge-based authentication method that does not violate privacy but is ineffective in identifying exact age. There is no middle ground solution that protects children's personal information while also protecting them from harmful content.²⁵⁸

As previously stated, many underage children disclose personal information online, according to Pew Research Center research and EU Kids Online survey results (e.g., social media network sites). As many websites only require self-verification methods, children may easily deceive the system. These legislative threshold ages and age verification procedures appear to be ineffective in preventing children from accessing inappropriate online content. In this case, it should be noted that, in addition to the legal requirements and the restrictions imposed by data controllers and operators, additional supporting solutions are necessary.

²⁵⁵ Apple, Use Face ID on your iPhone or iPad Pro, <https://support.apple.com/en-us/HT208109#:~:text=Tap%20Set%20Up%20Face%20ID,your%20head%2C%20tap%20Accessibility%20Options>. (last visited 10 March 2023).

²⁵⁶ Asli Alkis: Investigating the usefulness of online age verification methods, *Studia Iurisprudentiae Doctorandorum Miskolciensium*, (2021) vol.1, 16-17.

²⁵⁷ Children may also have bank accounts with the consent of their parents or guardians. For instance: HSBC, Children's Bank Accounts, <https://www.hsbc.co.uk/current-accounts/products/children/> (last visited 10 March 2023).

²⁵⁸ Asli Alkis: Investigating the usefulness of online age verification methods, *Studia Iurisprudentiae Doctorandorum Miskolciensium*, (2021) vol.1, 21.

It is important to note at this point that euCONSENT is an ongoing EU-funded project comprised of twelve partners including academic institutions, NGOs, and technology providers²⁵⁹ that aims to design and provide an EU-wide network that is trying to complete age verification systems and secure online parental consent when children share their personal data online. The primary purpose of this initiative is to safeguard children from potential damage when they access age-restricted adult content online, while also advocating their rights to access appropriate online content that the Internet provides for children.²⁶⁰

The first large-scale pilot of this project was completed between February 17th and March 3rd, 2022. More than 2000 people from five countries in Europe took part in the study, including Greece, the United Kingdom, Germany, Cyprus, and Belgium. In this first part of the project, they aimed to understand the current situation in the online sphere, such as how businesses (e.g., social media channels, online shops, etc.) obtain parental consent and verify the age of the children, how they implement GDPR requirements, and what children and parents expect in terms of the safety and security of their personal data.²⁶¹

To analyse them, they assigned specific missions to project members to perform. Each participant was required to accomplish three tasks and then complete the questionnaires connected to these missions. For example, the first mission was to access the dummy alcohol seller website, and in order to do so, the children should verify their age using one of the methods provided. Then the website should direct them to the protected website, where they are warned that they are too young to access that adult content website. The second objective was to enter the dummy social networking site, but because they were identified as underage in the prior mission, they now need parental consent to progress. The third assignment was to a dummy chat website, where they also requested parental consent to finish the mission. Other scenarios included a dummy knife seller website and a dummy dating site.²⁶²

According to the statistics, over 81% of the participants completed at least two missions, and 63% finished all three missions while following the instructions. The research indicated that face recognition was by far the most often used method for age verification by 68% of all participants due to its quickness and simplicity, whereas credit card verification was

²⁵⁹ UpcoMinds, AgeCheck, JusProg, Lisal Expert, Revealing Reality, AGEify, Aston University, London School of Economics and Political Science, Leiden University, Digie, AVPA, John Carr. <https://euconsent.eu/partners/> (last visited 21 January 2023).

²⁶⁰ euCONSENT, FAQ: What is euCONSENT?, <https://euconsent.eu/faq/> (last visited 21 January 2023).

²⁶¹ euCONSENT, euCONSENT's first large scale pilot (18 March 2022) <https://euconsent.eu/euconsents-first-large-scale-pilot/> (last visited 21 January 2023).

²⁶² euCONSENT, euCONSENT's first large scale pilot: What did the participants have to do? (18 March 2022) <https://euconsent.eu/euconsents-first-large-scale-pilot/> (last visited 21 January 2023).

chosen by only 3% of all participants. The research also revealed that while 91% of parents thought it was vital for them to offer consent each time their children wished to disclose personal data online, 74% of them displayed willingness in real-life settings. The next phase of the project will be resumed as soon as the project finds a new funder, as the EU fund is exhausted in this first phase.²⁶³

In our perspective, having such a study to assess the existing situation and provide suggestions to EU legislators using the findings of these surveys is a critical step, and it may serve as an example for other countries around the world. Nonetheless, there are certain gaps in the initial phase of this project. For example, the project shows that the most commonly used age verification method is facial recognition preferred by 68% of all participants. However, we do not deduce how effective it was in completing the missions, because, as previously stated, facial recognition cannot be accurate in cases where, for example, a 16-year-old may appear to be 18 years old and have access to age-restricted consent simply because he/she seems to be 18 years old. It is a simple method to use, as stated on the project website, however, it would have been ideal to illustrate the obstacles and challenges of the procedures as well. Furthermore, the least popular method was the use of credit cards as a means of age verification with only 3% of participants in the euCONSENT project, but the reason behind this is not mentioned.²⁶⁴

Furthermore, within the scope of this project, the only way to gain parental consent was to contact them through email using parental consent provider applications JusProg and Upcom.²⁶⁵ It would have been preferable, however, to include other parental consent-granting methods in order to compare them and identify which method is the most and least popular among parents. Thus, we might have gained insight into the relative efficacy of the indicated parental consent providing methods.

In the following phases of this research, we believe that it would be ideal to provide more extensive results using comparative methodologies and also, not only reporting what they discovered, but rather interpreting the findings with the challenges and benefits. It

²⁶³ euCONSENT, A summary of the achievements and lessons learned of the euCONSENT project and what comes next (7 December 2022) <https://euconsent.eu/a-summary-of-the-achievements-and-lessons-learned-of-the-euconsent-project-and-what-comes-next/> (last visited 21 January 2023).

²⁶⁴ euCONSENT, A summary of the achievements and lessons learned of the euCONSENT project and what comes next (7 December 2022) <https://euconsent.eu/a-summary-of-the-achievements-and-lessons-learned-of-the-euconsent-project-and-what-comes-next/> (last visited 21 January 2023).

²⁶⁵ euCONSENT, euCONSENT's first large scale pilot: How about parental consent? Which Parental Consent Providers were involved? How was the process? (18 March 2022) <https://euconsent.eu/euconsents-first-large-scale-pilot/> (last visited 21 January 2023).

would also be beneficial to include other EU Member States in order to create a larger scale project with a more comprehensive approach.

Taking all into account, the spirit of GDPR and COPPA clearly demonstrates that they are both founded on parental supervision and responsibility. However, given the natural flow of life, parents cannot always monitor their children. Even if they could monitor, they would be invading the children's privacy. Because even though parents are in charge of their children's online activities, children are still distinct individuals, not extensions of their parents. Besides, their need for and expectation of privacy grows with age, making teenagers' privacy demands incomparable to those of young children. In this scenario, we advocate for the implementation of a system that prevents children from accessing inappropriate content without jeopardizing their privacy.²⁶⁶

The European Commission also acknowledges that, despite the GDPR, age verification methods and parental consent tools are ineffective, because most users are only asked to provide a birth date or tick a box at registration.²⁶⁷ As a result, in accordance with its eID proposal,²⁶⁸ the Commission encourages the Member States to implement effective age-verification methods.²⁶⁹ According to the Commission, children can use their eIDs to prove their age without revealing any other personal information (e.g., name or address).²⁷⁰ On one hand, it would be a trustworthy solution, because it would be based on reliable government databases.²⁷¹ On the other hand, it may result in discrimination against those who do not

²⁶⁶ Asli Alkis: Investigating the usefulness of online age verification methods, *Studia Iurisprudentiae Doctorandorum Miskolciensium*, (2021) vol.1, 18-19.

²⁶⁷ European Commission, Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions a Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+), Brussels, 11.5.2022 COM (2022) 212 final, 6.

²⁶⁸ European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, Brussels, 3.6.2021 COM (2021) 281 final 2021/0136 (COD).

²⁶⁹ European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, Brussels, 3.6.2021 COM (2021) 281 final 2021/0136 (COD), 11-12.

²⁷⁰ European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, Brussels, 3.6.2021 COM (2021) 281 final 2021/0136 (COD), 4.

²⁷¹ Jules Polonetsky, *Online Age Verification for Our Children A Report on the Tools and Resources Available for Safeguarding the First Generation of Digital Natives*. 31st International Conference of Data Protection and Privacy Commissioners in Madrid, Future of Privacy Forum, (2009), 9.

wish to participate in this system; thus, this system would be preferable if it remained a voluntary choice.²⁷²

Furthermore, due to the mass storage of official documents and biometric data of users, this system would pose certain security and privacy risks. Thus, the system should be effectively protected against malicious cyber-attacks and hacking and moreover, governments or service providers should not abuse the system by monitoring individuals' use of eIDs.²⁷³ Nonetheless, we welcome that unlike traditional personal ID verification solutions, the eID concept is based on the data minimisation principle²⁷⁴ and is designed to provide selective disclosure of features (for example, allowing age verification without revealing the legal name, address, or other irrelevant data).²⁷⁵ If the abovementioned security and privacy issues are mitigated, we agree that this eID solution will result in an EU-wide recognized proof of age based on date of birth that is both privacy-friendly and secure.²⁷⁶

3.5 Short summary

Chapter 3 covered the concept of parental consent, when it is required, and how to verify it before processing children's personal data. COPPA provides data controllers with various non-exhaustive methods to get parental consent. Whereas the GDPR lacks this guidance. We recommended that the GDPR transplant these COPPA sample methods under Article 8.

Under the Subchapter 3.3, we discussed how the GDPR partially transplanted the COPPA's threshold age of online consent. To determine whether age of digital consent is consistent and significant, we compared it to other consent ages in other legal disciplines.

²⁷² BEUC (The European Consumer Organisation), Making European Digital Identity as Safe as It Is Needed, https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-016_eidas_position_paper.pdf, 1 (last visited 21 February 2023).

²⁷³ BEUC, Making European Digital Identity as Safe as It Is Needed https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-016_eidas_position_paper.pdf, 1 (last visited 21 February 2023).

²⁷⁴ Data minimisation principle requires that the “personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”. GDPR, Article 5(1)(c).

²⁷⁵ BEUC, Making European Digital Identity as Safe as It Is Needed, https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-016_eidas_position_paper.pdf, 3 (last visited 10 March 2023) and European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, Brussels, 3.6.2021 COM (2021) 281 final 2021/0136 (COD), 18 https://eur-lex.europa.eu/resource.html?uri=cellar:5d88943a-c458-11eb-a925-01aa75ed71a1.0001.02/DOC_1&format=PDF (last visited 10 March 2023).

²⁷⁶ European Commission, New European strategy for a Better Internet for Kids – Questions and Answers, 11 May 2022, 12. How will the new strategy address age verification?, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_2826 (last visited 10 March 2023).

We found out via research and surveys conducted in the EU and the US that digital consent ages are neither relevant nor consistent for protecting children's personal data. Besides, these threshold ages do not have practical effects on children's internet activity habits and behaviours. Thus, we questioned the necessity of these threshold ages in the GDPR and COPPA. But still, since this is the actual reality of both of the legislation, we promoted awareness that Member States should at least uniform the age of consent and justify their choice.

As these are long-term remedies, we discussed the current solutions regarding Internet age restrictions under the Subchapter 3.4. We examined age verification methods for implementing these restrictions. We observed that existing methods to prevent children from age-restricted consent are either privacy-friendly but not useful or effective but not privacy-friendly. In the worst cases, they are neither useful nor reliable in terms of protecting personal data. So, we examined the Commission's eID proposal and found that if security and privacy risks (e.g., cyber-attacks, hacker activities) are mitigated, this eID solution would provide a privacy-friendly and EU-wide age verification method.

4. Main rights of the children and their parents under the GDPR and COPPA

Children have the same rights as adults under the GDPR. They have the right to be informed, the right to access, the right to rectification, the right to erasure (including the right to be forgotten), the right to processing restriction, the right to data portability, the right to object, and the right not to be subject to a decision based solely on automated processing, including profiling.²⁷⁷

First and foremost, data subjects have the right to have easily understandable information about who is processing their data, what data is being processed, and what is the purpose of processing.²⁷⁸ Article 12 of the GDPR requires data controllers to use plain and clear language, particularly when any information relates to a child.²⁷⁹

Second, data subjects have the right to request access to any personal information about them obtained by data controllers.²⁸⁰ If feasible, the data controller shall provide data subjects with remote access to a secure system where they can have direct access to their personal information.²⁸¹ For example, if a child wishes to access his/her data that is being processed by an educational children's website (e.g., Funbrain.com²⁸²), the privacy policies usually mention this right for European residents.²⁸³ However, the children may be unaware of the privacy policies, therefore, it would be ideal for them to create short videos or colourful vivid pictures with plain language so that the children can understand their data protection rights much better.

Third, data subjects have the right to rectification, which means they have the right to request that the data controller rectify any inaccurate information on them without undue delay.²⁸⁴ Fourth, data subjects have the right to erasure, which they can exercise when the purposes for which the data controller collected their data no longer exist; if the data subjects withdraw their consent; where the data subjects object to the processing of their personal information.²⁸⁵ Most importantly, the data subjects exercise this right if they give consent

²⁷⁷ GDPR, Article 12-23.

²⁷⁸ GDPR, Article 12-14.

²⁷⁹ GDPR, Article 12.

²⁸⁰ GDPR, Article 15.

²⁸¹ GDPR, Recital 63.

²⁸² Fun Brain: <https://www.funbrain.com/> (last visited 10 March 2023).

²⁸³ Fun Brain, Privacy Policy: <https://www.funbrain.com/privacy-policy> (last visited 10 March 2023).

²⁸⁴ GDPR, Article 16.

²⁸⁵ GDPR, Article 17.

when they are children and are not fully aware of the consequences and risks. Even if the data subject is now an adult, he/she can still use this right.²⁸⁶

Furthermore, Article 17(2) of the GDPR refers to the right to be forgotten.²⁸⁷ The "right to be forgotten" is a broader concept that originated in a European Court of Justice decision.²⁸⁸ It allows individuals to request that search engines remove links to information about them, which is inaccurate, inadequate, irrelevant, or excessive for the purpose it was processed.²⁸⁹ The right to erasure is limited to personal data retained by the controllers, whereas the right to be forgotten extends to publicly available information on the internet.

In the US, for example, there is a case named *Sidis v. F-R Publishing*. Sidis, the child prodigy, became a public figure in the early 1900s due to his parents' desire. When he became an adult, the *New Yorker* published an article about him, and Sidis filed a lawsuit because he didn't want to be seen by the public. However, the court ruled against his free will because, like all other famous persons, the public is interested in learning more about them.²⁹⁰ Was it, however, Sidis' decision to be in the spotlight at the beginning? Did he have a saying when his parents put him in front of the public when he was a child? Sidis' privacy would not have been violated, if he had the right to have his information erased from the newspaper. Thus, the GDPR's right to be forgotten is critical, particularly in cases like Sidis'.

Fifth, data subjects have the right to restrict the processing of their personal information. These limitations might include, but are not limited to, temporarily relocating their personal data to another processing system, making certain personal data inaccessible to other users, and temporarily deleting published data from the website. The processing restriction should be noted on the given system.²⁹¹ This right may be too complicated for a child to exercise, but their parents can exercise it on their behalf if necessary.

Sixth, if the personal data is obtained based on consent or the performance of a contract, and the processing of personal data is managed by automated means, data subjects have the

²⁸⁶ GDPR, Recital 65.

²⁸⁷ GDPR, Article 17(2).

²⁸⁸ The first time the "right to be forgotten" was used in a case decided by the European Court of Justice (ECJ) was in the case of *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*, which was decided on May 13, 2014.

Case C 131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* EU:C:2014:317.

²⁸⁹ Case C 131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* EU:C:2014:317, para 92.

²⁹⁰ Case 113 F.2d 806, *Sidis v. F-R Pub. Corporation* (No. 400), Judgement of the Court of Appeals for the Second Circuit, New York, 22 July 1940 cited in Stacey B. Steinberg: *Sharenting: Children's privacy in the age of social media*, *Emory LJ*, 66 (2016), 859-860.

²⁹¹ GDPR, Recital 67.

right to transmit their data from one controller to another in order to strengthen their control over their data. If technically feasible, data subjects should be able to transmit their data directly from one controller to another.²⁹² As the previous right, parents can use this right to data portability on children's behalf if they feel it is necessary.

Data subjects have the right to object to processing where it is based on the performance of a task in the public interest, the exercise of official authority vested in the data controller, or the controller's legitimate interests. The controller must cease processing the personal data unless it proves compelling legitimate reasons for the processing that outweigh the data subject's interests, rights, and freedoms.²⁹³ However, justifying the legitimate interest is hard for the data controller where the data subject is a child, because Article 6(1) states that the interests, freedom, and fundamental rights of the data subject take precedence over the interests of the data controller or third parties particularly when the data subject is a child.²⁹⁴ In addition, data controllers shall perform a data protection impact assessment (DPIA) before processing the personal data of children, since doing so poses a high risk to the rights and freedoms of children and other vulnerable natural people, as well as to their physical, material or non-material wellbeing.²⁹⁵

Furthermore, data subjects have the absolute right to object to the use of their personal data for direct marketing purposes. In such a case, the data controller has no exemptions or reasons for refusal. In other words, the processing of the personal data for such purposes should cease.²⁹⁶ Besides, the GDPR's preamble offers additional protections for children when it comes to the use of their data for direct marketing purposes.²⁹⁷ This special protection should, in our view, be interpreted so that, if a child objects to a processing for direct marketing purposes, the data controller should act immediately, without waiting for parental consent.

Eighth, data subjects have the right not to be the subject of a decision based solely on automated processing, including profiling, unless the decision

“is necessary for entering into, or performance of, a contract between the data subject and a data controller; is authorised by Union or Member State law to which the controller is subject and which

²⁹² GDPR, Article 20 and Recital 68.

²⁹³ GDPR, Article 21(1).

²⁹⁴ GDPR, Article 6(1)(f).

²⁹⁵ GDPR, Article 35(1) and Recital 75.

²⁹⁶ GDPR, Article 21(2) and Article 21(3).

²⁹⁷ GDPR, Recital 38.

also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or is based on the data subject's explicit consent."²⁹⁸

Although Recital (71) indicates that profiling should not be used on children, Recital (38) does not deny profiling but requires special protection for underage children.²⁹⁹ Furthermore, because Article 22 does not explicitly exclude children from its content, the GDPR's spirit on child profiling is unclear. However, we strongly advocate that, given the children's relative immaturity and naïve understanding of the consequences of algorithms and personalized advertisements on websites, data controllers should not use the exceptions mentioned above - specified in Article 22(2) - to justify children profiling.³⁰⁰

Although the rights outlined above apply to children, the GDPR does not specify how or when children can exercise these rights. And there is no guidance as to whether parents can use these rights on behalf of their children, or how they might do so in practice. However, it may be instructive to review other countries' applications in this circumstance.³⁰¹ In Scotland, for example, there is a rebuttable assumption that a child of 12 has reached the maturity to exercise their data protection rights until shown otherwise. This assumption does not exist throughout the rest of the United Kingdom. They think that competency is determined by one's level of understanding rather than by one's age. Therefore, if the child is competent to give consent for their personal data processing, they believe it is reasonable to assume that those children are also competent to exercise their own data protection rights.³⁰²

According to the Data Protection Commission of Ireland, not only the child's age and maturity should be considered, but also the type of personal data being processed, the service offered by the data controller to a child and the context of processing, the type of request a child seek, whether enabling children to exercise their rights is in their best interests, and whether the child seeks parental assistance or participation to exercise their rights. Because, for example, accessing or erasing sensitive data (e.g., medical data) on the Internet requires

²⁹⁸ GDPR, Article 22(1) and (2).

²⁹⁹ GDPR, Recital 38 and 71.

³⁰⁰ GDPR, Article 22(2).

³⁰¹ Data Protection Commission Ireland, Children Front and Centre, Fundamentals for a Child-Oriented Approach to Data Processing-Draft Version for Public Consultation, December 2020, 33.

³⁰² Information Commissioner's Office (ICO), What rights do children have?, When may a child exercise these rights on their own behalf?, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/what-rights-do-children-have/> (last visited 10 March 2023).

a different handling than accessing or erasing personal data shared on social media networks (e.g., Facebook).³⁰³ We consider that Ireland's approach in this respect is more comprehensive, and we also endorse the idea that not only age and maturity but also the sorts of rights held by children should be examined.

To summarize, while the GDPR has not clarified it, children should have the right to exercise their data protection rights whenever it is in their best interests. It would be preferable if children could use their rights individually, depending on the types of rights, or via parental representation if they have not reached maturity or the age of consent.³⁰⁴ Additionally, it would be ideal if there was soon to be official guidance for children and their parents to exercise these mentioned data protection rights.

Moreover, children's privacy rights are not addressed in the COPPA, but rather “parental rights” regarding the children's personal information are specified. First and foremost, there is a parental right of notice, which requires operators to offer notice and get verifiable parental consent before collecting, using, or disclosing personal information from children.³⁰⁵ Second, parents have the right to review any personal information provided online by their children, and the operator should provide that parent with the option “to refuse the operator's further use or future online collection of personal information from that child at any time, and to direct the operator to delete the child's personal information.”³⁰⁶

It would have been ideal, though, if the children had such rights rather than their parents having them on their behalf. Because there is no reason why children should be prevented from asserting their rights if they are mature enough to do so. If we merely provide their parents access to their data, it may not always be in the best interests of the children. Assuming, for example, that the children submitted personal information on a website and, after some time, discovered that the information is no longer relevant and decides to delete it. They should have the right to have their personal information deleted, and operators should make this process easier for children, because the information they want to delete could be more sensitive for them, and the longer the process takes, the riskier it is to keep that information online, especially if the data is open to the public.

³⁰³ Data Protection Commission Ireland, Children Front and Centre, *Fundamentals for a Child-Oriented Approach to Data Processing-Draft Version for Public Consultation*, December 2020, 34.

³⁰⁴ Data Protection Commission Ireland, Children Front and Centre, *Fundamentals for a Child-Oriented Approach to Data Processing-Draft Version for Public Consultation*, December 2020, 34-35.

³⁰⁵ 16 CFR COPPA 312.4(a).

³⁰⁶ 16 CFR COPPA 312.6(a)(2).

Loss of control over one's own personal information can have tragic consequences, as can be seen in case of *Amanda Todd*, a Canadian teenager who killed herself after being exposed to long-term bullying because of a single photo she couldn't erase. In the end, Amanda had created a silent YouTube video in which she shared her story using a collection of handwritten notes before she committed suicide. Amanda says on one of the notes: "I can never get the photo back, it's out there forever...". These sorts of events may happen to anyone, due to the increasing use of social media among children and teenagers. Therefore, it is essential to broaden the COPPA's provided rights to include children.³⁰⁷

Furthermore, considering the above-mentioned GDPR data subject rights, at least the right to access, ratification, deletion, and not being subject to a decision based solely on automated processing (especially profiling) should be provided to children under the COPPA as well. If the children are not mature enough to exercise these rights and have not yet reached the age when they may grant consent for their online actions, parents can exercise these potential rights on their behalf. Otherwise, the children may exercise these rights themselves.

Children enjoy several rights under the United Nations Convention on the Rights of the Child (UNCRC)³⁰⁸, which the US has signed but not ratified, while all EU Member States have signed and ratified. These rights include the right to freely express themselves and be heard,³⁰⁹ the right to seek and receive any kind of information in any form written, orally, in the form of art, or via any other media that a child chooses,³¹⁰ and the right to engage in play and recreational activities appropriate to their age and maturity.³¹¹ Accordingly, it is critical for parents to give these opportunities to their children and allow them to use their rights freely within the limits of what is possible. However, the GDPR's, particularly the COPPA's overprotective parent approach, would have a severe impact on the mentioned children's rights. Therefore, it is very important to offer a safe environment for children without depriving them of the benefits of the internet, while also attempting to protect their right to privacy and data protection from third parties without being infringed by their own parents. The GDPR and COPPA should not disregard this, and children should be given as much

³⁰⁷ My story: Struggling, bullying, suicide, self-harm, *Thesomebodytoknow* videos, available at: <https://www.youtube.com/watch?v=vOHXGNx-E7E> (10 March 2023) cited in Asli Alkis Tümtürk, Implications of parental sharing of children's personal data online (not published yet).

³⁰⁸ UN Commission on Human Rights, Convention on the Rights of the Child, E/CN.4/RES/1990/74, 07.03.1990.

³⁰⁹ UNCRC, Article 12.

³¹⁰ UNCRC, Article 13.

³¹¹ UNCRC, Article 31.

control over their personal data as feasible, appropriate with their age and maturity level. This may be achievable by granting them specific rights that they can exercise independently of their parents to a reasonable extent. Finally, we suggest for the expansion and implementation of these children's privacy and data protection rights in practice.

This is not a result that can be achieved just by legislation, but rather with the active engagement of parents, the service providers and the data controllers. First, parents should provide their children with the benefits of the Internet, secure their children's personal data from malicious third parties by participating appropriately, when necessary, without jeopardizing their children's privacy, and be able to manage this balance sufficiently. Second, data controllers and service providers (e.g., third party suppliers) should be able to communicate and display these rights to children using colourful and vivid pictures and simple and clear language.

In this case, children will be more aware of their rights and will be able to comprehend the limitations to which they may use their rights, as well as how much assistance they need from their parents if necessary. The main obligations imposed on data controllers will be discussed in further depth in the next chapter.

4.1 Short summary

In brief, under the GDPR, children have the same data protection rights as adults. However, we concluded that neither the children nor their parents are given any guidance on how to exercise these rights. Unlike the GDPR, COPPA does not explicitly grant children privacy rights; rather, it grants parental rights over their children's personal information.

We acknowledged that certain rights may be too complicated for children to exercise, thus parents should be able to do so if required. Nonetheless, the right to access, ratification, and deletion may be easier for children to exercise without parental participation if they are mature enough to understand the consequences of their online actions. Besides, we claimed that enjoying these rights should not cause dangerous situations for them in the ordinary course of events.

As we mentioned in the previous chapter, children should not lose control over their data since it might lead to detrimental consequences, such as Amanda Todd's suicide because she was unable to remove it on her own.

Ergo, we reached the conclusion that data controllers, service providers, and parents must collaborate to provide a secure online environment for children. Because children

may learn about their rights and either exercise them themselves or ask their parents to do so on their behalf.

5. Main obligations imposed on data controllers

The GDPR defines the data controller as “[t]he 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”³¹² and the first and foremost obligation of the data controller under the GDPR is to comply with the Regulation. Article 24 of the GDPR explains it as follows:

“Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.”³¹³

This implies that the data controller should be well-versed in the GDPR's responsibilities and adhere to the personal data processing principles outlined in Article 5. These are the principles of lawfulness, fairness, and transparency, as well as accuracy, purpose limitation, data minimisation, storage limitation, integrity, confidentiality, and accountability of the controller for this compliance.³¹⁴

The following measures should be implemented by the data controller: as technical measures, pseudonymisation and encryption of personal data are used,³¹⁵ and organizational measures include risk assessment which means mitigating solutions to reduce risks³¹⁶ and having effective and compliant data protection policies in place.³¹⁷ In addition, the data controller shall make it possible and easy for data subjects to exercise their rights.³¹⁸ More importantly, the data controller must safeguard children and their rights, and they must make all reasonable attempts to get consent for processing children's data from the holder of parental responsibility for the child if the child is underage, considering available technology.³¹⁹

³¹² GDPR, Article 4(7).

³¹³ GDPR, Article 24(1).

³¹⁴ GDPR, Article 5(1)(a)(b)(c)(d)(e)(f).

³¹⁵ GDPR, Article 32(1)(a).

³¹⁶ GDPR, Article 35 (Data Protection Impact Assessment).

³¹⁷ GDPR, Article 24(2).

³¹⁸ GDPR, Article 12(2).

³¹⁹ GDPR, Article 8(2).

Approved codes of conduct, as defined in Article 40 of the GDPR,³²⁰ or approved certification mechanisms, as defined in Article 42 of the GDPR,³²¹ might be used to demonstrate that the data controller is appropriately implementing the obligations.³²²

Another obligation of the data controller is to guarantee that the concept of data protection by design and by default is followed.³²³ Adopting data protection principles from the design stage all the way through the life cycle of a new project, product, or asset is what data protection by design includes. Data protection by default implies that data controllers only handle data that is necessary for their processing objectives. It is linked to the fundamental principles of data minimization and purpose limitation. In this case, if the data controller's personal data processing changes, or if the data controller decides to process more data of the data subject, the data subjects must provide updated consent.³²⁴

Furthermore, if data controllers involve someone to process personal data on their behalf, they should ensure that these processors are knowledgeable, reliable, and have adequate resources to ensure the requirement of appropriate technical and organizational measures that meet the Regulation's requirements.³²⁵

These processors are defined as “a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller” under the GDPR³²⁶ and

³²⁰ GDPR, Article 40. “Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to: fair and transparent processing; the legitimate interests pursued by controllers in specific contexts; the collection of personal data; the pseudonymisation of personal data; the information provided to the public and to data subjects; the exercise of the rights of data subjects; the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained; the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32; the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects; the transfer of personal data to third countries or international organisations; or out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.”

³²¹ GDPR, Article 42 and Recital (100): “In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.”

³²² GDPR, Article 24(3).

³²³ GDPR, Article 25.

³²⁴ ICO, Data protection by design and default, at What is data protection by design?, and at What is data protection by default?, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/#dgd3> (last visited 10 March 2023).

³²⁵ GDPR, Article 28(1) and Recital 81.

³²⁶ GDPR, Article 4(8). For more information about the obligations of the controllers, processors and their relationships: EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version

should be governed by a legal contract that includes the following: the type of personal data that they are processing and the categories of data subjects, the purpose and scope of processing, the risk to the data subjects' rights, and their certain tasks and responsibilities regarding the relevant processing.³²⁷ The processor's responsibility also includes returning or deleting the processed data at the end of processing, if demanded by the data controller.³²⁸

Each data controller and processor should also document their processing actions and make them available to the supervisory authority if required, so that this documentation may be used to monitor such processes. This documentation should include: the name and contact details of the controller and, if available, the processor; the purpose of the processing; the type of personal data and categories of data subjects; with whom the personal data have been shared or will be shared, e.g., third parties or international organisations; documentation of the adequate safeguards if the collected personal data has been shared with third parties; the time limit for the erasure of processed data; and the description of implemented technical and organisational security measures.³²⁹

If required, data controllers and processors should collaborate with the supervisory authority to perform its tasks.³³⁰ Furthermore, as soon as the data controller gets aware of a

2.1 Adopted on 07 July 2021, pp. 1-51. https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf (last visited 10 March 2023).

³²⁷ GDPR, Article 28(3) and Recital (81).

³²⁸ GDPR, Article 28(3)(g).

³²⁹ GDPR, Article 30 and Recital (82).

³³⁰ GDPR, Article 32 and for information about the tasks of supervisory authority see Article 57: "...monitor and enforce the application of this Regulation; promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention; advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing; promote the awareness of controllers and processors of their obligations under this Regulation; upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end; handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary; cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation; conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority; monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices; adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2); establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4); give advice on the processing operations referred to in Article 36(2); encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5); encourage the establishment of data protection certification

personal data breach, they must notify the supervisory authority within seventy-two hours of being aware of it.³³¹ Because failure to address the data breach might

“[r]esult in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned”.³³²

If the personal data in question is related to children, data controllers must proceed with greater caution, since a data breach might have far-reaching negative implications for children than for adults. For example, in September 2021, NBC News gathered and examined school files from hackers' dark web pages and discovered they were rife with children's personal data including permanent information such as birth dates and social security numbers, which can result in a lifetime of identity theft because these data remain the same even when they become adults.³³³ However, children are likely to be less aware of the ramifications and dangers of identity theft. Therefore, it is the obligation of data controllers to notify the supervisory authority of such data breaches without any delay.³³⁴ Furthermore, if the data breach is likely to result in a high risk to a data subject's rights and freedoms, they should notify the data subject without undue delay. This communication should be made with plain and clear language and should include at least the name and contact information of the data protection officer, a description of the potential consequences

mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5); where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7); draft and publish the requirements for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43; conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43; authorise contractual clauses and provisions referred to in Article 46(3); approve binding corporate rules pursuant to Article 47; contribute to the activities of the Board; keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and fulfil any other tasks related to the protection of personal data.”

³³¹ GDPR, Article 33(1).

³³² GDPR, Recital (85).

³³³ NBC News, Hackers are leaking children's data — and there's little parents can do, 10 September 2021, by Kevin Collier, <https://www.nbcnews.com/tech/security/hackers-are-leaking-childrens-data-s-little-parents-can-rcna1926> (last visited 10 March 2023).

³³⁴ GDPR, Recital 38: “Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.” and Article 33(1).

of the personal data breach, and a description of the measures taken or proposed to be taken by the controller to reduce the negative effects.³³⁵

Data subjects may not need to be communicated in some cases. First, if the data controller has established appropriate technological and organisational protections, such as encryption, the communication is not required. Second, where the controller has taken steps to reduce the high risk to data subjects' rights and freedoms, contacting them is also unnecessary. Third, the communication shall not be required when disproportionate effort is involved. Instead, in such cases, public communication may occur to inform data subjects.³³⁶

If data controllers apply this personal data breach notification obligation to children's personal data, they must consider the age and maturity of the children whose personal data has been violated. In case the affected children can consent to the processing of their personal data, the data controllers consider notifying the children about the data breach. Nonetheless, it would be more reassuring if both parents and children were informed simultaneously. Yet, when the children are underage, data controllers should contact their parents and notify them of the data breach. In addition, data controllers may opt to directly notify other individuals in order to mitigate certain potential impacts on children.³³⁷ For instance, a teacher or principal of the impacted child may be chosen if the data breach involves a student's personal details from school records (e.g., cyber attackers hacking into school databases and stealing students' personal data).

The occurrence of a data breach involving children's data with sensitive nature might lead to even more dangerous scenarios. For example, if some computers were taken from a children's health centre that collected health³³⁸ and social welfare data on a particular number of children, the children and their families may be put in jeopardy. Because sensitive information about those children has now fallen into the hands of unauthorized and malicious individuals, anything is possible, including blackmailing those parents and children using the gathered sensitive information or targeting parents of critically ill children to profit from their vulnerability (e.g., charlatans).³³⁹

³³⁵ GDPR, Article 34(1) and (2).

³³⁶ GDPR, Article 34 (3)(a)(b) and (c).

³³⁷ Article 29 Data Protection Working Party, Opinion 03/2014 on Personal Data Breach Notification, 693/14/EN WP 213, 25 March 2014, p. 5-6.

³³⁸ Health data falls into special category of personal data with sensitive nature under the Article 9(1) of the GDPR.

³³⁹ Article 29 Data Protection Working Party, Opinion 03/2014 on Personal Data Breach Notification, 693/14/EN WP 213, 25 March 2014, p. 5.

Given the vulnerability of children, as well as the risks and consequences of data breaches, data controllers should not apply the aforementioned exceptions to their notification obligation for data breaches. Even if they have put in place the necessary technological and organizational safeguards, they should notify the parents and children as quickly as possible. Furthermore, they shall give guidance and advice to parents in order to help them mitigate the adverse impact of personal data breaches on their children.³⁴⁰

If there will be personal data processing utilizing new technologies that will likely pose a high risk to data subjects' rights and freedoms, it is required to conduct a data protection impact assessment (DPIA) of the proposed processing operations on personal data protection prior to processing.³⁴¹ It is particularly applicable to large-scale processing activities that aim to process a large amount of personal data. However, if medical physicians or lawyers process the personal data of their patients or clients, a data protection impact assessment is not mandatory. Because, according to the GDPR, their personal data processing “should not be considered to be on a large scale”.³⁴² The reason of this exception can be due to the obligation of confidentiality of these professions.

When conducting the data protection impact assessment, the data controller should consult authorised data protection officers.³⁴³ The data controller or processor shall assist

³⁴⁰ GDPR Recital (86) states: “The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible [...]”. We suggest that we apply this statement even more strongly to situations of breach of personal data of children, which are significantly more sensitive and may include severe risk scenarios.

³⁴¹ GDPR, Article 35(1).

³⁴² GDPR, Recital (91).

³⁴³ GDPR, Article 35(2).

and provide enough resources to data protection officers in order for them to carry out their functions and obligations as outlined in Article 39³⁴⁴ of the GDPR.³⁴⁵

Accordingly, companies have been forming new teams for data protection and privacy operations only to assess whether personal data processing is being carried out in accordance with the GDPR and other data protection legislation.³⁴⁶ There are new online platforms (e.g., OneTrust) that data protection officers may use to create, disseminate, and analyse data protection impact assessments using pre-built templates, including questions regarding the scope, purpose context and nature of that process for better comprehension, which helps to estimate the risk score of the new project, asset, or product.³⁴⁷

Before processing personal data, the data controller shall consult the supervisory authority if the data protection impact assessments indicate that the processing would pose a high risk. If the supervisory authority opines that the proposed data processing might breach the GDPR, they must provide written advice within eight weeks of receiving the consultation request, and this time period can be extended by up to six more weeks considering the complexity of the planned data processing.³⁴⁸

Data protection impact assessments are an essential component of data protection by design and by default. For example, data protection officers and data controllers can use data protection impact assessments to establish the technical and organizational measures to put in place to limit the risks of the proposed processing. Unlike the privacy by design principle,

³⁴⁴ GDPR, Article 39:” The data protection officer shall have at least the following tasks:

- (a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
- (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- (c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
- (d) to cooperate with the supervisory authority;
- (e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.”

³⁴⁵ GDPR, Article 38(2).

³⁴⁶ If we search on LinkedIn or other job search platforms, we may come across several announcements for open positions such as data protection/privacy officer, data privacy specialist, privacy operations specialist, and so on: LinkedIn, Privacy Officer jobs in Hungary, <https://www.linkedin.com/jobs/search/?geoId=100288700&keywords=privacy%20officer&location=Hungary> (last visited 10 March 2023).

³⁴⁷ For more information about OneTrust platform and their automated data protection impact assessment system: OneTrust, products> PIA and DPIA Automation, <https://www.onetrust.com/products/pia-and-dpia-automation/> (last visited 10 March 2023).

³⁴⁸ GDPR, Article 36 (1) and (2).

the data protection impact assessment is only necessary, when there is a high risk to the data subjects' rights and freedoms. However, it would be preferable if data protection impact assessments were performed in any case, just to be on the safe side.³⁴⁹

There is a long list of risks to natural persons' rights and freedoms in GDPR Recital (75), including physical, material, and non-material damage, and it is explicitly stated that the risk may result from data processing, especially where vulnerable natural persons' personal data, particularly children's personal data, is processed. As a result, while dealing with children's data, the data protection impact assessment should be carried out with extra care, because the processing is likely to be high risk in this case.³⁵⁰

Furthermore, when analysing the processing of children's data, data controllers, data processors and data protection officers should also consider the children's age, maturity, and capacities. However, their capacities are not fixed, but rather evolve as a result of their age and other environmental circumstances. As a result, while assessing the data protection impact, measurements must be revised based on children's short and long-term development.³⁵¹

The term “operator” is used instead of “data controller” in the COPPA. The operator is defined as:

“...any person who operates a Web site located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such Web site or online service, or on whose behalf such information is collected or maintained, or offers products or services for sale through that Web site or online service, where such Web site or online service is operated for commercial purposes involving commerce among the several States or with 1 or more foreign nations; in any territory of the United States or in the District of Columbia, or between any such territory and another such territory or any State or foreign nation; or between the District of Columbia and any State, territory, or foreign nation.”³⁵²

³⁴⁹ ICO, Data protection by design and default, How does data protection by design and by default link to data protection impact assessments (DPIAs)?, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/#:~:text=A%20DPIA%20is%20a%20tool,by%20design%20and%20by%20default>. (last visited 10 March 2023).

³⁵⁰ GDPR, Recital (75).

³⁵¹ United Nations Committee on the Rights on the Child (2013) General Comment No. 14 on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1). CRC/C/GC/14, p. 18, para. 84. See also: Simone van der Hof and Eva Lievens: The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR, Communications law 23.1 (2018), 20.

³⁵² 16 CFR COPPA 312.2 “Operator”.

The term “processor” does not appear in the COPPA, but they are defined as “an agent or service provider of the operator” who collects or maintains personal information on behalf of the operators.³⁵³

The first obligation of operators under the COPPA is to post a privacy policy on their websites outlining their practices with children's personal information collected online. The description should go into detail regarding how they will use and disclose this information.³⁵⁴ The regulation does not specify a way for doing so.

In our opinion, it would be ideal if the privacy policy included some vivid graphics that a child could comprehend and be attracted to read. There may be videos for younger children that explain collection procedures and their consequences so that the children may also have a comprehension of the operators' process.

Second, before collecting information from children, operators should provide direct notification to parents and get verifiable parental consent from them.³⁵⁵ There are, however, several exceptions to these prior parental consent requirements. For example, if the operator's sole purpose for collecting a child's or parent's information is to alert the parents about the collection, the operator does not need to get parental consent beforehand. They should erase this contact information if they do not get parental consent within a reasonable time.³⁵⁶ However, the duration in this phrase is vague, because everyone has a different understanding of what "reasonable" duration means. Other examples would be the collecting of a child's e-mail address in order to respond to a child's request³⁵⁷ or for the child's safety³⁵⁸. If the operator believes that the child's safety is in jeopardy, they should use all reasonable efforts to reach out to the parents and inform them about the risks.³⁵⁹

Nonetheless, reasonable efforts are likewise a vague phrase in this context, as it is in Article 8 of the GDPR.³⁶⁰ Because, for example, some website operators may interpret reasonable efforts as searching for parents on social networking services and giving up if they are unable to locate their account there.

³⁵³ 16 CFR COPPA 312.2 “Operator” (1) and (2).

³⁵⁴ 16 CFR COPPA 312.3(a).

³⁵⁵ 16 CFR COPPA 312.4(a)(b).

³⁵⁶ 16 CFR COPPA 312.5(c)(1).

³⁵⁷ 16 CFR COPPA 312.5(c)(3).

³⁵⁸ 16 CFR COPPA 312.5(c)(5).

³⁵⁹ 16 CFR COPPA 312.5(c)(5).

³⁶⁰ GDPR, Article 8(2): “The controller shall make *reasonable efforts* to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.”

Third, the operator shall provide parents the choice of providing consent for the collection of their children's data without giving consent for the disclosure of such data to third parties.³⁶¹ Fourth, the operator guarantees that parents have access to their children's personal data in order to review and/or delete it.³⁶²

Fifth, operators should provide parents with the option to restrict future use or collection of their children's personal information.³⁶³ It is beneficial for the children that their parents have this level of control over their personal information. However, one question remains unanswered: Wouldn't it be better if children had also control over their data, if they have the capability and maturity to do so?

Undoubtedly, an online service provider cannot measure a child's capability or maturity. However, if a child requests erasure of his or her personal data, prohibits future use of his or her data, or prohibits disclosure of his or her personal data, providers may assume that the child should have the capacity to manage their data. In this instance, we argue that the online service provider should erase the data immediately without waiting for the parents' reaction. It is because, in the usual course of events, deletion, restriction of usage, or restriction of disclosure should not be harmful to children.

Sixth, the operators should keep the information they gather from children confidential, secure, and intact. This requirement includes disclosing the children's collected information to parties they trust with the same level of confidentiality and security.³⁶⁴ Nevertheless, it should be critical to obtain parental consent before disclosing information. Even if the third party whom the operator trusted and released the information is trustworthy for the operator, they might not be trustworthy for the parents. Thus, in our point of view, it is critical to notify the parents ahead of time and obtain their consent before releasing the child's personal data.

The seventh obligation of operators under the COPPA is consistent with the GDPR's purpose limitation.³⁶⁵ The operator shall only keep the obtained information for as long as it is required for the purpose for which it was collected in the first place.³⁶⁶ Finally, the eighth obligation of operators under the COPPA is consistent with the GDPR's data minimisation principle.³⁶⁷ It is prohibited for operators to condition children's participation in a game or

³⁶¹ 16 CFR COPPA 312.5(a)(2).

³⁶² 16 CFR COPPA 312.6(a).

³⁶³ 16 CFR COPPA 312.3(c).

³⁶⁴ 16 CFR COPPA 312.8.

³⁶⁵ GDPR Article 5(1)(b).

³⁶⁶ 16 CFR COPPA 312.10.

³⁶⁷ GDPR Article 5(1)(c).

other online activities on disclosing more information about the children than is required to engage in such activity.³⁶⁸ For example, if the game simply requires a nickname to join, the operators cannot ask for further information such as the children's full name, e-mail address, or any other identifying information.

Comparing the two approaches, it is evident that the GDPR is more comprehensive and detailed in terms of data controller obligations since data controllers shall protect the personal data of data subjects by making it possible and easy for data subjects to exercise their rights, cooperating with supervisory authorities when necessary, and conducting data protection impact assessments to reduce the risks of processing. However, the GDPR lags behind in terms of data controllers' obligation for children's data protection.

The GDPR makes some distinctions between data subjects as adults and data subjects as children (e.g., data controllers should conduct a data protection impact assessment with additional care when processing children's data and shall make all reasonable efforts to get parental consent before processing the personal data of children); yet children require more special protection since they fall into a more vulnerable category of data subjects.

As stipulated by the legally binding United Nations Convention on the Rights of the Child (UNCRC), *"In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities, or legislative bodies, the best interests of the child shall be the primary consideration,"*³⁶⁹ and the data controller is not exempt from this requirement. Despite the fact that GDPR does not explicitly refer to this aspect, all the EU member states have signed and ratified the UNCRC, therefore it must be considered when processing children's personal data.

Hence, it would be ideal to have a dedicated GDPR article that lists solely the data controller's child-specific obligations based on the children's data protection rights and provides data controllers with guidance on how and when to interact children directly. As indicated previously, if a child is mature enough to request the deletion of his/her data, the data controllers may assume that they can directly communicate to the child instead of the parents. Accordingly, this approach is feasible for all online child activities with low risk. For instance, children may request the termination of the transfer of their data to third countries without the consent of their parents. For riskier actions, such as sharing content on

³⁶⁸ 16 CFR COPPA 312.7.

³⁶⁹ UNCRC, Article 3(1).

publicly available websites or transferring data, data controllers may still seek parental consent.³⁷⁰

Unlike the GDPR, all the obligations of the operators under the COPPA are related to the protection of children's privacy and how the operators should ensure parental control over their children's personal data. It is obviously advantageous when the children are young and unable to make decisions or comprehend the consequences of personal data processing. Nonetheless, the children should be allowed to undertake less risky activities such as removing data from a website, unsubscribing, or prohibiting the transfer of personal data to third parties without parental consent if they have the capacity and willingness to do so.³⁷¹

Consequently, operators under the COPPA and data controllers under the GDPR should at the very least provide these opportunities to children who wish to control their data and make less risky decisions about their online activities.

Furthermore, we propose that the COPPA should oblige operators to collaborate with supervisory authorities and impose data protection or privacy impact assessments for the processing of children's personal data, as the GDPR does. Because processing children's personal data would almost certainly pose a high risk, it would benefit the children, if operators collaborated with supervisory authorities and conducted data protection/privacy impact assessments through specialist data protection/privacy officers to enable to detect, assess, and mitigate risks before processing their personal data.

5.1 Short Summary

Chapter 5 examined data controller's obligations under the GDPR and operator's obligations under the COPPA comparatively. We claimed that the GDPR doesn't sufficiently address data controllers' obligations to process children's personal data. Accordingly, we suggested a GDPR article that includes only the data controller's child-specific obligations based on children's data protection rights.

Whereas the COPPA particularly addresses the obligations of operators regarding processing children's personal data. Yet, COPPA only requires operators to engage with parents to protect children's personal data. We proposed that operators provide children

³⁷⁰ Data Protection Commission Ireland, Children Front and Centre, Fundamentals for a Child-Oriented Approach to Data Processing-Draft Version for Public Consultation, December 2020, 33-35.

³⁷¹ Data Protection Commission Ireland, Children Front and Centre, Fundamentals for a Child-Oriented Approach to Data Processing-Draft Version for Public Consultation, December 2020, 33-35.

(when mature enough) control over their data, particularly when it comes to activities like erasing or restricting transfers to third parties/countries.

We also suggested that data controllers should collaborate with supervisory authorities and always conduct data protection/privacy impact assessments via data protection/privacy officers to detect, analyse, and mitigate risks before processing children's personal data. We justified this suggestion by asserting that processing children's personal data would almost certainly pose a high risk owing to children's vulnerability.

Furthermore, data controllers have an additional important responsibility under the GDPR. Personal data transfers to third countries can only occur if data controllers comply with the criteria outlined in Chapter 5 of the GDPR. In Chapter 6, all the requirements and responsibilities of data controllers will be thoroughly examined. The value of Chapter 6 in the literature resides in its contribution to a very critical subject that neither policymakers nor scholars are sufficiently interested in. We have not yet found a study in the literature that discusses data transfers including children's personal data. Nevertheless, in our research, while investigating data transfers, we will not disregard the transfer of children's personal data to third countries, particularly the US.

6. Trans-Atlantic data transfers involving child data in the EU

This chapter will discuss GDPR-compliant transfers of personal data to third countries. Transfers of personal data are only possible if data controllers meet the requirements established in Chapter 5 of the GDPR. We will analyse in depth all the obligations of data controllers surrounding the transfer of personal data from the EU to third countries, particularly the US. More importantly, we will also explore a topic that does not get sufficient concern from lawmakers or academics: the transfer of children's personal data.

In addition to evaluating the data transfer rules and Transatlantic data transfers of the past and present, we will also explore issues around the transfer of children's personal data. We will examine how the differing age thresholds will affect the transfer of children's data within the EU and to the US. In addition, we will investigate if the GDPR or the Commission's adequacy decisions include any requirements specific to children. We will provide recommendations for future transatlantic data transfers including the solutions for transfer of children's personal data.

We have noted in earlier chapters that the reason we chose US legislation to compare with EU legislation is because privacy was founded and initially developed in the US. Thus, the EU was influenced, but privacy and data protection evolved in a different, more comprehensive way under the EU legal system. Nonetheless, when it comes to data transfers, we must also specify another reason to compare the data transfers of the two jurisdictions, that is their robust economic collaboration.

The US has been the EU's greatest commercial partner, and the EU and the US have the largest bilateral trade and investment cooperation and the most integrated economic relationship in the world.³⁷² Moreover, the digital economy is an integral aspect of this economic relationship and the personal data flows are vital components of the global digital economy. While their approaches to data flows vary, none of them can afford to impede transatlantic data flows. Thus, negotiations on the free flow of personal data from the EU to the US have been proceeding.

³⁷² European Commission, Trade, EU trade relationships by country/region, Countries and Regions, United States, https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/united-states_en#:~:text=The%20European%20Union%20and%20the,and%20investment%20partner%20by%20far (last visited 26 February 2023)

The EU and the US regard the personal data and data flows differently because of their differing approaches to privacy and data protection.³⁷³ On one hand, personal data is regarded as a commercial commodity in the US³⁷⁴ and there is a sectoral approach, enacting limited legislation that only applies to specific targets.³⁷⁵ This allows for a significant deal of flexibility and freedom in US privacy legislation, since one sector might define privacy and data protection substantially different than the other sectors. However, in this instance, some sectors may be unregulated, if no legislation is in place to protect them.

Furthermore, because each state in the US has the power to adopt its own privacy regulations, more sector-specific laws such as the Biometric Information Privacy Act (BIPA)³⁷⁶ of Illinois or more general laws such as the California Consumer Privacy Act (CCPA)³⁷⁷ can be implemented in different states. These disparities in standards may have a negative impact on the European Commission's decision to consider the US to have an adequate level of data protection,³⁷⁸ as required by the GDPR.³⁷⁹

The EU, on the other hand, considers privacy and data protection to be fundamental rights and places a high value on them.³⁸⁰ Hence, the EU has established a comprehensive regulation called the GDPR after a long decision-making process in order to protect individuals' data protection rights and privacy, while also regulating the free flow of personal data.³⁸¹ As it is stated in the Recital (101) of the GDPR: "Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation."³⁸² However, data transfers from the EU

³⁷³ Emily Linn: A Look into the Data Privacy Crystal Ball: A Survey of Possible Outcomes for the EU-US Privacy Shield Agreement, *Vand. J. Transnat'l L.* 50, (2017), 1312-1313.

³⁷⁴ Paul M. Schwartz and Karl-Nikolaus Peifer: Transatlantic Data Privacy Law 106 *Geo. L.J.* (2017) 132-137 cited in Paul M. Schwartz: *Global Data Privacy: The EU Way* 94 *NYUL Rev.* (2019) 771-773.

For more information on the US approach, which considers privacy and personal data protection as a commodified property right, and the EU approach, which treats privacy and data protection as a noncommodified human right, see the following sources: Margaret Jane Radin: Incomplete commodification in the computerized world In Niva Elkin-Koren and Neil Weinstock Netanel (eds.): *The commodification of information*, The Hague: Kluwer Law International (2002), 17-18 cited in Corien Prins: *When Personal Data, Behavior and Virtual Identities Become a Commodity: Would a Property Rights Approach Matter*, *SCRIPTed: A Journal of Law, Technology and Society* 3, no. 4 (2006), 280.

³⁷⁵ Emily Linn: A Look into the Data Privacy Crystal Ball: A Survey of Possible Outcomes for the EU-US Privacy Shield Agreement, *Vand. J. Transnat'l L.* 50, (2017), 1316.

³⁷⁶ Biometric Information Privacy Act (BIPA) of 2018, 740 *ILL. COMP.STAT.* 14/1-99.

³⁷⁷ California Consumer Privacy Act (CCPA) of 2018, *CAL. CIV.CODE* §§ 1798.100-1798.199.100.

³⁷⁸ Emily A. Ivers: Using State-Based Adequacy Now, National Adequacy over Time to Anticipate and Defeat Schrems III, 62 *BC L Rev.* (2021) 2589-2591.

³⁷⁹ GDPR, Article 45(1).

³⁸⁰ Charter of Fundamental Rights of the European Union, OJ C 326, 26.12.2012, p. 391-407, Article 7-8.

³⁸¹ GDPR, Article 1(1) and (2).

³⁸² GDPR, Recital (101).

to third countries, including the US, are only possible, if those countries have an adequate level of data protection that is acknowledged and approved by the European Commission.³⁸³

As mentioned above, regardless of their legislation and approaches to personal data, they've spent several years negotiating free data flow agreements. First, the US was granted partial adequacy by Safe Harbour in 2000,³⁸⁴ but it lasted until the European Court of Justice (CJEU) invalidated it in 2015 with the Schrems I. case.³⁸⁵ Following that the Privacy Shield, the Safe Harbour's heir, entered into force in 2016.³⁸⁶ Likewise, it was invalidated by the CJEU in 2020 with the Schrems II. case³⁸⁷.

Furthermore, on March 25, 2022, the European Commission and the United States announced a new agreement in principle on a joint statement on the Trans-Atlantic Data Privacy Framework. This new framework seeks to address the shortcomings of the Safe Harbour and Privacy Shield systems, as well as the issues presented in both Schrems cases. Their objective is to reach an agreement that will not be invalidated by the CJEU, as previous agreements were.³⁸⁸ All agreements for free data flow from the EU to the US that were in place and may be in place in the future will be thoroughly investigated in this chapter. But first, the GDPR's requirements for data transfers to third countries or international organizations will be examined.

Although data transfers to countries outside the EU and to international organizations are substantial and necessary for the growth of international relations and the economy, they have prompted concerns about the data protection of EU residents and citizens.³⁸⁹ Therefore, all provisions in the GDPR's chapter on data transfers should be followed in order to ensure

³⁸³ GDPR, Article 45.

³⁸⁴ Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215, 26.07.2000, p. 7-47.

³⁸⁵ Case C-362/14 Maximilian Schrems v Data Protection Commissioner EU:C:2015:650.

³⁸⁶ Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207/1, 12.07.2016, 1-112.

³⁸⁷ Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems EU:C:2020:559.

³⁸⁸ European Commission: European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework (25 March 2022) https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087 (last visited 10 March 2023). For more information: European Commission: Trans-Atlantic Data Privacy Framework (25 March 2022) https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100 (last visited 10 March 2023).

³⁸⁹ GDPR, Recital (101).

that the degree of protection of natural persons granted by this Regulation is not jeopardized by controllers and processors.³⁹⁰

According to Article 45 of the GDPR, data transfers to a third country or an international organisation are only possible, if the European Commission decides that the third country or international organization provides an adequate level of data protection, as required by Regulation. If the European Commission determines that the third country or international organisation provides an adequate level of protection, no further authorisation is required for the transfer.³⁹¹

The European Commission should consider first the rule of law, respect for individuals' human rights and freedoms in that country, relevant legislation, such as public defence, criminal law, and national security, and the implementation of these legislations when assessing the adequate level for countries and international organisations. Moreover, data protection requirements should be in place in that country, such as restricted onward transfers to third countries or international organisations, proper data subject rights, and effective remedies and judicial redress mechanism where there is a violation of such data subject rights.³⁹²

Second, the European Commission should consider whether the third country to which the data would be transferred has an independent supervisory authority. This supervisory authority should be responsible for ensuring that data protection rules are followed as well as assisting data subjects in exercising their data protection rights. The supervisory authority should also cooperate with supervisory authorities in EU Member States.³⁹³

Third, the European Commission should take into account the third country's or international organisation's international commitments or legally binding agreements. It should also be considered whether they have any additional obligations regarding personal data protection as a result of their involvement in multilateral or regional systems.³⁹⁴ For example, the European Commission issued the United Kingdom (UK) an adequacy decision after it becomes a third country following Brexit on June 28, 2021³⁹⁵ especially because the UK has earned their trust owing to its continued adherence to

³⁹⁰ GDPR, Article 44.

³⁹¹ GDPR, Article 45(1).

³⁹² GDPR, Article 45(2)(a).

³⁹³ GDPR, Article 45(2)(b).

³⁹⁴ GDPR, Article 45(2)(3).

³⁹⁵ Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom under the Act on the Protection of Personal Information, OJ L 360, 11.10.2021, p. 1-68.

“[...] the jurisdiction of the European Court of Human Rights and [...] European Convention of Human Rights³⁹⁶ as well as to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data³⁹⁷, which is the only binding international treaty in the area of data protection”.³⁹⁸

Given the aforementioned strict requirements, only a few countries have been deemed competent thus far. Andorra, Argentina, Canada (commercial organisations), the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, the Republic of Korea, Switzerland, the United Kingdom, and Uruguay are among these countries. Since it solely applies to commercial organizations and does not extend to the entire Canadian jurisdiction, the adequacy decision should be regarded as a partial adequacy decision.³⁹⁹

Furthermore, it does not necessarily ensure that the domestic data protection law of these countries, which the European Commission has recognized as providing adequate protection, has attained this level of adequacy. Because, for example, Japanese data protection law, the Act on the Protection of Personal Information (APPI),⁴⁰⁰ applies higher standards to EU data subjects' personal data than to its own citizens and residents. In this context, we might also question whether the US can attain the adequacy decision, if it follows Japan's model and develops a system that meets higher standards for EU residents and citizens than for its own residents and citizens.⁴⁰¹ We will discuss if such a two-way approach can be an option for the United States later in this chapter.

If there is no adequacy decision in place, it is still possible to transfer personal data from the EU to a third country under the GDPR, if the data controller or processor provides appropriate safeguards, and if data subjects have rights that are enforceable as well as

³⁹⁶ Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, https://www.echr.coe.int/documents/convention_eng.pdf (last visited 10 March 2023).

³⁹⁷ Council of Europe (2018) Convention 108 + [2018] ETS 108 https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf (last visited 10 March 2023).

³⁹⁸ European Commission: Data protection: Commission adopts adequacy decisions for the UK (28 June 2021) https://ec.europa.eu/commission/presscorner/detail/ro/ip_21_3183 (last visited 10 March 2023).

³⁹⁹ European Commission: Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection' (13 January 2018) https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited 10 March 2023).

⁴⁰⁰ Personal Information Protection Commission: Amended Act on the Protection of Personal Information (Tentative Translation) (June 2020) https://www.ppc.go.jp/files/pdf/APPI_english.pdf (last visited 10 March 2023).

⁴⁰¹ Flora Y. Wang: Cooperative Data Privacy: The Japanese Model of Data Privacy and the Eu-Japan GDPR Adequacy Agreement 33 Harv. JL & Tech. (2020) 690-691.

effective legal remedies are in place.⁴⁰² Article 46 of the GDPR states that appropriate safeguards may include binding corporate rules (BCRs), standard contractual clauses (SCCs), certification mechanisms, and codes of conduct.⁴⁰³ While BCRs and SCCs are primarily aimed at controllers and processors that export personal data from the EU to third countries (e.g., the US), the certification system and codes of conduct were designed for controllers and processors in third countries that are not subject to the GDPR. Not the data exporter, but the data importer established in a third country may apply for and get certification and codes of conduct mechanisms.⁴⁰⁴

Moreover, if neither an adequacy decision nor appropriate safeguards exist, it may be allowed to transfer personal data to a third country or international organisation, if one of the exceptions listed in Article 49 of the GDPR applies. These exceptions include the following: the data subject has expressly consented to the transfer after being informed of the possible risks and consequences of such a transfer; there is a contract between the data subject and the controller; the transfer is necessary for reasons of public interest; or the transfer is necessary to protect the vital interests of the data subject, or another person and the data subject cannot consent to the transfer.⁴⁰⁵

However, the derogations stated in Article 49 cannot be utilised in any way that would involve the transfer of data in a repeated manner. These exceptional data transfers will only be accepted in specific circumstances, on an occasional basis, where absolutely necessary for a certain purpose.⁴⁰⁶ Accordingly, the transfer of personal data even the personal data with sensitive nature must be legal if, for example, an EU data subject is unconscious and in need of urgent medical care while travelling outside of the EU, and only a data exporter (for example, his regular doctor) based in a member state of the EU can offer some information regarding his/her health conditions. In this scenario, the transfer of these data would be legal.

⁴⁰² GDPR, Article 46(1).

⁴⁰³ GDPR, Article 46(2)(a-f).

⁴⁰⁴ For more information about the certification mechanism: EDPB, Guidelines 07/2022 on certification as a tool for transfers, version 1.0, 14 June 2022, 1-19. https://edpb.europa.eu/system/files/2022-06/edpb_guidelines_202207_certificationfortransfers_en_1.pdf (last visited 10 March 2023). For more information about the codes of conducts: EDPB, Guidelines 04/2021 on codes of conduct as tools for transfers, 2021, 1-14. https://edpb.europa.eu/system/files/2021-07/edpb_guidelinescodesconducttransfers_publicconsultation_en.pdf (last visited 10 March 2023).

⁴⁰⁵ GDPR, Article 49(1) (a-g).

⁴⁰⁶ GDPR, Recital 111 and Guidelines 2/2018 of the European Data Protection Board (EDPB) on derogations of Article 49 under Regulation 2016/679 7 (May 25, 2018), 4-5. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf (last visited 10 March 2023).

The reason for this is that the rule presupposes that the risk of possible harm to the data subject should be greater than the concerns for data protection.⁴⁰⁷

Until the EU-US agreement on principle for a new Trans-Atlantic Data Privacy Framework enters into force, EU data exporters may only transfer personal data to the US using appropriate safeguards, such as Binding Corporate Rules (BCRs) and Standard Contractual Clauses (SCCs) under Article 46 of the GDPR for ongoing and repeated transfers, as derogations under the Article 49 would only apply in exceptional and specific cases.

In this chapter, we will explore the previous US adequacy decisions, Safe Harbour and Privacy Shield, before analysing the current methods for transferring personal data from the EU to the US. After these, we will discuss the new agreement in principle and whether the US can finally be deemed adequate or whether this agreement will be merely politically accepted. Furthermore, in which case it will share the same fate as previous adequacy decisions and whether Schrems III case will occur. In addition to evaluating countries with adequacy decisions, we will offer our opinions and suggestions on whether and how the US may achieve an adequate level of data protection.

In addition, the current state of data exports from the EU concerning children in legal texts and in practice will be a central topic of discussion. Accordingly, we will analyse the legislations as well as several real-world examples to demonstrate whether Internet sites address the transfer of children's data specifically. The varying ages at which children may offer consent on digital platforms may potentially impact data transfer difficulties, therefore we aim to investigate this as well. In such a circumstance, we may discuss solutions to the problem. We would like to raise awareness in the doctrine, because we have not discovered any literature which is directed on the transfer of children's data throughout our research.

⁴⁰⁷ Guidelines 2/2018 of the European Data Protection Board (EDPB) on derogations of Article 49 under Regulation 2016/679 7 (May 25, 2018), 12.
https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf (last visited 10 March 2023).

6.1 Safe Harbour

Similar to the GDPR, the previous EU Directive 95/46/EC required an adequate level of protection for data transfers to third countries under Article 25.⁴⁰⁸ In accordance with Article 25(1) of Directive 95/46/EC, the Commission decision 2000/520/EC certified that the EU-US data transfer framework, known as Safe Harbour, provided an adequate level of protection for EU data subjects whose personal data were transferred to US companies or organisations that voluntarily chosen to comply with Safe Harbour's principles.⁴⁰⁹

A company in the US that received personal data from the European Union, was required to adhere to the Safe Harbour privacy principles, which were as follows: notice, choice, onward transfer, security, data integrity, access, and enforcement.⁴¹⁰ Any US company that submitted a self-certification to the Department of Commerce confirming that it followed Safe Harbour principles, would be eligible for such benefits of free data flow from the EU towards their US-based company. Companies could self-certify for the Safe Harbour by sending a letter to the Department of Commerce (or its designee) that includes the following information at a minimum: the company's name, contact address, activities related to personal data received from the EU, and a description of the organization's privacy policy for such personal data.⁴¹¹ Besides, all companies that self-certified their compliance

⁴⁰⁸ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50, Article 25(1).

⁴⁰⁹ Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215, 26.07.2000, pp. 7-47.

⁴¹⁰ Safe Harbour, Annex I- Safe Harbour Privacy Principles, 11-12. “Notice- An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. Choice- An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party (1) or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice. Onward Transfers- To disclose information to a third party, organizations must apply the Notice and Choice Principles. Security- Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction. Data Integrity- Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. Access- Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate. Enforcement- Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed.”

⁴¹¹ Safe Harbour, FAQ 6-Self Certification, 15.

“1. name of organization, mailing address, e-mail address, telephone and fax numbers;

with the Safe Harbour principles, should have made that fact clear in their published privacy policies.⁴¹²

Although the self-certified companies asserted that they complied with the Safe Harbour principles, only 348 businesses out of a total of 1,597 met even the most fundamental requirements of the Safe Harbour framework, such as being in compliance with the concept of enforcement set forth in the seventh principle.⁴¹³ According to the enforcement principle of the Safe Harbour, effective privacy protection must include mechanisms for ensuring compliance with the principles. If a data breach has occurred as a result of noncompliance with the principles, recourse mechanisms should be available for individuals whose data have been compromised, sanctions should be available for organisations that did not comply with the principles, and those organisations should also address problems of data integrity.⁴¹⁴

However, it was discovered that the United States National Security Agency (NSA) gathers internet communications from several US internet companies, including Google, Facebook, and Microsoft, using a programme with the codename PRISM. *Edward Snowden*, a whistle-blower, revealed facts regarding the NSA's monitoring programme in 2013.⁴¹⁵

In reaction to the revelations that were provided by Edward Snowden, the privacy advocate *Max Schrems* has lodged a complaint with the Irish Data Protection Commission. This is the case as a result of the fact that Facebook's Irish subsidiary transfers part or all of the information that Mr. Schrems provided to Facebook to servers located in the United States, where it is processed. The issue of Mr. Schrems was that the United States does not provide an adequate level of protection against the public surveillance of the data that is

2. description of the activities of the organization with respect to personal information received from the EU; and 3. description of the organization's privacy policy for such personal information, including: (a) where the privacy policy is available for viewing by the public, (b) its effective date of implementation, (c) a contact office for the handling of complaints, access requests, and any other issues arising under the safe harbor, (d) the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the annex to the Principles), (e) name of any privacy programs in which the organization is a member, (f) method of verification (e.g. in-house, third party) (1), and (g) the independent recourse mechanism that is available to investigate unresolved complaints.”

⁴¹² Safe Harbour, FAQ 7-Verification, 16.

⁴¹³ Cunningham McKay: Complying with International Data Protection Law, *University of Cincinnati Law Review* 84, no. 2 (2016), 446-447. See the study: Chris Connolly: The US Safe Harbor - Fact or Fiction?, *Galexia* (2008), 7-8.

https://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/08_galexia_safe_harbor_/08_galexia_safe_harbor_en.pdf (last visited 10 March 2023).

⁴¹⁴ Safe Harbour, Annex I Safe Harbour Privacy Principles, Enforcement, 12.

⁴¹⁵ BBC News, Edward Snowden: Leaks that exposed US spy programme, 17 January 2014, <https://www.bbc.com/news/world-us-canada-23123964> (last visited 10 March 2023).

transferred to that country. However, the Irish Data Protection Commissioner rejected, stating that the Safe Harbour covered the transfers.⁴¹⁶

When Mr. Schrems filed an appeal against the ruling, the European Court of Justice was consulted. Finally, the CJEU clarified that while self-certified US companies were required to comply with the Safe Harbour principles, US public authorities were not. It should have been guaranteed that the US government's surveillance was restricted to what was required for national security, and following the data leak, there should have been appropriate legal remedies for individuals whose data protection and privacy rights were breached.⁴¹⁷

However, these were not something that self-certified companies could accomplish themselves without the enforcement policies and procedures that are enforced by the government. In addition, the Commission's adequacy decision does not prevent national supervisory authorities in Member States from querying whether the framework is compatible with the protection of privacy, fundamental rights, and individual freedoms.⁴¹⁸ Since the abovementioned conditions did not meet the expectations of the GDPR's adequacy level of data protection, the CJEU declared that the Safe Harbour framework was invalid.⁴¹⁹

6.2 Privacy Shield

Following the invalidation of Safe Harbour, the EU and the US decided to replace it with a new framework known as Privacy Shield. The European Commission issued an adequacy decision on the Privacy Shield on July 12, 2016.⁴²⁰ In other words, companies may have only been considered adequate, if they agree to self-certifying in compliance with the Privacy Shield principles. The framework included seven principles as the Safe Harbour framework did: notice, data integrity and purpose limitation, choice, security, access, recourse, enforcement and liability, and accountability for onward transfer.⁴²¹

⁴¹⁶ Court of Justice of the European Union, The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid, Press Release, 117/15, Judgment in Case C-362/14 Maximilian Schrems v Data Protection Commissioner, 6 October 2015, 1.

⁴¹⁷ Case C-362/14 Judgment of the Court (Grand Chamber) of 6 October 2015 Maximilian Schrems v Data Protection Commissioner ECLI:EU:C:2015:650, para 82 et seq.

⁴¹⁸ Court of Justice of the European Union, The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid, Press Release, 117/15, Judgment in Case C-362/14 Maximilian Schrems v Data Protection Commissioner, 6 October 2015, 2.

⁴¹⁹ Case C-362/14 Judgment of the Court (Grand Chamber) of 6 October 2015 Maximilian Schrems v Data Protection Commissioner ECLI:EU:C:2015:650, para 107/2.

⁴²⁰ Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207/1, 12.07.2016, 1-112.

⁴²¹ Privacy Shield, para 19 et seq.:

Unlike Safe Harbour, there were also supplemental principles that self-certifying companies should follow. The supplemental principles include, but are not limited to, sensitive data processing, the function of Data Protection Authorities, the Federal Trade Commission's activities related to dispute resolution and enforcement, and restrictions regarding access requests by public authorities.⁴²² As a result, if US companies implemented the Privacy Shield framework's principles and registered their certification, they might have achieved an adequate level and transferred European data subjects' data from the EU to the US without additional processes.⁴²³

In comparison to the Safe Harbour, there were new redress mechanisms: data subjects may have filed complaints directly to the self-certified company, which provided specific remedies. Furthermore, the US authorities assured the European Commissioner that they would only allow intelligence agencies access to personal data in exceptional circumstances and *as tailored as feasible*. Furthermore, the European Commission welcomed the new Ombudsperson role, which was independent of the US intelligence community. The Ombudsperson was required to respond to individual complaints with either confirmation of compliance or remediation of non-compliance, depending on the nature of the complaint.⁴²⁴

“Notice: Organisations are obliged to provide information to data subjects on a number of key elements relating to the processing of their personal data (e.g., type of data collected, purpose of processing, right of access and choice, conditions for onward transfers and liability).

Choice Principle: Where a new (changed) purpose is materially different but still compatible with the original purpose, this principle gives data subjects the right to object (opt out).

Data Integrity and Purpose Limitation: Personal data must be limited to what is relevant for the purpose of the processing, reliable for its intended use, accurate, complete, and current.

Security Principle: Organisations creating, maintaining, using or disseminating personal data must take ‘reasonable and appropriate’ security measures, taking into account the risks involved in the processing and the nature of the data.

Access Principle: Data subjects have the right, without need for justification and only against a non-excessive fee, to obtain from an organisation confirmation of whether such organisation is processing personal data related to them and have the data communicated within reasonable time.

Recourse, Enforcement and Liability Principle: Participating organisations must provide robust mechanisms to ensure compliance with the other Principles and recourse for EU data subjects whose personal data have been processed in a non-compliant manner, including effective remedies.

Accountability for Onward Transfer Principle: Any onward transfer can only take place (i) for limited and specified purposes, (ii) on the basis of a contract (or comparable arrangement within a corporate group and (iii) only if that contract provides the same level of protection as the one guaranteed by the Principles, which includes the requirement that the application of the Principles may only be limited to the extent necessary to meet national security, law enforcement and other public interest purposes.”

⁴²² Privacy Shield, Annex II.III.1-16.

⁴²³ GDPR, Article 45(1).

⁴²⁴ EPRS, Update on the state of play of the EU-US data transfer rules, Members' Research Service, 14-20. [https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/625151/EPRS_IDA\(2018\)625151_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/625151/EPRS_IDA(2018)625151_EN.pdf) (last visited 10 March 2023).

After the judgement that invalidated Safe Harbour, on December 2, 2015, Mr. Schrems revised his complaint, stating that his transferred personal data is not adequately protected in the United States, and he sought to prohibit his data transfer to the United States, not only on the basis of an adequacy decision, but also on the basis of SCCs. The Irish regulatory agency filed the issue before the High Court (Ireland).⁴²⁵

The High Court inquired as to whether the GDPR applies to data transfers via SCCs in accordance with Decision 2010/87, and if so, what level of protection is necessary for such transfers, as well as the function of the supervisory authorities in such cases. The High Court also questioned the validity of both Decision 2010/87⁴²⁶ and Decision 2016/1250⁴²⁷ (Privacy Shield).⁴²⁸

The Court of Justice ruled on 16 July 2020 that first of all, the GDPR applies to all data transfers for commercial purposes from one operator in a Member State to another operator in a third country. Second, the level of protection required by the GDPR is essentially equivalent to the level of protection granted within the EU by the GDPR and the EU Charter of Fundamental Rights. Thirdly, the Court of Justice ruled that the supervisory authorities should suspend or prohibit the data transfer if the SCCs are not or cannot be complied with in the receiving country and the protection of the transferred data required by EU law cannot be achieved by other means.⁴²⁹

Moreover, the Court of Justice then ruled that the decision 2010/87 is not invalid because it contains effective mechanisms that enable compliance with the GDPR's required

⁴²⁵ CJEU, Judgment in Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, Press Release No 91/20, 16 July 2020, 1-3, 1-2.
<https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf> (last visited 10 March 2023).

⁴²⁶ Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 OJ L 344/ 100, 17.12.2016, p. 100-101.

⁴²⁷ Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207/1, 12.07.2016, 1-112.

⁴²⁸ CJEU, Judgment in Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, Press Release No 91/20, 16 July 2020, 1-3, 2.
<https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf> (last visited 10 March 2023).

⁴²⁹ CJEU, Judgment in Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, Press Release No 91/20, 16 July 2020, 1-3, 2.
<https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf> (last visited 10 March 2023).

adequate level of data protection and that, in the event of a breach of personal data, the transfer of data would be suspended or prohibited.⁴³⁰

However, concerns raised regarding the inadequacy of necessity and proportionality of US government surveillance authorities, the absence of an effective legal remedy for EU data subjects, and the lack of independence for the Ombudsperson. In other words, the improvements made by Privacy Shield in comparison to Safe Harbour failed to live up to expectations. Hence, the Schrems II. case ruled that the Privacy Shield did not provide the “essentially equivalent” level of data protection that is mandated by EU legislation and because of this, the Privacy Shield was deemed to be invalid.⁴³¹

6.3 The “essentially equivalent” level of data protection

There are EU Guidelines that clarify the scope of essentially equivalent level of data protection. First, the EU Working Party described it in the document titled 'Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive' (WP12).⁴³² Then, the updated version, Adequacy Referential (WP254 rev.01), improved the previous WP12 in light of the new GDPR and the Schrems cases.⁴³³

The data protection system of a third country or international organisation does not have to be identical to the data protection level established by the GDPR. The fundamental content and procedural/enforcement principles, however, should be in place.⁴³⁴ The following are the mentioned content principles: “1. Concepts, 2. Grounds for lawful and fair processing for legitimate purposes, 3. Purpose limitation principle, 4. Data quality and proportionality principle, 5. Data Retention principle, 6. Security and confidentiality principle, 7.

⁴³⁰ CJEU, Judgment in Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximilian Schrems, Press Release No 91/20, 16 July 2020, 1-3, 2-3.
<https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf> (last visited 10 March 2023).

⁴³¹ CJEU, Judgment in Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximilian Schrems, Press Release No 91/20, 16 July 2020, 1-3, 3.
<https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf> (last visited 10 March 2023).

⁴³² Working Party’s Working Document on the Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU Data Protection Directive, DG XV 1998 D/5025/98 WP12.

⁴³³ Article 29 Data Protection Working Party, Adequacy Referential, 18/EN 6 February 2018 WP 254 rev01.

⁴³⁴ WP254 rev.01, Chapter 3, p. 5.

Transparency principle, 8. Right of access, rectification, erasure, and objection and 9. Restrictions on onward transfers.”⁴³⁵

Additional content principles should be applied to specific types of processing: “1. Special categories of data, 2. Direct marketing, and 3. Automated decision making and profiling.”⁴³⁶

The following are elements of Procedural and Enforcement Mechanisms: 1. Competent Independent Oversight Authority, 2. The data protection system must ensure a good level of compliance, 3. Accountability, 4. The data protection system must provide support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms.”⁴³⁷

In addition, WP29 (Article 29 Data Protection Working Party)⁴³⁸ provided a guidance on how the public authorities of a third party should conduct their surveillance, and this guidance comprises four criteria that are considered to be essentially equivalent: “a. Processing should be based on clear, precise and accessible rules (legal basis); b. Necessity and proportionality with regards to legitimate objectives pursued need to be demonstrated; c. The processing has to be subject to independent oversight; d. Effective remedies need to be available to the individuals.”⁴³⁹

6.3.1 Content Principles

First, the concepts do not have to be identical, but they must be consistent with the GDPR's key data protection concepts. Personal data, data controller/processor, and data processing, for example, should be similar or reflective concepts. Second, the data processing should take place on a legal basis, such as where the data subject consents, where the data controller has a legitimate interest, where there is a national legislation that makes the processing legal, or where the processing is necessary for the fulfilment of a contract.⁴⁴⁰

⁴³⁵ WP254 rev.01, Chapter 3/A: Content Principles 1-9.

⁴³⁶ WP254 rev01, Chapter 3/B: Examples of additional content principles to be applied to specific types of processing 1-3.

⁴³⁷ WP254 rev01, Chapter 3/C: Procedural and Enforcement Mechanisms 1-4.

⁴³⁸ “This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC.” Directive 95/46/EC, Article 29 and 30.

⁴³⁹ WP254 rev01, Chapter 4: Essential guarantees in third countries for law enforcement and national security access to limit interferences to fundamental rights 1-4.

⁴⁴⁰ WP254 rev.01, Chapter 3/A: Content Principles 1-2.

Thirdly, the processing must be limited to a specific purpose, and the gathered data must not be used for a different, incompatible purpose. Fourth, the obtained data should be correct and kept up to date if necessary. Fifth, the data should be stored for no longer than is required for the initial purposes for which it was obtained. For instance, if an employer collects employee data, it should be retained for the duration of the work contract, unless there is a valid reason to preserve the data for a longer or shorter period of time.⁴⁴¹

Sixth, the personal data shall be handled in a manner that protects the security of personal data by technological and organisational measures, taking into account the state of the art and the current level of technology available. Seventh, each data subject shall be clearly, easily accessible, and transparently informed about the aspects of the processing of their personal data. These aspects should contain the name of the data controller, the purpose of the processing, the rights of the data subjects, and any other information that may be required for the processing to be fair. There may be exceptions to the transparency requirement, such as criminal investigations, national security or public interest since these exceptions are also included in Article 23.⁴⁴²

Eighth, data subjects should have the right to access their data at any time, as well as the right to acquire a copy of any data pertaining to them. In addition, they should request rectification, if the processed data is no longer accurate or relevant. They can request deletion, if the processing of their data is no longer lawful or needed. In addition, the data subject should have the right to object at any time, and this should effectively stop or prevent the data controller from processing their personal data, unless the data controller demonstrates legal bases that outweigh the data subject's freedoms and rights, or if the processing is for exercising their legal rights. Nevertheless, there are no exceptions to the right to object when personal data is used for direct marketing purposes.⁴⁴³

⁴⁴¹ WP254 rev.01, Chapter 3/A: Content Principles 3-5.

⁴⁴² WP254 rev.01, Chapter 3/A: Content Principles 6-7.; GDPR, Article 23(1): “[...] (a) national security; (b) defence; (c) public security;(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; (e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security; (f) the protection of judicial independence and judicial proceedings; (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; (h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g); (i) the protection of the data subject or the rights and freedoms of others; (j) the enforcement of civil law claims.”

⁴⁴³ WP254 rev.01, Chapter 3/A: Content Principles 8.

Ninth and finally, after the initial transfer from an EU country to a recipient third country, the latter should also ensure that any following transfers to other recipient countries from that third country are also having adequate level of data protection in accordance with the requirements of the GDPR. Even if the next recipient countries do not have an adequate level of data protection, at least the appropriate safeguards should be taken.⁴⁴⁴ For example, if one of the Member States, say Hungary, transfers data to the UK, the UK should also make sure that no data is sent to third countries that do not have adequate level of data protection. Even if they choose to transfer data to, say, the US, they should always make sure that the US company has the appropriate safeguards in place, like only keeping data that is encrypted or has been pseudonymised so that it can't be linked to a specific individual.

6.3.2 Additional Content Principles

If the processing of personal data with sensitive nature is involved, special and more stringent data protection measures should be in place, such as requiring the explicit consent of the data subject prior to processing his/her health-related data. Second, if the data is being processed for the purposes of direct marketing, the data subject shall have the right to object at any time, and the data controller should cease processing for such purposes. Thirdly, the subject of the data shall have the right to not be subject to a decision based only on automated processing, which includes profiling. There may be exceptions when a decision based on an automated decision is allowed, such as when it is necessary for the fulfilment of a contract, where the data subject grants explicit consent, or when it is mandated by national legislation. In any situation, however, the third country should give the appropriate protections to the data subject, such as the right to be informed, the right to amend inaccurate information, or the right to object to the processing of inaccurate information about him or her.⁴⁴⁵

6.3.3 Procedural and Enforcement Mechanisms

First, there should be one or more independent and competent supervisory authorities responsible for monitoring and ensuring compliance with data protection and privacy requirements. Second, the data protection system of the third country should ensure that data

⁴⁴⁴ WP254 rev.01, Chapter 3/A: Content Principles 9.

⁴⁴⁵ WP254 rev.01, Chapter 3/B: Examples of additional content principles to be applied to specific types of processing 1-3.

subjects properly exercise their rights, data controllers are aware of their obligations and tasks, and are subject to sanctions, if they do not comply with their responsibilities, and finally, there should be effective supervisory authorities in place to ensure compliance with the rules and conduct audits as required.⁴⁴⁶

Thirdly, the data protection mechanism of the third country should require data controllers and processors to comply with data protection rules and be accountable for their processing activities. For example, being able to provide data protection impact assessments, keeping records for a reasonable amount of time (such as the duration of a contract), appointing data protection officers, and respecting the principle of data protection by design and by default can demonstrate that the data controllers/processors adhere to certain legal obligations. When required, they should also be able to demonstrate their compliance to the supervisory authority/authorities.⁴⁴⁷

Lastly, if data controllers do not comply with the data protection requirements, the data subjects shall have access to efficient and prompt legal remedies. These remedies should include compensation for the damage that the data subjects have suffered as a result of the unlawful processing of their data.⁴⁴⁸

6.3.4 Essential conditions for public authorities to use surveillance and get access to personal data of individuals in third countries

Even though these criteria may be applied in different ways, these four criteria should still be met whenever the government needs access to the personal data of individuals, whether for reasons of national security or for law enforcement, in order to be seen as having an adequate level of protection:

- a. The processing of personal data by the government should be based on clear, transparent, and accessible rules so that data subjects are aware of the legal basis for the processing.
- b. The necessity and proportionality of the processing by the public authorities should be demonstrated.
- c. The public authorities should also be subject to independent oversight mechanisms.

⁴⁴⁶ WP254 rev.01, Chapter 3/C: Procedural and Enforcement Mechanisms 1-2.

⁴⁴⁷ WP254 rev.01, Chapter 3/C: Procedural and Enforcement Mechanisms 3.

⁴⁴⁸ WP254 rev.01, Chapter 3/C: Procedural and Enforcement Mechanisms 4.

d. If an individual's data protection rights are violated, there should be appropriate legal recourse.⁴⁴⁹

However, the US failed to consider the above-mentioned important principles, criteria, and conditions, and as a result, it lost its adequacy decision with the CJEU's judgement in the Schrems cases. As we have already discussed, public authority access and surveillance in the US were disproportionate and there were no effective legal remedies for EU data subjects, there was no independent oversight mechanism, such as an independent Ombudsperson, to monitor the processing activities of public authorities. In order to avoid the potential Schrems III decision, these principles and guidelines should be implemented into the planned Transatlantic data privacy framework between the EU and the US.⁴⁵⁰

Last but not least, the US should take into account Recital (105) of the GDPR, which states that international agreements should be considered for an adequacy decision, especially Convention 108+ of the Council of Europe,⁴⁵¹ the updated version of first legally binding international agreement addressing the protection of personal data.⁴⁵² This Convention has not been accessed by the United States, and its accession would be a significant step for the future Transatlantic data privacy agreement.⁴⁵³

6.4 Existing methods for transferring personal data from the EU to the US in the absence of an adequacy decision

As pointed out earlier, the SCCs and BCRs are the only existing procedures for transferring personal data from the EU to the US for repeated and continuing personal data transfers, as the derogations under Article 49 of the GDPR are limited to particular and exceptional transfers.⁴⁵⁴

BCRs can be utilised for international internal transfers within a company outside of EU. It developed from the necessity of a large number of transfers within a company and the

⁴⁴⁹ WP254 rev01, Chapter 4: Essential guarantees in third countries for law enforcement and national security access to limit interferences to fundamental rights 1-4.

⁴⁵⁰ Asli Alkis-Tümtürk: Uncertain future of transatlantic data flows: Will the United States ever achieve the 'adequate level' of data protection? Hungarian Journal of Legal Studies, vol. 63 issue. 3 (2022), 301.

⁴⁵¹ Council of Europe, Convention 108+ Convention for the protection of individuals with regard to the processing of personal data, ETS No. 108 (2018)

https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf (last visited 10 March 2023).

⁴⁵² GDPR, Recital (105).

⁴⁵³ Asli Alkis-Tümtürk: Uncertain future of transatlantic data flows: Will the United States ever achieve the 'adequate level' of data protection?, Hungarian Journal of Legal Studies, vol. 63 issue. 3 (2022), 301.

⁴⁵⁴ GDPR, Article 46-49.

desire to avoid having several SCCs for each internal data transfer. However, they take a long time to go into effect due to the fact that companies must submit their BCRs to the relevant Data Protection Authority (DPA) of their EU country for approval, which might entail several DPAs given that the subject company may have many entities in the EU. The DPAs will then get the opinion of the European Data Protection Board (EDPB) to finalise the approval of BCRs.⁴⁵⁵ As a result, it often takes around two years to obtain approval, which makes this process challenging and impractical compared to SCCs, but it remains a viable alternative for large companies with many entities in the EU and other third countries.⁴⁵⁶ The official website of the European Data Protection Board provides access to the list of BCRs approved by Data Protection Authorities under the GDPR as well as pre-GDPR prior to May 25, 2018.⁴⁵⁷

A joint survey conducted by Business Europe, DIGITALEUROPE, the European Round Table for Industry, and European Automobile Manufacturers Association reveals that just 5% of businesses employ BCRs, adequacy decisions, and derogations altogether.⁴⁵⁸ Whereas, according to the same survey, 85% percent of all respondents use SCCs for data transfers. Therefore, our focus will be on SCCs, as they are one of the most used methods for transferring personal data for transactions involving international commerce.⁴⁵⁹

SCCs are model contract clauses that have been pre-approved by the European Commission and can be used as the basis for data transfers from data controllers/processors in the EU to data controllers/processors outside the EU. The European Commission adopted modernised contractual clauses for data transfers to third countries on June 4, 2021, in accordance with the requirements of the GDPR.⁴⁶⁰ Moreover, EU data controllers should be

⁴⁵⁵ European Commission, Binding Corporate Rules (BCR), https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en (last visited 10 March 2023).

⁴⁵⁶ Nigel Cory, Ellyse Dick, and Daniel Castro: The Role and Value of Standard Contractual Clauses in EU-US Digital Trade, Information Technology and Innovation Foundation (2020), 13.

⁴⁵⁷ European Data Protection Board, Approved Binding Corporate Rules, https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en?page=1 (last visited 28 February 2023).

⁴⁵⁸ Nigel Cory, Ellyse Dick, and Daniel Castro: The Role and Value of Standard Contractual Clauses in EU-US Digital Trade, Information Technology and Innovation Foundation (2020), 13.; For the mentioned survey report see: Business Europe, DIGITALEUROPE, the European Round Table for Industry, and European Automobile Manufacturers Association: Schrems II: Impact Survey Report, 2020, 1-14. <https://www.digitaleurope.org/resources/schrems-ii-impact-survey-report/> (last visited 10 March 2023).

⁴⁵⁹ Nigel Cory, Ellyse Dick, and Daniel Castro: The Role and Value of Standard Contractual Clauses in EU-US Digital Trade, Information Technology and Innovation Foundation (2020), 4.

⁴⁶⁰ European Commission, Standard Contractual Clauses, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (last visited 10 March 2023).

aware that they may need to implement supplementary measures in addition to the SCCs in order to guarantee an essentially equivalent level of data protection, as required by the CJEU in Schrems II.⁴⁶¹

Following the Schrems II judgement, the EDPB issued recommendations on supplementary transfer options for companies/organisations to guarantee GDPR compliance. Since Article 46 requires that SCCs be operated on a case-by-case basis, controllers/processors acting as data exporters to other countries must be responsible for determining whether the third country's legislation and practise contravenes the effectiveness of such SCCs. If this is the case, data exporters can still implement supplementary measures to bring third-country data protection levels up to EU standards. This EDPB recommendation document guides data exporters in comprehending how to assess the data protection level of third countries, as well as providing some examples of relevant supplemental measures that exporters may adopt if necessary.⁴⁶²

Examining the third countries data protection legislation and practices should be especially necessary where:

“(i) legislation in the third country formally meeting EU standards is manifestly not applied/complied with in practice; (ii) there are practices incompatible with the commitments of the transfer tool where relevant legislation in the third country is lacking; (iii) your transferred data and/or importer fall or might fall within the scope of problematic legislation (i.e. impinging on the transfer tool’s contractual guarantee of an essentially equivalent level of protection and not meeting EU standards on fundamental rights, necessity and proportionality).”⁴⁶³

In these above situations, exporter data controllers/processors shall either suspend the data transfer or implement adequate supplementary measures, if the transfer is to proceed. In the third situation described above, data controllers/processors may choose not to suspend or implement supplementary measures provided, if they are able to demonstrate that relevant problematic legislation will not be implemented in practise to cover the transferred data and

⁴⁶¹ Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems EU:C:2020:559, para 133.

⁴⁶² EDPB: Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0, 18.06.2021, 3. https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf (last visited 10 March 2023).

⁴⁶³ EDPB: Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0, 18.06.2021, 4.

the importer.⁴⁶⁴ These supplementary measures may be technological, contractual, or organisational in nature. Implementing one or more of the measures outlined in this recommendation does not ensure that exporters will fulfil the EU's data protection standard. Therefore, data exporter controllers/processors should be careful when selecting the supplemental measures that will provide an essentially equivalent level of protection for their transfers. In light of the fact that the examples described in this recommendation are not exhaustive, new supplemental measures would be implemented to keep up with the requirements of future technical and legal developments.⁴⁶⁵

Encrypting and pseudonymizing personal data are examples of technical measures. Encryption is a process that transforms readable, identifiable data into random values so that only those with access to the decryption keys may view the encrypted data. Encryption may be used as a reversible masking for pseudonymisation, because no one can access the clear data without the decryption keys.⁴⁶⁶

The process of pseudonymisation entails that personal data are no longer associated with or linked to identifiable persons without additional information. For example, blood types and names are gathered for health-related research; if they are stored and accessible concurrently, persons can be identified. However, if the names were encrypted and kept secret, the obtained health data could no longer be associated with the data subjects.⁴⁶⁷

Additional contractual measures may include a commitment to transparency. To be transparent, the data importer from a third country should implement effective controls to prevent public authorities, especially intelligence services, from accessing the transferred personal data of EU-based data exporters and should notify the data exporter each time a public authority requests access. As well as data importers should disclose the extent to which they are permitted to provide information to those indicated in relation to the data surveillance of the public authorities.⁴⁶⁸

⁴⁶⁴ EDPB: Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0, 18.06.2021, 4.

⁴⁶⁵ EDPB: Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0, 18.06.2021, 28.

⁴⁶⁶ EDPB: Why a good additional technical safeguard is hard to find- A response to the consultation on the EDPB draft recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 2 https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/response_to_edpb_recommendations.pdf (last visited 10 March 2023).

⁴⁶⁷ GDPR, Article 4(5).

⁴⁶⁸ EDPB: Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0, 18.06.2021, para 105 et seq.

Data importer obligations to perform specific actions may constitute an additional contractual measure. For example, in the case of a conflict with the EU data protection legislation, there should be a legal action in place in the third country such as a temporary suspension of the transfer or the necessity of a judicial review and/or warrant. The importer shall prove and document that all the essential steps has done in their best practise to fulfil this obligation.⁴⁶⁹ In addition, the data importer should encourage and help data subjects in exercising their rights. For example, if there is a disclosure of personal data transferred in breach of the commitments, the data importer in the third country shall help the data subjects in seeking effective redress mechanisms. The remedy may consist of the data importer compensating the victim for all material and non-material damages suffered. Clearly, this supplementary measure can only be effective, if the third country offers law enforcement and redress mechanisms before its national courts, to which data subjects or data importers on behalf of data subjects may appeal, including against surveillance activities.⁴⁷⁰

Adoption of standards and best practises can be considered a measure of an organisation. For instance, strong data protection and privacy policies based on EU certification or codes of conducts or international standards (e.g., ISO certification) and best practises (e.g., ENISA) might be implemented according to the risk associated with the categories of data being processed and transferred.⁴⁷¹

The SCCs and additional precautions have already been implemented in practise, as stated in the privacy policies of big companies. Google (including YouTube), for instance, specify in their privacy policy that they employ SCCs for data transfers from EU nations to third countries.⁴⁷² Meta also disclosed in their privacy policies that they utilise European Commission-approved SCCs to transfer user data from the EU to third countries in order to provide an equivalent level of data protection for its users.⁴⁷³

⁴⁶⁹ EDPB: Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0, 18.06.2021, para 118 et seq.

⁴⁷⁰ EDPB: Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0, 18.06.2021, para 122 et seq.

⁴⁷¹ EDPB: Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0, 18.06.2021, para 141 et seq.

⁴⁷² Google, Privacy&Terms: Data transfers <https://policies.google.com/privacy?hl=en-US#infosharing> (last visited 10 March 2023); YouTube help, Manage privacy settings: Understanding the basics of privacy on YouTube apps <https://support.google.com/youtube/answer/10364219?hl=en#:~:text=YouTube%20does%20not%20sell%20your.results%2C%20and%20serving%20relevant%20ads>. (For their privacy policy they direct you to the above-mentioned Google Privacy Policy) (last visited 10 March 2023).

⁴⁷³ Facebook, Data Policy: How do we operate and transfer data as part of our global services? <https://m.facebook.com/privacy/policy/version/20220104/> (last visited 10 March 2023).; Facebook data policy includes Instagram terms as well, but you may also check it here: Instagram, Help Centre, Data Policy:

Spotify does not specifically reference SCCs, but it does state that it uses transfer tools to guarantee the same level of protection as EU users.⁴⁷⁴ In addition to SCCs, Johnson & Johnson's privacy policy lists EU-approved codes of conduct and certification as transferring tools.⁴⁷⁵ Vodafone does not specify the transfer method either, but they do state that if the country of the data importer is not deemed to have laws that are equivalent to EU data protection standards, Vodafone will require the third-country importer to enter into a legal agreement that reflects those standards.⁴⁷⁶

6.5 Transfer of children's personal data from the EU to third countries

There is no particular provision in the GDPR addressing the transfer of children's data. However, we believe that children's data should be considered special categories of data and should be handled differently and with more consideration than the data transfer of adults. In order to create a comparison, we may use the real-life examples described above. For example, Facebook and Instagram privacy policies state no explanation regarding the child-specific data transfers within the EU or to other third countries outside of the Union.⁴⁷⁷

In terms of children data policy, Google has a comparatively improved application called Family Link, with which parents may control the Google accounts of their underage children.⁴⁷⁸ Google clarifies that they can share children's data with parental consent that their external processor can process children's data on their behalf according to their instructions, and that they can also process them for legal reasons (e.g., to comply with any applicable law, to prevent/detect/address fraud or security issues).⁴⁷⁹

How do we operate and transfer data as part of our global services?

<https://help.instagram.com/155833707900388> (last visited 10 March 2023).

⁴⁷⁴ Spotify Privacy Policy: Transfer to other countries <https://www.spotify.com/us/legal/privacy-policy/#7-transfer-to-other-countries> (last visited 10 March 2023).

⁴⁷⁵ Johnson & Johnson Privacy Policy: Crossborder Transfers <https://www.jnj.com/corporate/privacy-policy#:~:text=Unless%20we%20specifically%20request%20or.life%20or%20sexual%20orientation%2C%20criminal> (last visited 10 March 2023).

⁴⁷⁶ Vodafone Privacy and Cookie Policy: International data transfer <https://www.vodafone.com/cookie-policies> (last visited 10 March 2023).

⁴⁷⁷ Facebook, Privacy Policy: How do we share information?, https://privacycenter.instagram.com/policy/?section_id=9-HowDoWeTransfer (last visited 10 March 2023).

Instagram, Data Policy: IX. How do we operate and transfer data as part of our global services?, https://help.instagram.com/519522125107875/?helpref=uf_share (last visited 10 March 2023).

⁴⁷⁸ Google Family Link <https://families.google/familylink/> (last visited 10 March 2023).

⁴⁷⁹ Google Family Link, Privacy Notice for Google Accounts and Profiles Managed with Family Link, for Children under 13 (or applicable age in your country) ("Privacy Notice"): Information Google Shares <https://families.google.com/familylink/privacy/child-policy/> (last visited 10 March 2023).

YouTube Kids is a new and relatively safer platform for children, and its privacy standards are identical to those of Google.⁴⁸⁰ It means that they share children's data under the following conditions: if parental consent is obtained, if their trusted processors process children's data on their behalf in accordance with their instructions, and if they process children's data for legal reasons (for example, to protect Google's, its users', or the public's rights and safety as permitted or required by law).⁴⁸¹

The sole statement Johnson & Johnson made in their privacy policy addressing children's data was that they do not offer services to individuals under the age of 16 and request that these individuals do not provide them with personal information. If parents discover that their children have provided them with personal information, they ensure that they may contact them to get the information removed.⁴⁸² However, they make no mention of the processing or transfer of their data, since they claim that they do not provide services for children. This does not, however, imply that children will be excluded from these services in reality. According to the most recent news, Johnson & Johnson is undertaking study on children to determine the efficacy of COVID-19 vaccinations in various age ranges. It implies that they should collect the personal data of children in the vaccinated group and the control group in order to perform a comparison for research purposes.⁴⁸³ The news claims that the Centers for Disease Control and Prevention (CDC) will collect data from vaccine recipients, which raises privacy concerns, because the CDC may share these data with sensitive nature with third parties or there could be a cyber-attack and disclosure of these sensitive information even without the CDC's knowledge.⁴⁸⁴ Johnson & Johnson is also based in the US; consequently, according to these latest updates, the data protection and

⁴⁸⁰ YouTube Kids: An application specially designed for children <https://www.youtube.com/kids/> (last visited 10 March 2023).

⁴⁸¹ YouTube Kids Privacy Notice: Information we share <https://kids.youtube.com/t/privacynotice> (last visited 10 March 2023).

⁴⁸² Johnson & Johnson, Privacy Policy: Use by Minors <https://www.jnj.com/corporate/privacy-policy> (last visited 10 March 2023).

⁴⁸³ Carrie MacMillan: COVID-19 Vaccine Authorized For Kids Ages 5 to 11: What Parents Need to Know, Yale Medicine, 20 May 2022, <https://www.yalemedicine.org/news/covid-vaccine-for-ages-5-to-11> (last visited 10 March 2023).

CHOC (Children's Hospital of Orange County): The COVID-19 vaccine for kids under 12: What parents should know, last updated 11 November 2022, <https://health.choc.org/the-covid-19-vaccine-for-kids-under-12-what-parents-should-know/> (last visited 10 March 2023).

⁴⁸⁴ Rachel Sandler: CDC Will Collect Personal Data On Vaccine Recipients, Raising Privacy Concerns, Forbes, 8 December 2020, <https://www.forbes.com/sites/rachelsandler/2020/12/08/cdc-will-collect-personal-data-on-vaccine-recipients-raising-privacy-concerns/?sh=2ac8021d50ec> (last visited 10 March 2023).

privacy rights of Johnson & Johnson vaccine study participants, who are children, are at risk of being violated.⁴⁸⁵

According to Vodafone's child data privacy policy, if there is any personal data processing involved at an early stage of a product or project, they should undergo the Privacy Impact Assessment (PIA), which is equal to the data protection impact assessment (DPIA) under the GDPR. Such DPIAs include explicit parental consent, child-friendly language, and the avoidance of child profiling. If Vodafone collects children's personal data, DPIAs forbid direct marketing to children.⁴⁸⁶

GDPR defines profiling as follows:

“[...] any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements”.⁴⁸⁷

Vodafone's approach to child privacy goes beyond the GDPR's obligations in terms of profiling and direct marketing. Because GDPR Article 22 does not distinguish between children's and adult data and thus profiling of children's data is not prohibited.⁴⁸⁸ Nonetheless, Recital (38) requires specific protection where personal data of children is processed for the purposes of marketing or profiling, as well as the collection of personal data with regard to children when using services offered directly to a child.⁴⁸⁹

Although Recital (71) states that solely automated decision-making, including profiling should not apply to children, this recital is not reflected in Article 22 itself. When we consider the previously mentioned related recitals and articles, we cannot say that GDPR completely prohibits neither profiling nor direct marketing. Nevertheless, WP29 suggested⁴⁹⁰ that data

⁴⁸⁵ “Johnson & Johnson Services, Inc., located at One Johnson & Johnson Plaza New Brunswick, New Jersey 08933, is the company responsible for collection, use, and disclosure of personal information under this Privacy Policy.” Johnson & Johnson, Privacy Policy: Contacting us <https://www.jnj.com/corporate/privacy-policy> (last visited 10 March 2023).

⁴⁸⁶ Vodafone, Child rights and online safety: Privacy and Product Safety <https://www.vodafone.com/sustainable-business/operating-responsibly/child-rights-and-online-safety> (last visited 10 March 2023).

⁴⁸⁷ GDPR, Article 4(4).

⁴⁸⁸ GDPR, Article 22.

⁴⁸⁹ GDPR, Recital (38).

⁴⁹⁰ Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN WP251rev.01, last revised and adopted on 6 February 2018, p. 1-37, 26.

controllers follow the wording of Recital (71) wherever possible and do not justify their children profiling activities with the exceptions under the Article 22(2).⁴⁹¹ Consequently, we should give Vodafone credit for enhancing its privacy policy toward children even more than the GDPR requires, and for completely forbidding profiling and direct marketing to children.

According to the facts provided, we endorse Google, YouTube, and Vodafone methods since they do not ignore children engaging in online activities on their platforms and services, as do Facebook, Instagram, and Johnson & Johnson. Accepting their online presence is a significant first step, and the next and most important step is to establish child-specific data protection and privacy rights. We advocate that Vodafone's avoidance of profiling and direct marketing to children is noteworthy, and it should serve as an example for other data controllers.

According to above-mentioned companies' privacy policies, they can disclose children's data with either explicit parental consent or based on some legal reasons. We cannot argue that these activities are unlawful or invalid, since there is no guidance in the GDPR or the EDPB/WP29 recommendations. However, there are some transfers that would be invalid, and we haven't encountered any legislation, guidance or doctrinal discussions on the subject thus far. The problem is that, in our opinion, when processing personal data based on consent, children in EU member states have varying age requirements, which would almost certainly result in unlawful data transfers even within the EU. As noted in the previous chapters about the threshold age for parental consent, the following are the EU Member States' digital platform-related consent ages for children: Austria (14), Belgium (13), Bulgaria (14), Croatia (16), Cyprus (14), Czech Republic (15), Denmark (13), Estonia (13), Finland (13), France (15), Germany (16), Hungary (16), Greece (15), Ireland (16), Italy (14), Latvia (13), Lithuania (14), Luxembourg (16), Malta (13), the Netherlands (16), Poland (16), Portugal (13), Romania (16), Slovakia (16), Slovenia (15), Spain (14), and Sweden (13).⁴⁹²

In this scenario, a 13-year-old child in Finland can consent to the transfer of his or her data to Hungary. However, according to local data protection rules in Hungary, a child under the age of 16 cannot provide consent to transfer his/her data to anyone/anywhere without parental consent. Therefore, from the standpoint of Hungarian privacy, this consent and data

⁴⁹¹ GDPR, Article 22(2): "Paragraph 1 shall not apply if the decision: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent."

⁴⁹² See the Table 1 of this thesis under the Subchapter 3.3.

transfer would be invalid. This is a really problematic situation, yet it does not appear to raise sufficient concern among academics or lawmakers.

The first Commission report on the assessment and review of the GDPR, particularly regarding the implementation and functioning of the regulations on the transfer of personal data to third countries and the rules on cooperation and consistency,⁴⁹³ raises some concerns about this matter. According to this report, the GDPR offers a unified approach to data protection throughout the EU, but facultative specification clauses cause fragmentation. It is claimed that varying age of consent for information society services across Member States generates uncertainty and difficulties for cross-border commerce.⁴⁹⁴

The Commission Staff Working Paper accompanying the first report notes that distinguishing ages for offering online services to children by Member State is contradictory to the GDPR's core purpose of ensuring equal protection for individuals and business opportunities in all Member States. Moreover, the Commission also concerns about national divergences' costs. National differences in legislation implementation and data protection authorities' interpretation raise EU legal compliance costs.⁴⁹⁵

Notwithstanding these concerns raised in the first report and accompanying Commission Staff Working Document, no improvements have been implemented addressing the harmonisation of the varying age of online consent across Member States. This gap should be filled, in our opinion, either by making the age requirement uniform throughout all EU Member States or by enforcing effective legal guidance surrounding this problem. For instance, the GDPR might oblige any EU-based data importer to make all reasonable efforts to verify the transferred children's data against the age threshold criteria of their country of origin. Although the optimal option would be for the EU to adopt a uniform age requirement, there are still some online practices (e.g., Google and YouTube),

⁴⁹³ Article 97 of the GDPR mandates that the Commission examine and assess the Regulation beginning with the first report after two years and continuing every four years.

See the report: European Commission, Communication from the Commission to the European Parliament and the Council Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, Brussels, 24.6.2020, COM (2020) 264 final, pp. 1-18.

⁴⁹⁴ European Commission, Communication from the Commission to the European Parliament and the Council Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, Brussels, 24.6.2020, COM (2020) 264 final, 7.

⁴⁹⁵ European Commission, Commission Staff Working Document, Accompanying the document Communication from the Commission to the European Parliament and the Council Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, Brussels, 24.6.2020, SWD(2020) 115 final, pp. 1-52, 17.

which are respecting the domestic data protection law and their different age requirements for obtaining the consent for data processing.

In terms of SCCs, there is no difference between children's and adults' data transfer in the current state. The European Commission adopted two sets of SCCs on 4 June 2021, one for use between data controller-processor⁴⁹⁶ and the other for the transfer of personal data to third countries⁴⁹⁷. None of them provides particular data protection standards for children. In our opinion, to raise awareness among data exporter controllers/processors, and data importer controllers/processors, it would be ideal to include child-specific protections inside the SCCs.

We argue that a separate clause, analogous to the one for data falls under special categories, would be incorporated to require additional protections regarding children's personal data.⁴⁹⁸ Additional safeguards (e.g., pseudonymisation/encryption of the data, assuring data minimisation and purpose limitation etc.) may be implemented. Besides, stricter restrictions should be required, for example, limited access to such data (e.g., only for personnel who have undergone special training), retention periods for a definite period of time and restricted onward transfers (guarantees that children's data will not be transferred to countries with inadequate level of data protection).⁴⁹⁹

Furthermore, each Member State would have its own clauses regarding threshold age of consent for internet activities. For instance, as children under the age of 16 in Hungary cannot consent to the transfer of their data,⁵⁰⁰ the clause should incorporate age-specific restrictions if such data are to be transferred from Hungary to the US. Each time an under-age child is involved in a data transfer, extra measures must be taken to ensure that the parental consent is provided for the transfer to be lawful.

⁴⁹⁶ European Commission, Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council, OJ L 199/18, 7.6.2021, p. 18-30.

⁴⁹⁷ European Commission, Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, OJ L199/31, 7.6.2021, p. 31-61.

⁴⁹⁸ See the Clause for data falls under special categories: European Commission, Annex to the Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, Brussels, 4.6.2021, C(2021) 3972 final, 6, Clause 8.6 "Sensitive Data".

⁴⁹⁹ European Commission, Annex to the Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, Brussels, 4.6.2021, C(2021) 3972 final, 29, Annex I.B.

⁵⁰⁰ 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, cikk 5 §(3).

It is not impossible to conclude that SCCs with additional measures can give an adequate level of protection. However, these solutions are not comprehensive and require case-by-case investigations. Consequently, this might place a financial burden especially on small and medium-sized companies due to the costly and demanding obstacles (e.g., establishing technology solutions and employing specialists to manage these technical solutions, such as encrypting/pseudonymizing transferred personal data).⁵⁰¹ Large and well-known businesses have a comparative advantage in the current challenging environment. Even if the SCCs are in place and data transfer has begun, there is always a chance that the data transfer could be suspended or ceased due to a violation (e.g., public authorities' access in the subject third party country, insufficient judicial remedy for the individuals whose data is transferred to a third country), which the data controller cannot control or prevent, but for which they are responsible and bear all the risk.⁵⁰²

To summarise, because SCCs are costly and case-by-case remedies, replacing the Privacy Shield with a new adequacy decision would be the best option. There are several scenarios under which it can be an effective solution while avoiding another invalidation by CJEU. First, public authorities' access would be limited and should only occur when absolutely necessary. Second, in the event of a data breach (e.g., as a result of intelligence services' monitoring activities), there should be effective judicial remedies for EU data subjects whose data is transferred to the US. Third, there should be an independent oversight mechanism (e.g., appointing a completely objective Ombudsman) to check and supervise the privacy of EU data subjects. And fourth, we suggest that there should be child-specific provisions regulating the transfer of data concerning children from EU countries to non-adequate third countries. If all of these were in place, we believe there would be no need for the Schrems-III, and in terms of dependability, stability, and accessibility (particularly for small and medium-sized companies), that would be a far safer option than SCCs.⁵⁰³

⁵⁰¹ Barbara Sandfuchs: The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18–Schrems II, *GRUR International* 70(3) (2021), 246.

⁵⁰² Barbara Sandfuchs: The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18–Schrems II, *GRUR International* 70(3) (2021), 248.

⁵⁰³ Barbara Sandfuchs: The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18–Schrems II, *GRUR International* 70(3) (2021), 248 cited in Asli Alkis: The impact of the Privacy Shield's invalidation on the EU-US dataflows, *Studia Iurisprudentiae Doctorandorum Miskolciensium*, (2022) vol.1, 34.

6.6 Impacts of the fact that Privacy Shield is no longer applicable, and SCCs are being utilised instead: Is Data Localization the best solution?

As highlighted in the previous chapter, the SCCs impose a high level of accountability on the data exporters and importers, and the importers cannot always anticipate or avoid data breaches (e.g., unjustified and unrestricted access to imported data by intelligence services). Therefore, the risk should be borne by the data exporter, who should take precautionary technological and/or organisational precautions. As we already discussed, these additional procedures would be too expensive for small and medium-sized companies to implement.

Even if supplementary measures are in place and the data importer has given timely warning of an expected or occurring data breach, the data exporter must cease or suspend the data transfer. This would be a time- and money-consuming problem for the data exporter, posing even another difficulty. Thus, we may have concluded that EU companies would prefer not to transfer data to third countries (such as the US) in order to avoid legal complexity, time-consuming procedures, costly measures, and uncertainty. This can result in the data remaining within the EU and not being transferred; — in other words, it can lead to data localisation.⁵⁰⁴

In fact, on 17 July 2020, one day after the Schrems II decision, the Berlin Commissioner for Data Protection and Freedom of Information, *Maja Smolczyk*, issued a statement stating that the data transfers from Germany to the US should be halted and that data exporters should not transfer data to the US until their data protection legislation will be reformed. In addition, *Maja Smolczyk* suggested that SCCs should not be used for third countries with state access possibilities. If such access rights of the public authorities exist, according to her, the SCCs cannot justify the data transfer to that third country. Per this statement, not just transfers to the US, but also transfers to other countries that may raise even higher data protection issues will be thoroughly reviewed before initiating the data transfer processes with them.⁵⁰⁵

Data localisation seems to overcome the difficulties posed by the Schrems II case at first appearance. If no information is transferred outside the EU, there is no need to consider the possibility that a data protection authority or court might declare the transfer invalid.

⁵⁰⁴ Nigel Cory, Ellyse Dick, and Daniel Castro: *The Role and Value of Standard Contractual Clauses in EU-US Digital Trade*, Information Technology and Innovation Foundation (2020), 12.

⁵⁰⁵ Berliner Beauftragte für Datenschutz und Informationsfreiheit: Nach „Schrems II“: Europa braucht digitale Eigenständigkeit, Pressemitteilung, 711.424.1, 17 Juli 2020. https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2020/20200717-PM-Nach_SchremsII_Digitale_Eigenstaendigkeit.pdf (last visited 10 March 2023).

Nevertheless, there are a number of reasons why data localization is not a reasonable choice. First and foremost, as we stated in the previous chapters, one of the primary purposes of the GDPR is to regulate the free flow of personal data not only within the EU but also to third countries.⁵⁰⁶ According to Recital (6) of the GDPR, technology has transformed economic and social life, and according to new standards, the EU should further facilitate the free flow of personal data within the EU, as well as to third countries and international organisations, while maintaining a high level of protection for personal data.⁵⁰⁷ Thereby, it is clear that data localization would be in direct opposition to the spirit of the GDPR.

In addition, we cannot assume that trying to retain the data only within the EU and third countries with adequacy decisions will prevent further data transfers. Because, for instance, the United Kingdom (the UK) has a level of data protection deemed appropriate by the European Commission. In addition, the UK is a member of the Five Eyes⁵⁰⁸ intelligence alliance, together with the US, Australia, New Zealand, and Canada. It would be highly optimistic to assume that they do not share the results of their surveillance and intelligence activities. In fact, Edward Snowden disclosed in 2013 that the Five Eyes had spied on each other's citizens and shared the information they had collected.⁵⁰⁹

There were reports that some US lawmakers would prefer to add Germany to the Five Eyes alliance, expanding it to six eyes.⁵¹⁰ Accordingly, there are some perspectives within the doctrine recommending that the US should take more steps to bring Germany or maybe France into the Five Eyes.⁵¹¹ In our viewpoint, it would not foster a climate of trust in the EU, but would instead undermine the credibility and trustworthiness of the GDPR and the data protection rights and freedoms of EU data subjects. Moreover, this Five Eyes

⁵⁰⁶ GDPR, Article 1(1)(3).

⁵⁰⁷ GDPR, Recital (6).

⁵⁰⁸ “In 1946, an alliance was formed between five anglophone countries and their security agencies: the US (NSA), the UK (GCHQ), Australia (ASD), Canada (CSEC) and New Zealand (GCSB) comprising of a series of bilateral agreements on surveillance and intelligence-sharing. [...] Pursuant to these arrangements, each of the Five Eyes states conducts interception, collection, acquisition, analysis and decryption activities, sharing all intelligence information obtained with the others by default.”

Privacy International, Five Eyes, <https://privacyinternational.org/learn/five-eyes> (last visited 28 February 2023).

⁵⁰⁹ The Guardian: US and UK struck secret deal to allow NSA to 'unmask' Britons' personal data, 20 November 2013, <https://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data> (last visited 10 March 2023).

⁵¹⁰ Deutsche Welle: The sixth eye?, 22 November 2013, <https://www.dw.com/en/us-lawmakers-push-for-german-entrance-to-five-eyes-spy-alliance/a-17246049> (last visited 10 March 2023).

⁵¹¹ Jonah Force Hill: The growth of data localization post-snowden: Analysis and recommendations for us policymakers and business leaders, The Hague Institute for Global Justice, Conference on the Future of Cyber Governance (2014), 32.

partnership might make it difficult for the UK to maintain an adequate level of data protection in the coming years due to the risk of potential inadequate onward transfers to the US.⁵¹²

Not only have intelligence services been cooperating between English-speaking countries, but also with EU Member States and the US. Despite being one of the most outspoken critics of National Security Agency (NSA) spying, Germany was considered a “prolific partner” of the NSA in terms of data sharing. The “*Der Spiegel*” stated that the German foreign intelligence agency called Bundesnachrichtendienst (BND) was collaborating with the NSA and that the NSA was accessing around 500 million German metadata records each month.⁵¹³

It is claimed that data localisation makes it easier to fight against cyberattacks, because a well-trained cybersecurity staff can easily protect personal data in a single centre.⁵¹⁴ However, location is typically not the primary element in the fragility of cybersecurity; rather, it is the lack of appreciation for the effective and broad use of personal data encryption. If the data is transferred securely using technical measures (such as encrypting or pseudonymizing), the transferred location does not pose a high threat to cyber security.⁵¹⁵ Besides, a corporation conducting business in multiple countries would be required to operate a data storage centre in each country based upon the data localisation requirements of the domestic data protection legislation of these jurisdictions. It would expand the cyber-attack surface for hostile attackers, and if the updates were delayed, it would weaken the defences against cyber-attacks in several locations.⁵¹⁶

Furthermore, it would be highly expensive for businesses operating in many countries to localise their operations in each and every country and employ multiple service providers for data gathering and storage. Duplicating the infrastructural framework across all jurisdictions would make upgrading and cybersecurity procedures more challenging. As

⁵¹² Oliver Patel and Nathan Lea: EU-UK data flows, Brexit and no-deal: Adequacy or disarray?, UCL European Institute, Brexit Insights, (2019), 10.

⁵¹³ Spiegel International: German Intelligence Used NSA Spy Program, 20 July 2013, <https://www.spiegel.de/international/germany/german-intelligence-agencies-used-nsa-spying-program-a-912173.html> (last visited 10 March 2023) cited in Anupam Chander: Is Data Localization a Solution for Schrems II?, Journal of International Economic Law, vol. 23.3, (2020), 781.

⁵¹⁴ John Selby: Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?, International Journal of Law and Information Technology, 25.3 (2017), 230.; Anupam Chander: Is Data Localization a Solution for Schrems II? Journal of International Economic Law, vol. 23.3, (2020), 783.

⁵¹⁵ Dan Svantesson: Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines, OECD Digital Economy Papers, No. 301, OECD Publishing (2020), 15.

⁵¹⁶ Anupam Chander: Is Data Localization a Solution for Schrems II?, Journal of International Economic Law, vol. 23.3, (2020), 783.

previously mentioned, the need for case-by-case adequacy testing and privacy impact assessments makes SCCs rather costly for small companies. In addition, because data localisation is costly, the small and medium sized companies might completely avoid data transfers.⁵¹⁷ However, this would contradict the GDPR's enhanced international commerce and international cooperation aims.⁵¹⁸

Data localisation appears to be a simple solution to the unlimited and excessive surveillance by the US government at first glance. However, as we have shown in this chapter, there are now a number of concerns with data localisation, and in the digital age in which we live, a single click may provide instant access to massive amounts of data. Therefore, we should come to a conclusion that where you store personal data is no longer the primary or most important concern.⁵¹⁹

6.7 The new Transatlantic Data Privacy Framework: Is the Schrems III coming?

As previous discussions have demonstrated, both the EU and the US need a new adequacy decision since they are each other's "important trading partners"⁵²⁰ with a combined \$7,1 trillion in economic relations⁵²¹. Accordingly, it was reported in March 2022 that they had reached an agreement on a new joint statement in principle regarding the Transatlantic Data Privacy Framework. This new framework attempts to remedy the deficiencies of its Safe Harbour and Privacy Shield predecessors.

⁵¹⁷ Anupam Chander: Is Data Localization a Solution for Schrems II?, *Journal of International Economic Law*, vol. 23.3, (2020), 782.

⁵¹⁸ GDPR, Recital (101).

⁵¹⁹ Asli Alkis: The impact of the Privacy Shield's invalidation on the EU-US dataflows, *Studia Iurisprudentiae Doctorandorum Miskolciensium*, (2022) vol.1, 36.

⁵²⁰ "As the adequacy decisions adopted so far show, it is possible for the Commission to recognise a diverse range of privacy systems, representing different legal traditions, as being adequate. These decisions concern countries that are closely integrated with the European Union and its Member States (Switzerland, Andorra, Faeroe Islands, Guernsey, Jersey, Isle of Man), important trading partners (Argentina, Canada, Israel, the United States), and countries that have a pioneering role in developing data protection laws in their region (New Zealand, Uruguay)." European Commission: Communication from the Commission to the European Parliament and the Council Exchanging and Protecting Personal Data in a Globalised World, COM/2017/07 final, 10.01.2017, 7.

⁵²¹ "Transatlantic data flows are critical to enabling the \$7.1 trillion EU-U.S. economic relationship." The White House: Fact Sheet: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework (7 October 2022), <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/> (last visited 10 March 2023).

Surveillance by the US government's intelligence services will be proportionate and conducted only when necessary for national security; the Data Protection Review Court will be established and will review EU complaints in a “two-layer” system for redress; self-certification of companies will continue with strict obligations; and to ensure the limited surveillance activities, there will be objective and independent oversight mechanisms for intelligence agencies.⁵²²

On 7 October 2022, US President *Joe Biden*⁵²³ signed an Executive Order to implement the Transatlantic Data Privacy Framework, which was announced into US law in March 2022.⁵²⁴ On this basis, the European Commission has now declared that they will prepare an adequacy decision and initiate its adoption procedure.⁵²⁵ The new Executive Order requires the establishment of legally enforceable safeguards to limit the intelligence services' access to the personal data transferred from the EU to what is necessary and proportional for national security.⁵²⁶

At this point, we question the content of the proportionate access. Indeed, *Max Schrems* challenged whether the proportionality is based on the European idea of proportional or the American understanding.⁵²⁷ Because, if this were the American approach to proportionate

⁵²² European Commission: European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework (25 March 2022) https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087 (last visited 10 March 2023). For more information: European Commission: Trans-Atlantic Data Privacy Framework (25 March 2022), https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100 (last visited 10 March 2023).

⁵²³ “Joe Biden is the 46th president of the United States (2021–). Biden was born on November 20, 1942, in Scranton, Pennsylvania. He has a bachelor’s degree from the University of Delaware and a law degree from Syracuse University.”

Britannica, Joe Biden, <https://www.britannica.com/biography/Joe-Biden> (last visited 28 February 2023).

⁵²⁴ The White House: Fact Sheet: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework (7 October 2022), <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/> (last visited 10 March 2023).

⁵²⁵ European Commission: Questions & Answers: EU-U.S. Data Privacy Framework (7 October 2022) https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_6045 (last visited 10 March 2023).

⁵²⁶ The White House: Fact Sheet: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework (7 October 2022), <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/> (last visited 10 March 2023).

⁵²⁷ The EU and the US approaches to proportionality differ in terms of limiting the intelligence services' access to the personal data:

According to Article 5(4) of the TFEU, the concept of proportionality entails using authorities only to the amount necessary to achieve certain objectives. In light of this principle, Article 5(1)(b) of the GDPR requires that personal data be processed only when necessary and proportionate to fulfil the explicit, specified, and legitimate purpose for which it was collected. Accordingly, in *Klass and Others v. Germany*, the ECtHR stated that “[p]owers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions.”. Furthermore, in *Szabó and Vissy v. Hungary*, the ECtHR explained the expression of “strictly

access, it would likely not prevent mass surveillance.⁵²⁸ Therefore, regarding these further safeguards, the solutions and concepts still appear ambiguous.

On February 28, 2023, the EDPB published an opinion on the adequate protection of personal data under the Transatlantic Data Privacy Framework.⁵²⁹ With regards to the proportionality principle, the EDPB considered that the US law enforcement investigative measures meet the requirements of necessity and proportionality in relation to fundamental rights to privacy and data protection.⁵³⁰ In this opinion, EDPB asserts that, according to Executive Order 14086, two new requirements have been introduced to US law that correspond to the conditions highlighted by the CJEU in *Schrems II*. These requirements

necessary” as follows: “[t]he Court considers that the requirement “necessary in a democratic society” must be interpreted in this context as requiring “strict necessity” in two aspects. A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation.” On the other hand, “minimization” procedures of the 1978 Foreign Intelligence Surveillance Act (FISA) (and its amendments) compel intelligence agencies to collect and retain the personal information when it is necessary to achieve their intelligence objectives. The Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities requires intelligence agencies to collect and retain data “as tailored as feasible” to protect the privacy rights of the individuals. In spite of these, the US has traditionally placed a greater emphasis on surveillance and national security, particularly in the aftermath of the September 11 attacks. The EU approach gives greater importance to data protection rights and requires intelligence agencies to access to personal data only when necessary and proportional. The US restricts the collection and retention of personal data and compels intelligence agencies to protect privacy rights, although not as strictly as the EU. Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union Consolidated version of the Treaty on European Union Consolidated version of the Treaty on the Functioning of the European Union Protocols Annexes to the Treaty on the Functioning of the European Union Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007 Tables of equivalences, OJ C 202, 7.6.2016, p. 1–388, Article 5(4). GDPR, Article 5(1)(b).

Klass and Others v. Germany judgment on 6 September 1978, no. 5029/71 para. 42.

Szabó and Vissy v. Hungary judgment 12 January 2016, no. 37138/14 para. 73.

Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-1885, 25.10.1978, §1801(h) “Minimization procedures”.

Executive Order No. 14086, vol. 87 no. 198 Federal Register, 14.10.2022, pp. 62283-62297, Section 2(c)(i)(B).

Francesca Bignami and Giorgio Resta: Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance In Community Interests Across International Law (Eyal Benvenisti & Georg Nolte, eds., Oxford University Press, Forthcoming), GWU Law School Public Law Research Paper 2017-67 (2018), 10 and 18.

⁵²⁸ For the full interview: Euractiv: *Schrems: round three* (4 November 2022)

<https://www.euractiv.com/section/digital/podcast/schrems-round-three/> (last visited 10 March 2023).

⁵²⁹ EDPB, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework (28 February 2023), pp. 1-54, https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf (last visited 10 March 2023).

⁵³⁰ EDPB, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework (28 February 2023), pp. 1-54, para. 89.

indicate that measures involving signals intelligence may only be taken to advance the collection of validated intelligence priorities, and only to the amount necessary and proportional to the validated intelligence priority.⁵³¹

Besides, Executive Order 14086 states 12 purposes for which collection is allowed as well as 5 objectives for which signals intelligence collection operations are prohibited.⁵³² Yet, we are concerned that the President might, if required, add new objectives to these lists for new national security reasons.⁵³³ The same holds true for bulk collection, and granting this ability to the President would be problematic due to the vast quantity of data collected in comparison to targeted collection.⁵³⁴ The EDPB is further concerned that the objectives and safeguards mentioned in the section of Executive Order 14086 referring to bulk collection do not apply to temporary bulk collection to support the technical phase of initiated signals intelligence collection operations.⁵³⁵ This temporary bulk collection should be retained for a short period of time and then removed; however, the retention term is not specified.⁵³⁶ This derogation criterion should also be considered by the Commission when evaluating adequacy.

We suggest that the President's power should be limited at least with regard to the bulk collection of personal data. In addition, the retention period under Executive Order 14086 is not specified, and there are no stringent safeguards for onward transfers.⁵³⁷ The EDPB notes that bilateral or multilateral agreements with third countries for intelligence cooperation

⁵³¹ Executive Order No. 14086, vol. 87 no. 198 Federal Register, 14.10.2022, pp. 62283-62297, Section 2, (a)(ii)A and B and EDPB, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework (28 February 2023), pp. 1-54, para. 125.

⁵³² Executive Order No. 14086, vol. 87 no. 198 Federal Register, 14.10.2022, pp. 62283-62297, Section 2, (b)(i)A, 1-12 and Executive Order No. 14086, vol. 87 no. 198 Federal Register, 14.10.2022, pp. 62283-62297, Section 2, (b)(ii)A, 1-5.

⁵³³ Executive Order No. 14086, vol. 87 no. 198 Federal Register, 14.10.2022, pp. 62283-62297, Section 2, (b)(i)B.

⁵³⁴ Executive Order No. 14086, vol. 87 no. 198 Federal Register, 14.10.2022, pp. 62283-62297, Section 2, (c)(ii)(C).

⁵³⁵ EDPB, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework (28 February 2023), pp. 1-54, para. 160.

⁵³⁶ Executive Order No. 14086, vol. 87 no. 198 Federal Register, 14.10.2022, pp. 62283-62297, Section 2, (c)(ii)(D), 1-3.

⁵³⁷ EDPB, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework (28 February 2023), pp. 1-54, para. 163.

might have an effect on the rules for onward transfer.⁵³⁸ EDPB did not specifically provide any instances for such agreements, however here we may provide the example of Five Eyes as previously discussed. Hence, the Commission should consider these agreements and their provisions in its assessment of adequacy. Moreover, the Commission should assess the necessity for a specific retention period, particularly with regards to bulk collections (including temporary bulk collections). It is also important to clarify whether temporary bulk collections should only be carried out for the objectives listed under Executive Order 14086 when collecting personal data of EU residents and citizens, and not for any other objectives.

Furthermore, the new Executive Order establishes Data Protection Review Court (DPRC) to review and address complaints about US national intelligence agencies' access to EU data subjects' data. In order to implement the additional mandated safeguards, the Executive Order requires intelligence agencies to examine and update their rules and procedures.⁵³⁹ *Max Schrems* claims that he is ready for the third round, as these promises of effective redress mechanisms appear to be the same ineffective processes as previous ones.⁵⁴⁰ In our humble opinion, before the DPRC is operating, it is not possible to evaluate whether or not it will be truly impartial and independent, as intended.

What assurances does the "two-layer" redress mechanism offer? Under the first layer, the Civil Liberties Protection Officer in the Office of the Director of National Intelligence (CLPO) will conduct an initial investigation on EU complaints to determine whether EU individuals' rights and freedoms have been violated. And if so, the Officer will determine the appropriate remedy for those violations and ensure the compliance of US intelligence agencies with the privacy rights.⁵⁴¹

Based on the second layer, EU citizens have the right to appeal the decisions of the Civil Liberties Protection Officer before the newly established Data Protection Review Court (DPRC). The DPRC is comprised of qualified individuals selected from outside the US

⁵³⁸ EDPB, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework (28 February 2023), pp. 1-54, para. 154.

⁵³⁹ The White House: Fact Sheet: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework (7 October 2022), <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/> (last visited 10 March 2023).

⁵⁴⁰ For the full interview: Euractiv: Schrems: round three (4 November 2022) <https://www.euractiv.com/section/digital/podcast/schrems-round-three/> (last visited 10 March 2023).

⁵⁴¹ The White House: Fact Sheet: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework (7 October 2022), <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/> (last visited 10 March 2023).

Government. They cannot be ignored absent convincing reasons (e.g., they have convicted a crime, they have been deemed by serious mental or physical issues that they cannot perform their tasks anymore). This court can issue binding decisions, for instance, if it determines that intelligence agencies have violated the privacy rights of EU citizens, it can compel the erasure of the transferred data. The Executive Order also required that the DPRC select an advocate for each case to represent the complainants' concerns and interests before the court, so ensuring the fair trial concept.⁵⁴² The Attorney General established regulations to accompany the DPRC's establishment.⁵⁴³ The previous Ombudsman procedure lacked independence since the Ombudsman was part of the US Department of State and lacked the same investigative or decision-making authority. Therefore, we may conclude that the new oversight mechanism is more promising and gives us greater confidence that this system will function more efficiently this time.⁵⁴⁴

Inter alia, in one of our published articles, we reviewed the European Commission's adequacy decision for Japan, and we concluded that:

“Japan’s adequacy decision was chosen because Japan’s data protection and privacy perspective is comparable to that of the United States, in that personal data is regarded as an economic commodity, in contrast to the EU’s fundamental right approach. Consequently, its adequacy decision can serve as a model for the US to have two-way data protection; one way, which is the current situation, may be maintained for US citizens and residents, while the other way, which includes stricter rules with the Japan’s Supplementary Rules, including effective oversight and redress mechanisms, may be adopted only for EU citizens and residents. In addition, public authorities’ access to the personal data of the EU data subjects should be restricted and proportional.”⁵⁴⁵

As a matter of fact, the new Transatlantic Data Privacy Framework also offers a two-way approach through the development of a system that will fulfil stricter criteria for EU

⁵⁴² 28 CFR 201 Data Protection Review Court, Final Rule, 28 U.S.C §§ 509, 510-512, Federal Register Vol. 87, No. 198, 14.10.2022, pp. 62303-62308.

⁵⁴³ The White House: Fact Sheet: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework (7 October 2022), <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/> (last visited 10 March 2023).

⁵⁴⁴ European Commission: Questions & Answers: EU-U.S. Data Privacy Framework (7 October 2022) https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_6045 (last visited 10 March 2023).

⁵⁴⁵ Asli Alkis-Tümtürk: Uncertain future of transatlantic data flows: Will the United States ever achieve the ‘adequate level’ of data protection?, Hungarian Journal of Legal Studies, vol. 63 issue. 3 (2022), 307.

residents and citizens than for US residents and citizens, which is quite similar to the Japan example.

Last but not least, the new Transatlantic Data Privacy Framework should include regulations for the transfer of children's data between the EU and the US. Because the COPPA defines a child as an individual less than 13 years of age.⁵⁴⁶ Consequently, it means that any child who is 13-year-old or older can consent to the processing of their personal data under the US legislation. However, under the GDPR, a child cannot consent to the processing of their personal data until the age of 16 in certain EU Member States (e.g., Hungary, Germany), 15 in certain Member States (e.g., France, Greece), and 14 in certain Member States (e.g., Italy, Spain).⁵⁴⁷

It means that in some EU Member States, children older than 13 still need parental consent for data controllers to process their personal information; otherwise, the processing would be unlawful. Suppose, for example, that a company in the US intends to transfer children's data from an EU member state, such as Hungary. Both the US company importing the data and the Hungarian company exporting it should exercise extreme caution, as the consent of a 14-year-old Hungarian child for the transfer of personal data to the US is invalid without parental consent, although it is valid under US legislation.

This is a really significant topic, but policymakers consistently disregard it. In the upcoming third round, there should be rules and regulations governing the transfer of children's data and the difference in age requirement between US and EU countries. Because without the regulations, the responsibility would fall on the data importers and exporters, who would be obligated to make all reasonable efforts to protect the privacy rights of children's data.⁵⁴⁸

Yet, instead of making reasonable efforts, data controllers choose to close their eyes and disregard the fact that children have online accounts and engage in online activities on their websites by prohibiting them access.⁵⁴⁹ Yet, ignoring their online presence does not prevent

⁵⁴⁶ 16 CFR COPPA 312.2 “Child” : “means an individual under the age of 13.”

⁵⁴⁷ EuConsent, Digital Age of Consent under the GDPR: <https://euconsent.eu/digital-age-of-consent-under-the-gdpr/#:~:text=As%20per%20Article%208%20of,at%20least%2016%20years%20old> (last visited 10 March 2023).

⁵⁴⁸ “The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.” GDPR, Article 8(2).

⁵⁴⁹ For example, see Instagram’s privacy policy prohibiting the children’s access: “Instagram requires everyone to be at least 13 years old before they can create an account (in some jurisdictions, this age limit may be higher). Accounts that represent someone under the age of 13 must clearly state in the account's bio

children from having accounts, and as we mentioned in Chapter 3.4, it is easy for children to lie about their age and sign up. This means that disregarding the issue is not a solution, but establishing a framework that can accommodate the data flow of children from the EU to the US may be.

For example, while Facebook's privacy policy requires children to be at least 13 years old and may be higher in some jurisdictions, children who are 13 years old can create a Facebook account in Hungary, and their data will be transferred to the US.⁵⁵⁰ By pretending as a 13-year-old child in Hungary, we were successful in creating a Facebook account using dummy data and a phone number to validate the account, and Facebook did not need parental consent verification. There might be parents that provide consent for their children to have accounts. This, however, is immaterial. The main point we would like to make here is that Facebook's action violates Hungarian data protection legislation. If no one reports this account, Facebook has no recourse to delete it and will continue processing personal data as if it were lawful, despite the fact that it is illegal in Hungary to process the personal data of children under 16 without parental consent.⁵⁵¹

Facebook does not appear to be aware of the digital age of consent in any other Member State but Spain, where they have included a form on their website so that anybody may report the existence of a Facebook account for a child under 14 in Spain. They state that they respect

that the account is managed by a parent or manager. If your child is younger than 13 and has an account that isn't managed by you or a manager, you can show them how to delete their account.”

Instagram Help Centre, Tips for parents: How do I report a child under the age of 13 on Instagram?

<https://help.instagram.com/154475974694511> (last visited 10 March 2023).

See Facebook's privacy policy: “Facebook requires everyone to be at least 13 years old before they can create an account (in some jurisdictions, this age limit may be higher). Creating an account with false info is a breach of our terms. This includes accounts registered on behalf of someone under 13. If your underage child created an account on Facebook, you can show them how to delete their account. If you'd like to report an account belonging to someone under 13, please fill in this form. Please note that we'll promptly delete the account of any child under the age of 13 that's reported to us through this form.”

Facebook Help Centre, Reporting abuse: How do I report a child under the age of 13 on Facebook?,

https://www.facebook.com/help/157793540954833/?helpref=uf_share (last visited 10 March 2023).

⁵⁵⁰ “Information controlled by Meta Platforms Ireland Limited will be transferred or transmitted to, or stored and processed in:

Places we have infrastructure or data centres, including the United States, Ireland, Denmark and Sweden, amongst others

Countries where Meta Company Products are available

Other countries where our partners, vendors, service providers and third parties are located outside of the country where you live, for purposes as described in this Policy”

Facebook, Privacy Centre: Where is information transferred?

<https://www.facebook.com/privacy/policy/?subpage=9.subpage.2-WhereIsInformationTransferred> (last

visited 10 March 2023). Please note that the author successfully created a Facebook account for a 13-year-old using dummy data in Hungary.

⁵⁵¹ 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, cikk 5 §(3).

local regulations, however it appears that the procedure for deleting accounts is complaint-driven.⁵⁵²

Given the information presented above, we suggest that establishing a consistent age for everyone would be a far preferable and more viable approach in terms of cross-border data transferring. However, because this is not currently the case, this issue should be considered in the upcoming transatlantic data privacy framework, and the EU and US should reach an agreement on a solution to establish a more stable and assured environment for data exporters and importers.

For instance, potential self-certifying US-based companies may be challenged to prove compliance with local child privacy laws. If they cannot provide this evidence, they will not be deemed to have an adequate level of data protection and will not be certified under the new transatlantic data privacy framework. Google, unlike Facebook, does not allow children under 16 to create accounts in Hungary due to local privacy regulations.⁵⁵³ This demonstrates that this solution is feasible so long as companies pay attention to domestic jurisdictions and use privacy-friendly measures.

To sum up, in our previous article regarding transatlantic data transfers, we suggested that:

“[t]he best and quickest way for the US to achieve an adequate level of data protection may be a two-way data protection approach with stricter Supplementary Rules covering only EU data subjects; requiring intelligence services to stop accessing data received from the EU unless there is a reasonable concern for national security; ensuring an independent oversight mechanism; and providing effective redress mechanisms especially in the event of intelligence services’ non-proportional and limitless access.”

The Executive Order to Implement the EU-US Data Privacy Framework signed by *Joe Biden* appears to include the main suggestions and exceptions outlined in our previous article. *Max Schrems* or another challenger will not need to go to the third round if all of their pledges are fulfilled and if they handle the issues about the bulk collection and the

⁵⁵² Facebook, Help Centre: How do I report a child under the age of 14 on Facebook in South Korea or Spain?, https://www.facebook.com/help/100532533374396/?helpref=uf_share (last visited 10 March 2023). See the reporting form only for Spain and South Korea:

<https://www.facebook.com/help/contact/1408156889442791> (last visited 10 March 2023).

⁵⁵³ Google, Help Centre: Age requirements on Google Accounts, Find your country’s age requirement, <https://support.google.com/accounts/answer/1350409?hl=en#zippy=%2CEurope> (last visited 10 March 2023).

Please note that the author could not create a Google account for a 13-year-old using dummy data in Hungary.

proportionality and necessary criteria highlighted in the EDPB's Opinion appropriately. Even if one persists on proceeding, the potential Schrems III case would have little chance of succeeding under the anticipated and desired conditions. This time, we are more optimistic, because the two-way model is already working for Japan. Nonetheless, we will have a clearer picture once the new transatlantic data privacy framework goes into effect. Finally, and most crucially, we expect and strongly advocate for more restricted and stringent rules and guidelines regulating the transfer of children's data, as mentioned in this chapter.

6.8 Short Summary

In this chapter, we have discussed how data flow is a critical component of the global digital economy. The GDPR clearly states that data transfer between data controllers in EU countries and data controllers in third countries or international organisations is required for the growth of international trade and cooperation. However, due to fundamental disparities between the EU and the US in terms of privacy and data protection, there hasn't been a permanent and stable solution for data transfers from the US to the EU yet. Accordingly, they've been negotiating free data flow agreements for several years.

We began with adequacy decisions issued by the European Commission and went on to explore the Safe Harbour and Privacy Shield in depth, as well as how and why they were terminated by the CJEU in the Schrems I and Schrems II cases. Afterwards, we examined the current situation in the absence of adequacy decisions. Particularly, the commonly used SCCs were thoroughly explained. However, we asserted that they need case-by-case analysis and place significant burdens on data importers and exporters. As a result of these difficulties and the uncertain environment, we remarked that data localisation, which contradicts the GDPR's aims and objectives, may occur.

Hence, we noted that the EU and the US are currently preparing to establish a new Transatlantic Data Privacy Framework in order to create a more trustworthy and stable environment. We stated that this new framework contains considerable improvements with its two-way approach. This approach provides better protection for the EU residents and citizens comparing to the US residents and citizens.

In addition to those, we have discussed that the GDPR has no specific provisions regulating the transfer of children's data. However, we have suggested that children's data should be regarded distinct categories of data and handled differently and with greater care than adult data transfers. Besides we claimed that the varying age of digital consent across

the EU Member States could cause a significant problem when transferring data inside the EU and to the US. Thus, we concluded that the future Transatlantic Data Privacy Framework should include specific regulation governing the flow of children's data from the EU to the US.

Furthermore, we suggested that the two-way approach, the two-layer redress and oversight mechanism appear to be quite promising this time in terms of US finally having the adequate level of data protection. We have noted that the concerns mentioned regarding the proportionality and necessity principles and bulk collections should be addressed properly. Notably, we completed the chapter by asserting that we anticipate stricter regulations covering the transfer of children's data.

7. Examples from the practice - Social networking services, privacy policies, child influencers and parental sharing

The sociology and culture of memory sharing have been modified by social networking sites. Once upon a time, our family vacations, birthday parties, and graduation ceremonies were preserved solely in photo albums that were presented to visiting relatives. The most private aspects of children's lives and experiences were only disclosed over the phone or at family gatherings with family members and close friends. Child actors, models, and musicians were the only children whose photos and videos were available to the public. Nevertheless, those family photo albums are now accessible to the whole Internet community via social media; hence, every child has the potential to become a minor celebrity or child influencer with relative ease. Prior to the emergence of social networking sites such as Facebook, Instagram, and YouTube, children's privacy and data protection were not as significant concerns as they are currently.⁵⁵⁴

As Facebook, Instagram, and YouTube are the most popular social networks in the world.⁵⁵⁵ We will explore their data policies and practises concerning the privacy of children in this chapter. Since the Federal Trade Commission (FTC) considers children under the age of 13 to be vulnerable,⁵⁵⁶ and the COPPA rule defines a child as an individual under the age of 13,⁵⁵⁷ the majority of US-based social media platforms, including Facebook, Instagram, and YouTube, do not allow children under the age of 13 to have accounts.⁵⁵⁸ However, parents who post their children's who are younger than 13 material, images, and/or videos

⁵⁵⁴ Shannon Sorensen: Protecting Children's Right to Privacy in the Digital Age: Parents as Trustees of Children's Rights, *Children's Legal Rights Journal* 36, no. 3 (2016), 156-157.

⁵⁵⁵ Statista: Most popular social networks worldwide as of January 2022, ranked by number of monthly active users (in millions), <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/> (last visited 10 March 2023).

⁵⁵⁶ "In enacting the Children's Online Privacy Protection Act, Congress determined to apply the statute's protections only to children under 13, recognizing that younger children are particularly vulnerable to overreaching by marketers and may not understand the safety and privacy issues created by the online collection of personal information." Federal Trade Commission: Complying with COPPA: Frequently Asked Questions, Why does COPPA apply only to children under 13? What about protecting the online privacy of teens? <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions> (last visited 10 March 2023).

⁵⁵⁷ 16 CFR COPPA 312.2 "Child": "means an individual under the age of 13."

⁵⁵⁸ Facebook Help Center, How to Report Things, How do I report a child under the age of 13 on Facebook?: https://www.facebook.com/help/157793540954833/?helpref=uf_share (last visited 10 March 2023)

Instagram, Help Centre, Tips for Parents: How do I report a child under the age of 13 on Instagram? https://help.instagram.com/517920941588885/?helpref=uf_share (last visited 10 March 2023).

YouTube, Terms of Service, General Terms and Conditions: Who can use the service?, Age requirements <https://kids.youtube.com/t/terms> (last visited 10 March 2023).

online suffer no consequences and are not subject to any legal restrictions under COPPA or GDPR.⁵⁵⁹

It is an improvement that both the GDPR and the COPPA require parents to be accountable for their children's data protection and privacy. In other words, it is better than disregarding the presence of children in the online world. However, this is not always a wise idea, because some parents lack digital literacy skills or technology understanding and do not know what is best for their children. On the other side, there are those parents who are either oblivious to what is best for their children or are malicious. Consequently, they might share their children's digital footprints without understanding or ignoring the long-term consequences for their children's futures.⁵⁶⁰

Children's self-confidence, personal growth, and future academic and professional opportunities might all be damaged as a result of adults revealing an excessive amount of personal information and embarrassing anecdotes, images, and videos about the children in their lives. These kinds of posts also have the potential to lead to identity theft, cyberbullying, or bullying among peers or adults in the physical world (e.g., at the school or family gatherings).⁵⁶¹

In earlier chapters on the data protection and privacy rights of children, we discussed the tragic case of Amanda Todd, a Canadian girl who committed suicide after losing control over her personal data. We stated that she was subjected to long-term bullying because of a single photograph that she was unable to delete. Before her suicide, Amanda had prepared a YouTube video in which she told her tale through a series of handwritten letters. On one of the notes, Amanda writes, “*I'll never get the photo back; it's out there forever...*” These kinds of occurrences are possible for any youngster who endures long-term, severe bullying and blackmail.⁵⁶²

As with Amanda Todd, such occurrences may be caused by parental neglect. Nonetheless, we should also highlight that in Amanda's situation, not only her parents but

⁵⁵⁹ Asli Alkis Tümtürk: Implications of Parental Sharing of Children's Personal Data Online, *ArsBoni Jogi Folyoirat*, X. evfolyam 2022/1-2 (2022), 3 available at https://arsboni.hu/wp-content/uploads/2022/09/Arsboni-foly%C3%B3irat_2022_1_2.pdf (last visited 10 March 2023).

⁵⁶⁰ Asli Alkis Tümtürk: Implications of Parental Sharing of Children's Personal Data Online, *ArsBoni Jogi Folyoirat*, X. evfolyam 2022/1-2 (2022), 3 available at https://arsboni.hu/wp-content/uploads/2022/09/Arsboni-foly%C3%B3irat_2022_1_2.pdf (last visited 10 March 2023).

⁵⁶¹ Haley Keltie: Sharenting and the (Potential) Right to Be Forgotten, *Ind. LJ*, 95 (2020), 1006.

⁵⁶² My story: Struggling, bullying, suicide, self-harm, *Thesomebodytoknow* videos, available at: <https://www.youtube.com/watch?v=vOHXGNx-E7E> (10 March 2023) cited in Bunn Anna: Children and the 'Right to be Forgotten': What the right to erasure means for European children, and why Australian children should be afforded a similar right, *Media International Australia*, 170(1) (2019), 41.

also law enforcement officers were incompetent. Amanda Todd's Facebook account was suggested to be deleted by RCMP (Royal Canadian Mounted Police) officers as if it was the only alternative.⁵⁶³ Consequently, her parents urged her to deactivate her Facebook account, which she did for a few months without any positive outcomes.⁵⁶⁴ Amanda's response to the police officer's query about why she communicates with so many strangers online was heart-breaking: "I am lonely."⁵⁶⁵

Aydin Coban, a Dutch man suspected of sexual extortion, child luring, child pornography, and harassment, was not apprehended at the time owing to either a lack of technical infrastructure or inattentive police and law enforcement.⁵⁶⁶ The perpetrator was sentenced to 13 years in jail after a decade, however his crimes do not entail teenage suicide solicitation.⁵⁶⁷

The "right to be forgotten" provisions of the GDPR have been investigated in previous chapters; nevertheless, they only serve to erase the revealed material from the Internet and usually from search engines' results. However, after the information has been downloaded to the computer of the malevolent person, the right to be forgotten is no longer functional.⁵⁶⁸ Nevertheless, this right is vital for children to regain control over the data that pertains to them.

In today's digital age, it may not be reasonable to expect parents to share no information or to prohibit their children from sharing one at all, but there should be a balance between online sharing activities and freedom of expression and children's right to a private life.⁵⁶⁹ Accordingly, in this chapter, we will offer examples of child influencers and evaluate the

⁵⁶³ CBC News: Parents, Dutch police investigator testify in trial of man accused of cyberbullying Amanda Todd, (11 June 2022) <https://www.cbc.ca/news/canada/british-columbia/amanda-todd-week-one-1.6485200> (last visited 10 March 2023).

⁵⁶⁴ CBC News: Amanda Todd's parents recall teenager's anguish at recurring social media torment (7 June 2022) <https://www.cbc.ca/news/canada/british-columbia/todd-sextortion-trial-coban-1.6480477> (last visited 10 March 2023).

⁵⁶⁵ Global News: Exclusive: Mountie who worked Amanda Todd case speaks for first time (10 August 2022) <https://globalnews.ca/news/9050914/amanda-todd-officer-speaks/> (last visited 10 March 2023).

⁵⁶⁶ "Schadeck (*retired RCMP constable*) said she did not hold a high enough rank to know why the training or technology wasn't there to track down Coban at the time. Those tools, she added, may have improved in the decade since. But she said she still feels the system failed the teen's family." Global News: Exclusive: Mountie who worked Amanda Todd case speaks for first time (10 August 2022) <https://globalnews.ca/news/9050914/amanda-todd-officer-speaks/> (last visited 10 March 2023).

⁵⁶⁷ BBC News: Amanda Todd: Dutchman sentenced for fatal cyber-stalking (15 October 2022) <https://www.bbc.com/news/world-us-canada-63218797> (last visited 10 March 2023).

⁵⁶⁸ Asli Alkis Tümtürk: Implications of Parental Sharing of Children's Personal Data Online, *ArsBoni Jogi Folyoirat*, X. evfolyam 2022/1-2 (2022), 3 available at https://arsboni.hu/wp-content/uploads/2022/09/Arsboni-foly%C3%B3irat_2022_1_2.pdf (last visited 10 March 2023).

⁵⁶⁹ Stacey B. Steinberg: Sharenting: Children's Privacy in the Age of Social Media, *Emory Law Journal* 66, no. 4 (2017), 876-877.

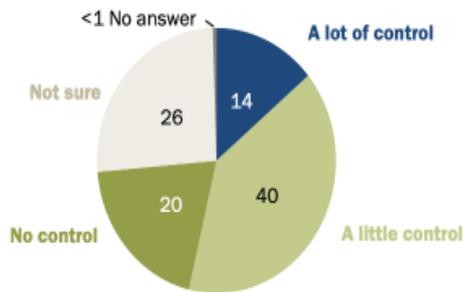
consequences and potential risks of parental sharing on these social media sites while addressing the balanced-rights approach, including the protection of children's privacy rights and the freedom of online expression for parents. In conclusion, we will attempt to offer suggestions for improving practises and privacy policies, as well as mitigating the risks associated with online sharing.

Since today's children, known as Generation Z, have grown up with computers and other electronic gadgets at their fingertips from an early age, they are more skilled at using them than their parents have been. They have been early adopters of several forms of technology, beginning use of computers, tablets, and smartphones. Within a decade or two, children surpassed their parents' competence with these devices, but they still lack an understanding for the need of privacy and data protection, the potential consequences of their online actions, or the inevitable unpredictability of the Internet.⁵⁷⁰

⁵⁷⁰ Sheila Donovan: 'Sharenting': The Forgotten Children of the GDPR, *Peace Human Rights Governance* 4(1), (2020), 43.

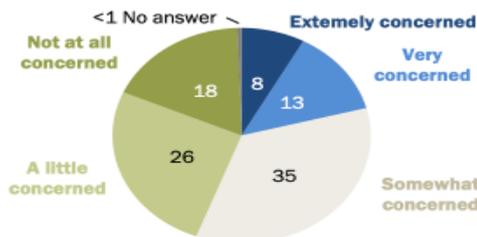
A majority of teens feel as if they have little to no control over their data being collected by social media companies ...

% of U.S. teens who say they think they have ___ over the personal information that social media companies collect about them



... but only one-in-five are extremely or very concerned about the amount of information these sites have about them

% of U.S. teens who say they are ___ about the amount of personal information social media companies might know about them



Note: Teens are those ages 13 to 17. Values may not add up to 100% due to rounding. Figures may not add up to NET values due to rounding.
 Source: Survey conducted April 14-May 4, 2022.
 "Connection, Creativity and Drama: Teen Life on Social Media in 2022"

PEW RESEARCH CENTER

Chart 5 and 6: How much control teenagers have over their data and how much they worry about it⁵⁷¹

For example, according to a Pew Research Center study, the majority of teenagers (60%) feel they have little control over the data collected by social media companies. Nonetheless, they are not much concerned about it, as seen in the above pie charts. Only 21% of respondents said that they are very or extremely concerned about the information these social media sites have on them. However, 44% of them have little to no concern regarding the amount of information that these businesses may possess. As seen, even relatively older children seem unconcerned, and it is reasonable to infer that younger children are much more

⁵⁷¹ Pew Research Center, Connection, Creativity and Drama: Teen Life on Social Media in 2022 (16 November 2022) <https://www.pewresearch.org/internet/2022/11/16/connection-creativity-and-drama-teen-life-on-social-media-in-2022/> (last visited 10 March 2023).

oblivious to the repercussions of social media companies knowing a great deal about them and their personal life.

While the focus of the survey is on how companies may access children's personal information, the results indicate that teenagers are more concerned with keeping their information protected from people than from companies. Hence, their notion of digital privacy relates to other individuals using these social media platforms rather than social media service providers or advertising companies, as evidenced by the responses of anonymous teenagers within the scope of this study⁵⁷²:

“What do you mean by digital privacy? ... I feel like all of my social media accounts personally are privated, so only the people I let follow me can see the stuff I post. I would feel weird if anyone could see my videos and stuff, I don't know.” – Teen girl

“I would describe it as keeping your personal life separate from your online identity and keeping that information off the internet.” – Teen boy

“Okay, what do you mean by digital privacy? You mean that any information I use on a social media platform does not go out to people, my phone number, my pictures, my videos are safe on that platform. ... My data [is] not being shared with anyone, that's what I understand by privacy.” – Teen boy

“I have private stories. I have a normal story where everybody can see it and then I have a private story just for my personal friends that I hang out with all the time and talk to all the time.” – Teen boy

“I don't like to post – say it's a funny picture or something – on my main story. Private story is more [for] like your close friends, the people you talk to. Not really family. Unless it's a cousin you're close with.” – Teen girl

Some teenagers answer that they have not given much thought to how companies may utilise their personal information. However, several are aware that social networking sites are monitoring them⁵⁷³:

“Social media groups use [data] to get insight on what people are into, or what they think users spend most of their time doing. So, it's more like they still use it to get better data

⁵⁷² Pew Research Center, Connection, Creativity and Drama: Teen Life on Social Media in 2022: Teens have a range of definitions for digital privacy (16 November 2022) <https://www.pewresearch.org/internet/2022/11/16/connection-creativity-and-drama-teen-life-on-social-media-in-2022/> (last visited 10 March 2023).

⁵⁷³ Pew Research Center, Teens' views about social media: In their own words: Teens explain what they think social media companies do with their data (16 November 2022) <https://www.pewresearch.org/internet/2022/11/16/2-teens-views-about-social-media/> (last visited 10 March 2023).

on people, on what people spend most of your time doing, searching online and that's just what I think. I'm not really sure."⁵⁷⁴ – Anonymous teen boy

“Something that I always felt was kind of weird about social media is, let's say you search up one thing on a platform and then it appears on another. So, that does show that social media does use that information. ... It's weird to know that they're tracking certain things. Like, let's say I'm shopping for something on one account and then it pops up as an ad for something else. It makes me a little uncomfortable almost.”⁵⁷⁵ – Anonymous teen girl

“I've seen some things like about it. I'm pretty sure they take the information about what you're interested in and things like that. And then they sell that to advertisers to try and get you to buy their products and things like that.”⁵⁷⁶ – Anonymous teen boy

“In grade school, I'm pretty sure one of my teachers did a study [where] she posted something online and then on her Amazon account she was getting recommended stuff [based] on what she posted. So I think they try to get you to buy things off what your interests are.”⁵⁷⁷ – Anonymous teen boy

Teens are vaguely aware of the tracking of social media sites, but they are unconcerned about it since they do not fully understand the effects of profiling and behavioural marketing. An EU study on the impact of marketing through social media, online games, and mobile applications on children's behaviour found that marketing practises of companies have clear and sometimes subliminal effects on children's consuming habits, meaning that they influence children's behaviour without their knowledge.⁵⁷⁸

But what happens if the parents also lack digital literacy, and they are not aware of the need of privacy and hazards of Internet? According to the same EU study referenced above,

⁵⁷⁴ Pew Research Center, Teens' views about social media: In their own words: Teens explain what they think social media companies do with their data (16 November 2022) <https://www.pewresearch.org/internet/2022/11/16/2-teens-views-about-social-media/> (last visited 10 March 2023).

⁵⁷⁵ Pew Research Center, Teens' views about social media: In their own words: Teens explain what they think social media companies do with their data (16 November 2022) <https://www.pewresearch.org/internet/2022/11/16/2-teens-views-about-social-media/> (last visited 10 March 2023).

⁵⁷⁶ Pew Research Center, Teens' views about social media: In their own words: Teens explain what they think social media companies do with their data (16 November 2022) <https://www.pewresearch.org/internet/2022/11/16/2-teens-views-about-social-media/> (last visited 10 March 2023).

⁵⁷⁷ Pew Research Center, Teens' views about social media: In their own words: Teens explain what they think social media companies do with their data (16 November 2022) <https://www.pewresearch.org/internet/2022/11/16/2-teens-views-about-social-media/> (last visited 10 March 2023).

⁵⁷⁸ European Commission, Study on the impact of marketing through social media, online games and mobile applications on children's behaviour (1 March 2016) https://commission.europa.eu/publications/study-impact-marketing-through-social-media-online-games-and-mobile-applications-childrens-behaviour_en (last visited 10 March 2023).

the majority of parents do not perceive online marketing directed at their children as problematic and believe their children are not influenced. Many parents are unprepared to protect their children's digital privacy, despite the fact that COPPA and the GDPR impose a considerable responsibility to do so. According to the study, parental approaches to managing their children's internet behaviour vary by country. In France, for instance, parents intervene less with their children's internet use, but Swedish parents are more involved and restricting with their children's online activities.⁵⁷⁹

What occurs regardless of whether parents are aware of the hazards of parental sharing and are reluctant to forego the advantages of posting updates on their children on social media platforms? What might be the advantages of parents revealing their children's most private moments? It might be feeling less alone and receiving support from other parents who are experiencing the same difficulties. Sharing the videos/photos of their children with relatives and friends who liked and commented on the shared postings enabled them to feel close and connected. Additionally, these shared experiences offer them with the approval they require when parenting. Parents want to be seen as good parents and Facebook, Instagram and YouTube posts assist them to fulfil the expectations of parents and offer them a positive online image of parenting. Earning money to save for their children's future or to provide them with a higher quality of living might be another motive for parents, given that collaborations with brand owners and advertising their products would generate a substantial amount of money.⁵⁸⁰

However, can it be said that these benefits outweigh the children's right to data protection and privacy? On one hand, parents may defend their online sharing activities based on their right to free speech. Indeed, everyone has the right to freedom of speech, as stated in Article 11 of the CFR, which includes the freedom to hold opinions as well as the

⁵⁷⁹ European Commission, Study on the impact of marketing through social media, online games and mobile applications on children's behaviour (1 March 2016) https://commission.europa.eu/publications/study-impact-marketing-through-social-media-online-games-and-mobile-applications-childrens-behaviour_en (last visited 10 March 2023).

⁵⁸⁰ Gaëlle Ouvrein and Karen Verswijvel: Sharenting: Parental adoration or public humiliation? A focus group study on adolescents' experiences with sharenting against the background of their own impression management, *Children and Youth Services Review* 99 (2019), 320.

freedom to receive and share information and ideas.⁵⁸¹ Regarding US, the freedom of speech is guaranteed by the first amendment of the US Constitution.⁵⁸²

On the other hand, as stated by the ECHR, freedom of expression should be limited so that it does not harm the reputation of others.⁵⁸³ The US government also restricts freedom of expression in certain categories, such as privacy invasion and the visual representation of children engaging in a variety of sexual activities or genital exposures in films or photographs.⁵⁸⁴ The sharing of naked photographs and the most intimate moments of children by millions of families is extremely likely to harm the children's self-esteem and dignity as well as their privacy, considering toilet training and the first bath as examples.

Sidis v. F-R Publishing is an example of an earlier case from the US that supports this viewpoint as it was also discussed in the previous chapter regarding the main rights of the children and their parents under the GDPR and COPPA. As a child prodigy in the early 1900s, Sidis rose to prominence in the public eye, but as he reached adulthood, he decided he did not want to continue to be in the spotlight. However, without his desire, *The New Yorker* published an article on him, and as a result, he decided to sue the publication. The judge concluded that Sidis, just like any other public person, was unable to hide from the scrutiny of the public. The court recognised that a person had the right to privacy and that

⁵⁸¹ Charter of Fundamental Rights of The European Union, OJ C 364, 18.12.2000, pp. 1-22, Article 11: “1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. 2. The freedom and pluralism of the media shall be respected.”

⁵⁸² U.S. Const. amend. I: “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.”

⁵⁸³ Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 04.11.1950, ETS 5, Article 10: “1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.”

⁵⁸⁴ The US government restricts the following categories of speech content: “Seditious Speech and Seditious Libel, Fighting Words and Other Threats to the Peace, Threats of Violence Against Individuals, Group Libel, Hate Speech, Defamation, False Statements, Invasion of Privacy, Emotional Distress Tort Actions, “Right of Publicity” Tort Actions, Publication of Legally Confidential Information, Obscenity, Child Pornography, Non-obscene But Sexually Explicit and Indecent Expression.” U.S. Government Publishing Office (GPO): *The Constitution of the United States of America Analysis and Interpretation Centennial Edition Interim Edition: Analysis of Cases Decided by the Supreme Court of the United States to June 27, 2016*, 112th Congress 2nd Session, Document No: 112-9, pp. 1-2835, 1285 et seq.

they had an interest in maintaining their private; yet they also accepted that the public had an interest in gaining knowledge about his life.⁵⁸⁵ Is it realistic to ask someone like Sidis, whose parents made a decision that thrust them into the public eye, to give up their right to privacy as a result of that decision? What if today's child influencers grow up to be adults who are unable to exercise the right to have their privacy respected simply because they have already been elevated to the status of public figures without their consent or knowledge? In our opinion, it would not be fair to draw conclusions about an adult's request based on the actions or behaviours of their parents in the past. This opinion is justified by the right to informational self-determination, which gives individuals control over their data by enabling them to choose when and for what purposes their personal information may be used and shared with third parties.⁵⁸⁶

In Europe, the German Federal Constitutional Court was the first to enunciate the concept of informational self-determination.⁵⁸⁷ Afterwards, it became one of the foundational pillars of Article 8 of the CFR's right to protection of personal data.⁵⁸⁸ Finally, it is consistent with the spirit of the GDPR, which offers people more control over their data⁵⁸⁹, for example by assuring the rights to access, rectify, delete, and object. In addition, the duties imposed by GDPR on data controllers, such as notifying the subject and obtaining consent, would be also based on the right to informational self-determination.⁵⁹⁰

At this time, we should argue whether or not children have the right to informational self-determination. When we examine Article 8 of the GDPR and the COPPA, we can generally assert that parents have the right to informational self-determination on their

⁵⁸⁵ Case 113 F.2d 806, *Sidis v. F-R Pub. Corporation* (No. 400), Judgement of the Court of Appeals for the Second Circuit, New York, 22 July 1940 cited in Stacey B. Steinberg: *Sharenting: Children's privacy in the age of social media*, *Emory LJ*, 66 (2016), 859-860.

⁵⁸⁶ Paul M. Schwartz: *Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, the State, and New Technology*, *William and Mary Law Review* 53, no. 2 (2011), 368 cited in Florent Thouvenin: *Informational Self-Determination: A Convincing Rationale for Data Protection Law?*, *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 12, no. 4 (2021), 248.

⁵⁸⁷ BVerfG, Order of the First Senate of 15 December 1983 - 1 BvR 209/83 -, paras. 1-214, BVerfGE 65, 1 - 71 Volkszählung.

⁵⁸⁸ Florent Thouvenin: *Informational Self-Determination: A Convincing Rationale for Data Protection Law?*, *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 12, no. 4 (2021), 248. CFR Article 8 provides the individuals control over their data with this paragraph: "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."

⁵⁸⁹ GDPR, Recital 7: "[...] Natural persons should have control of their own personal data. [...]".

⁵⁹⁰ Florent Thouvenin: *Informational Self-Determination: A Convincing Rationale for Data Protection Law?*, *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 12, no. 4 (2021), 250-252.

children's behalf. Parents may exercise this right by consenting to the processing of their children's personal data and by accessing, requesting rectification or deletion, and, if necessary, objecting to the processing.⁵⁹¹ Obviously, this right is not absolute; as children attain maturity, they may gain control over their data. This maturity is represented by the age of digital consent, which is 13 under the COPPA and 13 to 16 under the GDPR.⁵⁹² The content may also limit a parent's ability to exercise this right. If parents choose to post anything that might potentially compromise their children's privacy or future self-image, such as photos or videos of them engaging in activities that could be considered humiliating, then disclosing such content should be restricted.⁵⁹³

On the one hand, we think that it is a good idea to restrict children's right to informational self-determination until they reach maturity since they may not completely comprehend the repercussions of their online activities. However, as we mentioned previously in Chapter 4, when we discussed the privacy and data protection rights of children, if children (even if they are underage) choose to delete their data, this should indicate that the children are able to exercise their right to informational self-determination. Some less risky or risk-free online activities should be enabled by data controllers without parental consent.

Compared to Sidis' generation and the circumstances of the time, it is especially crucial to offer children greater control over their data, since parents now have more possibilities to share their children's family time and important events with the world through social media. Typically, children do not have a say in these postings before or after their parents share them. However, if they get a greater understanding of the repercussions of these sharing activities, they will be able to express their opinions and feelings about them more effectively and clearly. In fact, as already mentioned in the previous chapter regarding parental consent, a study conducted with 817 teenagers revealed that they are uncomfortable with their parents' social media posts about them and find them pointless and embarrassing.⁵⁹⁴

⁵⁹¹ For more information about the data protection and privacy rights of children and their parents see the Chapter 4 of this thesis.

⁵⁹² GDPR, Article 8 and 16 CFR COPPA 312.2 "Child".

⁵⁹³ The reason behind this restriction may be Preamble of the UNCRC as follows:

"Considering that the child should be fully prepared to live an individual life in society, and brought up in the spirit of the ideals proclaimed in the Charter of the United Nations, and in particular in the spirit of peace, dignity, tolerance, freedom, equality and solidarity, [...]" and the Article 16 of the UNCRC as follows: "No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation."

UNCRC, Article 16 and the Preamble.

⁵⁹⁴ Karen Verswijvel, Michel Walrave, Kris Hardies and Wannes Heirman: Sharenting, is it a good or a bad thing? Understanding how adolescents think and feel about sharenting on social network sites, *Children and youth services review* 104 (2019), 104401, 7.

Article 17 of the GDPR states that "the data subject shall have the right to obtain from the controller, without undue delay, the erasure of personal data concerning him or her where legal grounds apply."⁵⁹⁵ Moreover, the Recital (65) stipulates as follows:

“[...]That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. [...]”⁵⁹⁶

Moreover, Article 17(2) of the GDPR refers to the right to be forgotten as follows:

“Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.”

As discussed before in Chapter 4, the right to erasure allows individuals to request the deletion of their personal data, but the right to be forgotten is a broader concept that refers to the right of individuals to have specific information about them removed from the Internet (usually from the search engine results). Therefore, the right to be forgotten is a key aspect of the right to erasure in the GDPR.

Although freedom of speech is an exemption to the right to erasure and right to be forgotten under Article 17,⁵⁹⁷ where the data subject is a child, freedom of expression must be construed far more narrowly, as shown by *the Murray v. Express Newspapers Ltd (CA)* decision. The image of *J.K. Rowling's* son was shot by a photographer and published by a newspaper without his parents' consent. *J.K. Rowling* and her husband challenged this invasion of their son's privacy to court.⁵⁹⁸ The trial court ruled that publisher newspaper has the right to publish or acquire the publishing of the image in accordance with Article 10 of the European Convention on Human Rights.⁵⁹⁹ After this decision, *J.K. Rowling* and her husband filed an appeal, which the Court of Appeal allowed it on the grounds that:

⁵⁹⁵ GDPR, Article 17(1).

⁵⁹⁶ GDPR, Recital 65.

⁵⁹⁷ GDPR, Article 17(3)(a).

⁵⁹⁸ Case EWCA Civ446, *Murray v Express Newspapers plc and another*, Judgement of the Court of Appeal, England and Wales, 7 May 2008, 481.

⁵⁹⁹ Case EWCA Civ446, *Murray v Express Newspapers plc and another*, Judgement of the Court of Appeal, England and Wales, 7 May 2008, 512, para 62.

“The claimant's status as a child strongly enhances his claim to invoke the protection of article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms. In common with any other child, and regardless of who his mother is, the claimant has a reasonable expectation of privacy that he should be entitled to grow up and be brought up by his parents free from unwanted intrusion and interference by the media and, in particular, the paparazzi.”⁶⁰⁰

Accordingly, in the end, the Court of Appeal concluded that the balance between Article 8 (right to privacy) and Article 10 (right to freedom of speech) of the European Convention on Human Rights should favour the child's right to privacy.⁶⁰¹ In light of this example, and in our point of view, the Article 17 exemption referring to “exercising the right to freedom of speech and information” should not be invoked as a justification where the data subject is a child.⁶⁰²

As a result, we may infer that the right to be forgotten can strike a balance between the freedom of expression of parents and other adults and the right to a child's private life in favour of the child, and that it allows a child to regain control over his or her data. It does not imply that this right is absolute, because if one user downloaded the content of a child, no one can delete this information until the user removes it from their own device. However, the right to be forgotten remains a crucial right in terms of eliminating harmful material from the Internet, such as search engines (e.g., Google, Yandex etc.). This is the bare minimum that data controllers such as Google can do to assist children, and legislation and the government should also encourage data controllers to make it easier for children to exercise their right to be forgotten. Otherwise, terrible circumstances like the one with Amanda Todd might occur.⁶⁰³

Similar to the right to be forgotten, California implemented what is commonly known as the “Online Eraser Button Law”, which allows children to remove or de-identify online

⁶⁰⁰ Case EWCA Civ446, *Murray v Express Newspapers plc and another*, Judgement of the Court of Appeal, England and Wales, 7 May 2008, 485.

⁶⁰¹ Case EWCA Civ446, *Murray v Express Newspapers plc and another*, Judgement of the Court of Appeal, England and Wales, 7 May 2008, 512, para 62.

⁶⁰² Asli Alkis Tümtürk: Implications of Parental Sharing of Children’s Personal Data Online, *ArsBoni Jogi Folyoirat*, X. evfolyam 2022/1-2 (2022), 11 available at https://arsboni.hu/wp-content/uploads/2022/09/Arsboni-foly%C3%B3irat_2022_1_2.pdf (last visited 10 March 2023).

⁶⁰³ Asli Alkis Tümtürk: Implications of Parental Sharing of Children’s Personal Data Online, *ArsBoni Jogi Folyoirat*, X. evfolyam 2022/1-2 (2022), 11-12 available at https://arsboni.hu/wp-content/uploads/2022/09/Arsboni-foly%C3%B3irat_2022_1_2.pdf (last visited 10 March 2023).

material they uploaded.⁶⁰⁴ However, COPPA does not provide children with the right to be forgotten at the federal level. Instead, it gives parents the right to request the removal of content belonging to their children and to refuse to permit further collection or use of their children's data by data controllers.⁶⁰⁵ It would have been better to offer this right not just to parents, but also to children, as indicated by the GDPR, and even to individuals who are no longer children, as suggested by Recital (65).⁶⁰⁶

The COPPA, the GDPR and social media platforms' privacy policies do not appear to place a general restriction on what parents may share regarding their children, which could be associated with their freedom of expression. Nevertheless, to ensure the protection of children, YouTube restricted adults from sharing certain content relating to children. These include sexualisation of children, harmful or dangerous acts involving children, such as pranks, content that could cause children participants or viewers emotional distress, such as violence or simulating parental abuse, misleading family content that targets young people and involves drugs, sex, alcohol, death, etc., cyberbullying and harassment involving children, such as recording a child without their consent, and so on. This list is neither complete nor exhaustive. It can be improved.⁶⁰⁷ In addition, YouTube's policy includes “do not” recommendations such as filming children in private spaces (e.g., bedrooms and bathrooms), disclosing personal information about a child, and sharing content involving children's body twists or contortions that could attract unwanted attention from malicious individuals.⁶⁰⁸ YouTube's enforcement team may initially provide a warning; if the behaviour persists, they may issue a strike; if three strikes are issued, they may terminate the

⁶⁰⁴ James Lee: SB 568: Does California's Online Eraser Button Protect the Privacy of Minors, 48(3) U.C. Davis Law Review (2015), 1203.

For further information see the Online Eraser Button Law: S.B. 568, 2013 LEG. 2013-14 SESS. (Cal. 2013), https://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568 (last visited 10 March 2023).

⁶⁰⁵ 16 CFR COPPA Part 312.4(d)(3).

⁶⁰⁶ GDPR, Recital (65): “That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child.”

⁶⁰⁷ YouTube Help, YouTube Policies: Child Safety Policy, https://support.google.com/youtube/answer/2801999?hl=en&ref_topic=9282679#zippy=%2Ckorhat%C3%A1ros-tartalom%2Ckiskor%C3%BAakat-megc%C3%A9lz%C3%B3-tartalom (last visited 10 March 2023).

⁶⁰⁸ YouTube Help, YouTube Policies, Child Safety Policy: Content Featuring Minors, https://support.google.com/youtube/answer/2801999?hl=en&ref_topic=9282679#zippy=%2Ckorhat%C3%A1ros-tartalom%2Ckiskor%C3%BAakat-megc%C3%A9lz%C3%B3-tartalom%2Ccontent-featuring-minors (last visited 10 March 2023).

channel; and if they believe a child is in danger based on reported content, they will assist law enforcement in investigating the content.⁶⁰⁹

We do not consider that the policy and its sanctions are very stringent, as there are still several videos on YouTube that include restricted content. For instance, you may find a barber pranking a child by pretending to chop off his ear, and at thirty-seventh second in this video, it is stated that the boy's parents provided consent for the prank. You may observe his distress and pain in his eyes, body language, and facial expressions.⁶¹⁰ When the child reaches adolescence, he will likely find this video humiliating, and when he becomes an adult, he will probably take action to remove such terrible content.

Can we presume that parents are solely accountable for allowing the barber to share this information with the whole Internet community? Is the barber not responsible if he violates the child's privacy, body, and mind? YouTube is unable to effectively restrict such content to be published. Is YouTube not liable? Considering they are all liable, where is the regulation governing the child's data protection and privacy rights that applies? Because both the GDPR and COPPA were created with the intention of giving parents more authority over the data protection and privacy rights of their children. What results from a situation in which the parents have lost control? Who, then, has the authority to act against those parents' privacy decisions in relation to their children, and on what basis could such actions be made?

The *Martins* couple was sentenced to five years of probation for child abuse after releasing YouTube prank videos in which they shouted at and destroyed their children's toys. According to the prosecution, the Martins' pranks including yelling and causing to move their children to tears resulted in severe impairments of their mental or psychological well-beings. As a result, the Martins lost custody of their children after the recordings went viral on the Internet and sparked widespread criticism. Due to their probationary status, the Martins were not allowed to have contact with their children unless the court grants permission.⁶¹¹ Law enforcement is effective if there is a significant public response, as in the

⁶⁰⁹ YouTube Help, YouTube Policies, Child Safety Policy: What happens if content violates this policy, https://support.google.com/youtube/answer/2801999?hl=en&ref_topic=9282679#zippy=%2Ckorhat%C3%A1ros-tartalom%2Ckiskor%C3%BAakat-megc%C3%A9lz%C3%B3-tartalom%2Ccontent-featuring-minors (last visited 10 March 2023).

⁶¹⁰ YouTube, *Newsner.com* channel: Barber Pranks Kid By Pretending He's Cut His Ear Off, <https://www.youtube.com/watch?v=0TSNKp4Xs0U> (last visited 10 March 2023).

⁶¹¹ The Guardian: Couple who screamed at their kids in YouTube 'prank' sentenced to probation (12 September 2017) <https://www.theguardian.com/us-news/2017/sep/12/youtube-parents-children-heather-mike-martin> (last visited 10 March 2023).

instance of Martins, but it is far less effective if there is no public backlash, as in the case of the barber chopping off the ear of the child.

Children's privacy can also be violated without the use of nasty jokes or upsetting events. It may also be a peaceful video showing the daily routines of children with their parents. For instance, a video by a well-known influencer mother has more than one million views on YouTube, and its content is her three children's bedtime ritual. The majority of the video takes place in the bathroom and bedroom, which is against YouTube policy.⁶¹² Although the children in the video seem happy, they are probably unaware that these special memories are being shared with millions of strangers. Even if they were aware of this situation, they would be unable to comprehend the implications of this sharing practice.

When a social media user shares intimate moment with the world, he/she must also understand that there will be many remarks on their personal life. For instance, there are comments under this video regarding the children's hair that must be shaved and the D vitamins that they take, the ages of the children, the baby boy's new teeth, the breastfeeding machine, and everything else shown on the video.⁶¹³ What would these children feel when they get older and are able to read these comments and realise that many strangers have opinions on their private moments? How would they feel if they realized that their parents allow strangers to invade their personal space?

Furthermore, there are several videos of children practising yoga on YouTube. Unfortunately, these yoga sessions also feature children performing yoga positions, which may attract unwanted attention from ill-intentioned (e.g., paedophilic) YouTube users and be published to their forums, social media groups, and websites. Since the instructors are adults, it is unnecessary for children to participate in such videos. Instead of showing children's bodies, adult instructors would be clothed in a variety of vividly coloured apparel and the walls behind them would be covered with cartoon/anime characters to attract the interest of children. As previously described in this chapter, this is another sort of video that violates YouTube's terms of service, because it contains twists and/or contortions that might draw the attention of malicious users. However, we do not see any practical consequences of uploading such content, as a video containing a twenty-five minutes of yoga session for children with an adult instructor and two children following her has apparently been

⁶¹² YouTube, Simply Allie Channel: Night Time Routine of a Mom 2021 // Mom Of 3 // Preschooler, Toddler and Infant, <https://www.youtube.com/watch?v=Dx7Ty0Yg2-k> (last visited 10 March 2023).

⁶¹³ YouTube, Simply Allie Channel: Night Time Routine of a Mom 2021 // Mom Of 3 // Preschooler, Toddler and Infant, <https://www.youtube.com/watch?v=Dx7Ty0Yg2-k> (last visited 10 March 2023).

accessible on YouTube for more than five years without sanctions and has received approximately fifteen million views.⁶¹⁴

Not only YouTube, but also Instagram, serves as a platform for parents to share their children's daily routines or special moments, and it has been a huge trend over the past few years for parents to create Instagram accounts on their children's behalf, even creating a personality and posting as if they were the children themselves. One mother revealed why she posts her child's images and videos on a separate account under the child's name:

“I think everything my son does is cute and I would love to post pictures all day long of what he does—but, I didn’t want him to hijack my page... I'm still me—I’m a mom, but I'm also a daughter, girlfriend, employee. Although [child’s name omitted] is the most important thing in my life, it’s a step I took to make sure I remained me.”⁶¹⁵

A second mother who earns a job through social media marketing for other companies disagrees with her statement and adds,

“I have centered my career and my life on social media, and obviously see tremendous value in it from both a personal and professional point of view... But I knew right from the get-go that I would never create any social media profile in my child's name and update it as if I were him. My son should have the choice as a young adult about if he wants a social media presence, and what that presence will look like. I don't think it's a parent's place to make that decision on behalf of their child.”⁶¹⁶

We agree with the second mother that no parent should create an account on behalf of their child. What may a child think of a parent-created account that so-called belongs to him/her when the child reaches age of maturity? Parents should understand the close connection between privacy, dignity, and individuality.⁶¹⁷ Hence, they should be concerned

⁶¹⁴ YouTube, Storyhive Channel: Yoga for Kids! <https://www.youtube.com/watch?v=X655B4ISakg> (last visited 10 March 2023).

⁶¹⁵ Today: Have a social media account for your baby? 40 percent of millennial moms do (18 October 2014) <https://www.today.com/parents/have-social-media-account-your-baby-40-percent-millennial-moms-%201D80224937> (last visited 10 March 2023) cited in Shannon Sorensen: Protecting Children's Right to Privacy in the Digital Age: Parents as Trustees of Children's Rights, *Children's Legal Rights Journal* 36, no. 3 (2016), 160.

⁶¹⁶ Today: Have a social media account for your baby? 40 percent of millennial moms do (18 October 2014) <https://www.today.com/parents/have-social-media-account-your-baby-40-percent-millennial-moms-%201D80224937> (last visited 10 March 2023) cited in Shannon Sorensen: Protecting Children's Right to Privacy in the Digital Age: Parents as Trustees of Children's Rights, *Children's Legal Rights Journal* 36, no. 3 (2016), 160.

⁶¹⁷ Adrienn Lukács: What is privacy? The history and definition of privacy, In: Gábor Keresztes (ed.): *Tavaszi Szél 2016 Tanulmánykötet I.*, Budapest, Doktoranduszok Országos Szövetsége (2016), 259 <https://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf> (last visited 10 March 2023).

about their children's future self-image and reputation, as well as keeping them from being bullied or humiliated, as these are potential outcomes of loss of privacy.⁶¹⁸

Accordingly, banning all parental sharing would not be a practical solution, but there should be some legal restrictions. For instance, permitting only modest family images that do not reveal any personal information to others, or uploading photos of children exclusively from behind, or blurring their face, or adding emojis to their face, etc.⁶¹⁹

The Instagram Community Guidelines explicitly prohibit, for instance, the sharing of nudity.⁶²⁰ In reality, though, some parents share images of their children that are nearly nude with the internet community. For instance, there are parents who share potty training images of their children online, and once a mom acknowledged on her blog that she found her baby's naked potty-training photos on paedophilic websites and warned other parents on Twitter parent not to make the same mistake she made.⁶²¹

Another example is that the parents of a very famous child influencer are sharing their daughter's bikini photos with total strangers, and she has almost three hundred and fifty inappropriate comments under the photo, such as stating that “she is hot”, “very sexy”, and “only if someone catches her”, and other comments that will likely make her very disturbed and disgusted when she will be able to check those views and read the comments.⁶²²

Instagram claims that they encourage users under eighteen to have private accounts; consequently, when they create an account, the private account option will be selected by default rather than the public account option.⁶²³ It is a plus that the safer choice is automatically selected for teens, but it would have been ideal if they had no option to make their account public. The more accessible an account is to the public, the greater the danger and risk of being exposed to hate speech, bullying, condemnation, and severe criticism.

⁶¹⁸ Shannon Sorensen: Protecting Children's Right to Privacy in the Digital Age: Parents as Trustees of Children's Rights, *Children's Legal Rights Journal* 36, no. 3 (2016), 160.

⁶¹⁹ Asli Alkis Tümtürk: Implications of Parental Sharing of Children's Personal Data Online, *ArsBoni Jogi Folyoirat*, X. evfolyam 2022/1-2 (2022), 10 available at https://arsboni.hu/wp-content/uploads/2022/09/Arsboni-foly%C3%B3irat_2022_1_2.pdf (last visited 10 March 2023).

⁶²⁰ Instagram, Help Centre: Community Guidelines, https://help.instagram.com/477434105621119/?helpref=uf_share (last visited 10 March 2023).

⁶²¹ Twitter, BlogHer: “So I Posted Photos of My Kid Online and This is Where They Ended Up <http://ow.ly/2uSjRn>” (14 February 2013) <https://twitter.com/blogher/status/302079107901046784> (last visited 10 March 2023) cited in Stacey B. Steinberg: Sharenting: Children's privacy in the age of social media, *Emory LJ* 66 (2016), 847.

⁶²² Instagram, *Kids Diana Show* (image posted on 21 August 2021) <https://www.instagram.com/p/CSeZgdHjkVF/?hl=tr> (last visited 10 March 2023).

⁶²³ A Parent and Carer's Guide to Instagram: Manage Privacy, 15-16 https://www.internetmatters.org/wp-content/uploads/2021/11/UK_Instagram_-_parent_and_carer_guide_to_instagram.pdf (last visited 10 March 2023).

Moreover, users under the age of eighteen will not get personalised advertisements, although marketers may target them based on their location, gender, and age. They will eliminate the opportunity to opt-in to more personalised advertisements and apply these ad targeting restrictions internationally to all young Instagram users.⁶²⁴ It would be ideal, in our view, not to even allow the marketers to target their location, age, or gender, as these are still forms of personal data and may still influence teens' purchasing habits and mentality more effectively than most adults'. Due to their lack of information and life experiences, children may be more prone to manipulation. These can lead to a number of unpleasant results, such as mental and physical health disorders.

Teenagers acquire eating disorders such as anorexia and bulimia as a result of advertisements for diets and bodybuilding that employ manipulated body images. Similarly, one Instagram user reported seeing thirty-three Instagram stories from accounts she follows in addition to fourteen advertisements, many of which focused on physical looks, within two minutes of watching Instagram stories.⁶²⁵ Furthermore, in March of 2020, Instagram researchers posted on an internal message board that their survey data showed that one-third of the teenage girls who reported having body image issues felt worse after using Instagram.⁶²⁶

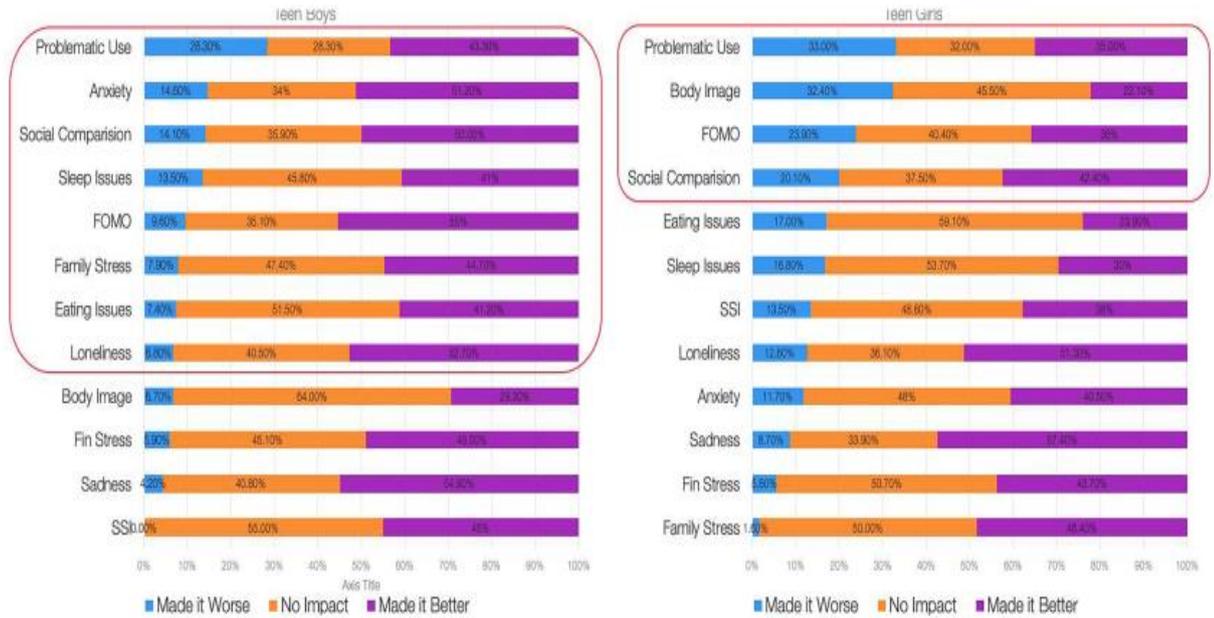
⁶²⁴ A Parent and Carer's Guide to Instagram: Manage Privacy, 24 https://www.internetmatters.org/wp-content/uploads/2021/11/UK_Instagram_-_parent_and_carer_guide_to_instagram.pdf (last visited 10 March 2023).

⁶²⁵ The Wall Street Journal, Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show (14 September 2021) https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739?mod=hp_lead_pos7 (last visited 10 March 2023).

⁶²⁶ Meta Newsroom: What Our Research Really Says About Teen Well-Being and Instagram (26 September 2021) <https://about.fb.com/news/2021/09/research-teen-well-being-and-instagram/> (last visited 10 March 2023).

BUT, WE MAKE BODY IMAGE ISSUES WORSE FOR 1 IN 3 TEEN GIRLS

Teens also generally thought that IG made things better or had no impact. However they were also more split around problematic social media use and the role we played in it. More teen girls thought that IG made body image issues worse rather than better



Q: What impact did using Instagram have on this experience?
 *Buckets highlight groups of issues that were not statistically different from each other.
 *All differences called out are statistically significant at 95% CI following a Bonferroni correction for multiple comparisons.

Chart 7: Slides from summary of Instagram’s 2019 research⁶²⁷

Besides to these aforementioned findings, Instagram has also addressed the issue of varying age requirements among EU Member States. Since it varies from country to country, Instagram has increased the minimum age for restricting personalised advertisements and creating private accounts by default to under eighteen, which we believe is a far better and more inclusive option.⁶²⁸ Thus, we should emphasize our prior recommendation that the EU should adopt a uniform age threshold requirement within the GDPR, rather than leaving this decision to the Member States.

⁶²⁷ Meta Newsroom: What Our Research Really Says About Teen Well-Being and Instagram (26 September 2021) <https://about.fb.com/news/2021/09/research-teen-well-being-and-instagram/> (last visited 10 March 2023).

⁶²⁸ A Parent and Carer’s Guide to Instagram: Manage Privacy, 24 <https://www.internetmatters.org/wp-content/uploads/2021/11/UK-Instagram-parent-and-carer-guide-to-instagram.pdf> (last visited 10 March 2023).

Due to the fact that they are both owned by the same parent company called Meta, Facebook's and Instagram's policies are similar. In Facebook's Community Guidelines, they also claim that they do not tolerate child sexual exploitation or anything that endangers children.⁶²⁹ Besides, in accordance with current law, they report instances of child sexual exploitation to the National Center for Missing and Exploited Children (NCMEC). Now that Facebook follows zero tolerance standards for child exploitation abuse and nudity, even if nude images are shared with good intentions, they attempt to remove the images due to the potential of abuse or misuse by the others.⁶³⁰

In one of our recent papers, we recommended that artificial intelligence (AI) and machine learning (ML) technologies be utilised by social media platforms to detect and eliminate nudity and other hazardous content related to children. We have emphasised that:

“For example, Facebook used to have face recognition technology to create name tags on images, and the face template was not shared with third parties according to Facebook's policy. [...] we recommend that social media sites, such as Facebook, may use this face recognition technology to protect children before their parents post photos as an alert and as a mild censor.” and also added “social media platforms may be expected to use Artificial Intelligence (AI) system to detect images of children that an adult wants to share, blurring the face or adding an emoji, or at the very least providing a clear map of the potential audience and risks of sharing and asking if the person is sure about sharing.”⁶³¹

Indeed, Facebook has begun employing these technologies to detect and remove shared harmful data in a manner similar to our earlier recommendation.⁶³² However, it would have been ideal if Facebook still employed these tools to notify and even prevent parents and other adults before they share content. Because removing them later is a good solution, but it might be insufficient, as once the photograph or video is uploaded on the Internet, it is not possible to predict who would have access to it and for what purpose they will use such content.

⁶²⁹ Meta, Facebook Community Standards, <https://transparency.fb.com/en-gb/policies/community-standards/?source=https%3A%2F%2Fwww.facebook.com%2Fcommunitystandards> (last visited 10 March 2023).

⁶³⁰ Facebook, Safety Centre, Online Child Protection: Our Policies <https://www.facebook.com/safety/onlinechildprotection> (last visited 10 March 2023).

⁶³¹ Asli Alkis Tümtürk: Implications of Parental Sharing of Children's Personal Data Online, *ArsBoni Jogi Folyoirat*, X. evfolyam 2022/1-2 (2022), 10 available at https://arsboni.hu/wp-content/uploads/2022/09/Arsboni-foly%C3%B3irat_2022_1_2.pdf (last visited 10 March 2023).

⁶³² Facebook, Safety Centre, Online Child Protection: Tools and Technology <https://www.facebook.com/safety/onlinechildprotection> (last visited 10 March 2023).

Therefore, it would be ideal to employ AI and ML to identify inappropriate data and prohibit its sharing before it reaches other users.

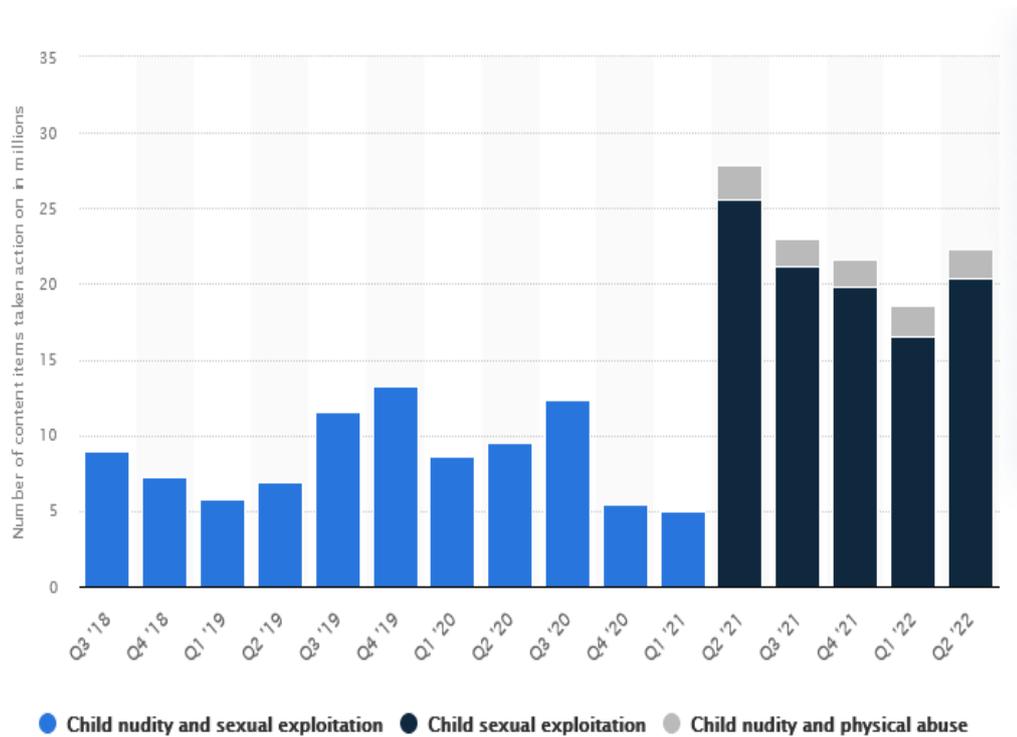


Chart 8: Global number of child nudity and sexual exploitation-related content items removed by Facebook from 2018 to 2022 (in millions)⁶³³

From 2018 through 2022, the above table displays the total amount of relevant content deleted by Facebook due to their association with child nudity and sexual exploitation. In the second quarter of 2021, as seen in the figure above, there was a sharp rise in the amount of content connected to child exploitation that Facebook deleted. The following quarters were not very different since the removals hover between twenty and twenty-five million.

There might be two potential explanations for this rapid rise. One possible explanation could be an increase in the prevalence of material that sexually exploits children. Second, it might be because Facebook has become better able to detect and remove such content as a result of the development of its own technology and tools. The second option seems more realistic and acceptable to us. Facebook's proactive approach, rather than waiting for users to report inappropriate material, is a significant improvement and much preferable solution.

⁶³³ Statista, Global number of child nudity and sexual exploitation-related content items removed by Facebook from 3rd quarter 2018 to 2nd quarter 2022 (in millions), <https://www.statista.com/statistics/1013776/facebook-child-exploitation-removal-quarter/> (last visited 10 March 2023).

In addition to cyberbullying, exposure to child pornography, and posting in paedophilic blogs or forums by a malicious individual, there may be other concerns linked with children's data being published on the Internet. For example, there is always a possibility of kidnapping or violent crimes against children whose comprehensive personal information was disclosed on social media by their parents or themselves. Not just strangers, but even certain ill-intentioned relatives or acquaintances using the same social media platforms may use the information provided to persuade or deceive children to follow them, which can lead to kidnapping and the demand for ransom to release the children. Concerns about non-strangers are understandable given the FBI research, which found that relatives or acquaintances were responsible for 76% of kidnappings and 90% of all violent crimes against children.⁶³⁴ Worse, children may find themselves in the hands of the organ mafia, which might result in the loss of vital organs and endanger their lives. In addition to these immediate consequences, releasing this information on the Internet may have long-term consequences, as the digital footprint remains. Due to the fact that the principle of equal opportunity has not yet been adopted by all organizations throughout the world, sensitive information about children's race, gender, or health may have a detrimental impact on their school/college life or career path.⁶³⁵

Another risk is that data brokers create profiles of individuals and sell them to advertisers, spammers, virus distributors, job agencies, and college admissions offices. The commercial market for new-borns and children in the US alone is worth hundreds of billions of dollars. As a result, it is not surprising that data brokers are attempting to gather as many profiles as they can sell. They merely need to collect the information submitted on the children by the parents or children themselves. Furthermore, the data brokers' mini profiles may be improved over time when children engage in further Internet activities, particularly through the use of social media sites.⁶³⁶

Aside from the threats posed by other individuals or businesses, there is also the possibility of governmental surveillance for children whose personal information is exposed in the Internet environment. By parental sharing or the children's own online activities, the

⁶³⁴ Tehila Minkus, Kelvin Liu, and Keith W. Ross: Children seen but not heard: When parents compromise children's online privacy, In Proceedings of the 24th international conference on World Wide Web (2015), 777.

⁶³⁵ Stacey B. Steinberg: Sharenting: Children's Privacy in the Age of Social Media, *Emory Law Journal* 66, no. 4 (2017), 849.

⁶³⁶ Tehila Minkus, Kelvin Liu, and Keith W. Ross: Children seen but not heard: When parents compromise children's online privacy, In Proceedings of the 24th international conference on World Wide Web (2015), 777.

children's likeness and identifying information are exposed to monitoring, such as that of intelligent services. When the children grow up, it will be extremely difficult for them to reduce their digital footprint.⁶³⁷ If we consider individuals over 30 years old, their internet presence only extends back 10 to 15 years at most, but when it comes to today's babies and children, their existence begins even before they are a foetus, due to the shared ultrasound images.⁶³⁸ According to one research, approximately 80% of youngsters in developed Western countries have a digital footprint by the age of 2, owing to their parents' online sharing habits.⁶³⁹

The potential dangers of surveillance could be blackmailing, discrimination, and persuasion. Because possessing personal information provides the tracer a lot of power, if the government is monitoring the individual, it gains a significant amount of power over people whose personal information is posted on the Internet in some manner. Information about embarrassing moments or disgraceful crimes, in particular, may be key components of blackmail. The information obtained through tracking people's online behaviour provides the government with a huge chance to influence, persuade, or even control people's choices, decisions, and subsequent actions. Furthermore, surveillance may be utilised as a technique for sorting and discriminating. For example, during World War II, census information provided an idea for locating Japanese internment camps in North America and concentration camps in Europe.⁶⁴⁰

⁶³⁷ Tehila Minkus, Kelvin Liu, and Keith W. Ross: Children seen but not heard: When parents compromise children's online privacy, In Proceedings of the 24th international conference on World Wide Web (2015), 777.

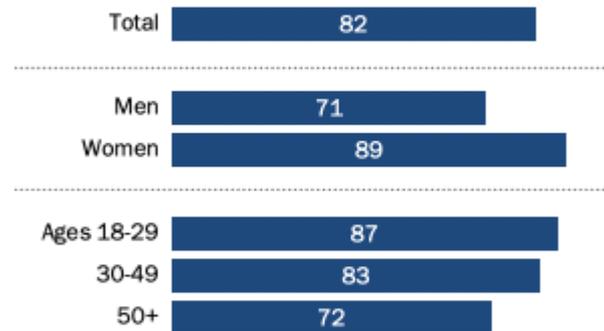
⁶³⁸ Stacey B. Steinberg: Sharenting: Children's Privacy in the Age of Social Media, *Emory Law Journal* 66, no. 4 (2017), 849-850.

⁶³⁹ United Nations, Office of the United Nations High Commissioner for Human Rights (OHCHR): Children's right to privacy in the digital age must be improved (15 July 2021) <https://www.ohchr.org/en/stories/2021/07/childrens-right-privacy-digital-age-must-be-improved> (last visited 10 March 2023).

⁶⁴⁰ Neil M. Richards: The dangers of surveillance, *Harvard Law Review* 126, no. 7 (2013), 1952-1958.

Roughly eight-in-ten parents who use social media have posted things about their children on these sites

Among U.S. parents who use social media, % who say they have ever shared photos, videos or information about their children on social media sites



Note: Based on parents who have at least one child under the age of 18 but may also have an adult child or children. Those who did not answer are not shown.

Source: Survey of U.S. adults conducted March 2-15, 2020. "Parenting Children in the Age of Screens"

PEW RESEARCH CENTER

Chart 9: Parents who share information about their children⁶⁴¹

Only 16% of parents at least sometimes worry about their children being upset about the things posted about them on social media

Among U.S. parents who have shared things about their children on social media, % who say they ___ worry that in the future their children might be upset about the things they posted about them on social media sites



Note: Based on parents who have at least one child under the age of 18 but may also have an adult child or children. Those who did not give an answer are not shown.

Source: Survey of U.S. adults conducted March 2-15, 2020.

"Parenting Children in the Age of Screens"

PEW RESEARCH CENTER

⁶⁴¹ Pew Research Center, Parenting Children in the Age of Screens: Parents' attitudes – and experiences – related to digital technology (28 July 2020) <https://www.pewresearch.org/internet/2020/07/28/parents-attitudes-and-experiences-related-to-digital-technology/> (last visited 10 March 2023).

Chart 10: Parents worry about their children being upset about the information they posted about them on social media⁶⁴²

Conversely, the practises and the tables above indicate that parents are not very worried about the online data they disclose about their children via social media sites. Roughly eight in ten parents say they share information about their children on social networking sites, and majority (84%) of them stated they seldom or never fear that their children may be upset in the future about the photos, videos and other information they shared about them.⁶⁴³

In this chapter, we have previously explored how difficult it would be for children and adolescents to comprehend the importance of digital privacy and its possible implications and risks in the event of violence. Accordingly, the time has come for parents to assume responsibility for their children's digital privacy and data protection rights, as required by the GDPR, COPPA, and social networking platforms. However, what happens when parents do not realize the future ramifications and dangers of disclosing their children's private lives online? In this scenario, we suggest that the law should restrict the parents' ability to share private moments with their children.

As previously mentioned, parents' right to informational self-determination on behalf of their children is not absolute. We asserted that both the age and the content may be used as restrictions. For instance, if the parents choose to share anything including their children's sensitive information, private moments, or anything that might affect their dignity, honour or reputation either now or in the future, this content should be restricted.⁶⁴⁴

Indeed, social networking platforms have made some progress in restricting some content pertaining to children, and Facebook has already taken steps to remove some restricted content relating to children. We assume that if the COPPA and GDPR restrict parental sharing, social media companies would be more compelled to prohibit certain content, particularly involving nudity, sexual exploitation, and violent content, but they

⁶⁴² Pew Research Center, Parenting Children in the Age of Screens: Parents' attitudes – and experiences – related to digital technology (28 July 2020) <https://www.pewresearch.org/internet/2020/07/28/parents-attitudes-and-experiences-related-to-digital-technology/> (last visited 10 March 2023).

⁶⁴³ Pew Research Center, Parenting Children in the Age of Screens: Parents' attitudes – and experiences – related to digital technology (28 July 2020) <https://www.pewresearch.org/internet/2020/07/28/parents-attitudes-and-experiences-related-to-digital-technology/> (last visited 10 March 2023).

⁶⁴⁴ The basis for this can be found in the Article 16 of the UNCRC: "1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation. 2. The child has the right to the protection of the law against such interference or attacks." UNCRC, Article 16(1) and (2).

should restrict even more. We assert that the only content that should be shared is reasonable family portraits or content that does not reveal any personal and/or sensitive information about children (e.g., a typical photo of family members celebrating Christmas/New Year), such as their age, race, address, health conditions, religious or political beliefs (if he/she is a teenager), biometric data, or any data that can be used to identify them. Additionally, some photos taken from behind, blurred images, or the insertion of emojis to the children's faces might potentially serve as a mild kind of censorship.⁶⁴⁵

In addition to the legal remedies and restrictions stated above, there is a more essential alternative that will be more difficult to adopt but more effective in the long-term. Digital literacy education for children and their parents is the solution. Digital literacy encompasses the ability to use digital devices or software safely, to generate meaningful content for the digital world and communities, and to be a conscious and responsible digital consumer.⁶⁴⁶

When discussing data and privacy literacy, keep in mind that education should focus on three types of privacy: first, interpersonal privacy, which involves an individual's digital footprint, second, institutional privacy, which involves how governments or public authorities collect information about individuals, and third, commercial privacy, which involves how businesses use individuals' personal information for marketing purposes.⁶⁴⁷

Furthermore, children and their parents should be aware of three types of data: the data given, which means that individuals have contributed this information about themselves, or others have contributed about those individuals; the data traces, which individuals have left behind, usually unknowingly, and which are captured using data-tracking technologies; and the inferred data, also known as profiling, which is the result of analysing the data given and data traces and posing a conclusion about individuals.⁶⁴⁸

The study conducted by *Livingstone et al.* (2019) on data and privacy online of children growing up in the digital age revealed that children aged 5-7, 8-11, and 12-17 have different understandings about the typology of privacy. But as we mentioned earlier in this chapter,

⁶⁴⁵ Asli Alkis Tümtürk: Implications of Parental Sharing of Children's Personal Data Online, *ArsBoni Jogi Folyoirat*, X. evfolyam 2022/1-2 (2022), 9 available at https://arsboni.hu/wp-content/uploads/2022/09/Arsboni-foly%C3%B3irat_2022_1_2.pdf (last visited 10 March 2023).

⁶⁴⁶ Fabio Nascimbeni and Steven Vosloo: Digital literacy for children: Exploring definitions and frameworks, UNICEF Office of Global Insight and Policy, Scoping Paper 1 (2019), 10.

⁶⁴⁷ Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri: Data and privacy literacy: The role of the school in educating children in a datafied society, *The handbook of media education research* (2020), 415.

⁶⁴⁸ Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri: Data and privacy literacy: The role of the school in educating children in a datafied society, *The handbook of media education research* (2020), 415 cited in Simone Van der Hof: I agree, or do I: a rights-based analysis of the law on children's consent in the digital world, *Wis. Int'l LJ* 34 (2016), 412-414.

all of their understandings are usually related to interpersonal privacy rather than commercial or institutional ones. It indicates that they responded to issues and queries regarding commercial and institutional processes in the context of interpersonal terms. This might be due to the children's familiarity with offline interpersonal situations, however online privacy does not operate like this, especially when it comes to data economy. Because children are less conscious of the activities of institutions and commerce, they may expose information about them without being aware of potential data breaches or exploitative commercial operations.⁶⁴⁹ An overview of the research is provided in the table below:

Ages of children	Interpersonal privacy	Institutional and commercial privacy
5-7	<ul style="list-style-type: none"> • Have a developing sense of ownership, fairness, and independence • Learning about rules but may not follow, and do not understand consequences • Use digital devices confidently, for a narrow range of activities • Getting the idea of secrets, know how to hide, but tend to regard tracking/monitoring by a trusted adult as helpful 	<ul style="list-style-type: none"> • Limited evidence exists on understanding of the digital world. • Low risk awareness (focus on device damage or personal upset). • Few strategies (can close the app, call on a parent for help). • Broadly trusting

⁶⁴⁹Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri: Data and privacy literacy: The role of the school in educating children in a datafied society, *The handbook of media education research* (2020), 416.

<p>8-11</p>	<ul style="list-style-type: none"> • Starting to understand the risks of sharing, but generally trusting <ul style="list-style-type: none"> • Privacy management means rules, not internalized behavior • Still see monitoring by a parent or other trusted adult positively, to ensure their safety • Privacy risks linked to “stranger danger” and interpersonal harms • Struggle to identify risks or distinguish what applies offline/ online 	<ul style="list-style-type: none"> • Still little research available <ul style="list-style-type: none"> • Gaps in ability to decide about trustworthiness or identify adverts • Gaps in understanding privacy terms and conditions • Interactive learning shown to improve awareness and transfer to practice
<p>12-17</p>	<ul style="list-style-type: none"> • Online as “personal space” for expression, socializing, learning <ul style="list-style-type: none"> • Concerned about parental monitoring yet put broad trust in parental and school restrictions • Aware of/attend to privacy risks, privacy mainly seen as interpersonal • Weigh risks and opportunities, but decisions are influenced by a desire for immediate benefits 	<ul style="list-style-type: none"> • Privacy tactics focus on online identity management, not data flows (see data as static and fragmented). <ul style="list-style-type: none"> • Aware of “data traces” (e.g., ads) and device tracking (e.g., location), but less personally concerned or aware of future consequences • Willing to reflect and learn, but do so retrospectively • Media literacy education is most effective if adolescents can use their

		knowledge to make meaningful decisions in practice.
--	--	---

Table 2: Children’s data and privacy literacy⁶⁵⁰

Even more confusing is the fact that interpersonal and commercial activities are no longer truly distinct, as they once were. For instance, when a child shares a photo with a friend via Instagram, the photo is shared with Instagram simultaneously and, depending on the settings of the Instagram account, with Facebook as well.⁶⁵¹ Dual-meaning online interactions are not only perplexing for parents, but also for the parents who should be guiding their children.⁶⁵²

⁶⁵⁰ Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri: Data and privacy literacy: The role of the school in educating children in a datafied society, *The handbook of media education research* (2020), 417.

⁶⁵¹ “When you add your Instagram account to the same Accounts Centre as your Facebook account, you can share content such as stories and posts directly from Instagram to Facebook.” Instagram Help Centre, Sharing to other social networks, <https://help.instagram.com/169948159813228> (last visited 1 March 2023).

⁶⁵² Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri: Data and privacy literacy: The role of the school in educating children in a datafied society, *The handbook of media education research* (2020), 419.

Ages of children	What children want to know about their data and privacy online	What children think companies should do differently
All ages	<ul style="list-style-type: none"> • Who has my personal data, how long they keep it, and what they do with it • Why they collect, share, and sell my information • Where deleted data goes, and whether it is really gone 	<ul style="list-style-type: none"> • Make deleted apps or information permanently gone. • Provide more and better privacy, security, and safety options. • Make accounts private, turn off geolocation, and disable cameras by default. • Don't share my data with other sites or services. • Be more responsiveness to user concerns and complaints. • Make Terms and Conditions understandable, short, and visual
11-12	<ul style="list-style-type: none"> • Why apps need to know your phone number • Who controls websites • Who can find out about my information • Why they set age restrictions so high (e.g. WhatsApp) • Why companies don't remove scamming sites • Why reporting stuff is so hard 	<ul style="list-style-type: none"> • Let children under 13 use social media, but keep their account private. • Make online content more appropriate for our age. • Take down hostile content (e.g. fat shaming)

	<ul style="list-style-type: none"> • Why they make mistakes about who you are 	
13-14	<ul style="list-style-type: none"> • Who can see what I search • Whether people can see me through my camera or hear my voice • What social media sites do with your information • What happens when you get hacked • What happens to your data when you die • What the dark web is • What they do with your face when you use facial recognition 	<ul style="list-style-type: none"> • Allow paid-for but private apps • Don't sell our data. • Don't show me what I'm not interested in. • Make it easier to erase your account.
15-16	<ul style="list-style-type: none"> • Where data is kept, how it travels across the internet, and what is shared with other companies • Why they need to know so much about me (e.g. my gender) • Whether sensitive data is shared 	<ul style="list-style-type: none"> • Leave me alone. • Keep biometric data safely. • Delete our data after a certain time (e.g. 2 years). • Only ask for information when relevant. • Allow you to opt out of data collection. • Have better checks on age restrictions. • Explain to you what information they have about you.

Table 3: Children’s views of how their data and privacy online should be addressed
(entries paraphrased and summarized by the authors)⁶⁵³

The responses indicate in the table above that children of all ages are concerned about who collects their personal data, how the data is gathered, and why the data is collected. It has been observed that children of different ages approach types of data differently. The younger children regard personal information as data given, such as phone numbers, but the older children are aware of data taken and inferred as well (e.g., via face recognition technology), along with the various types of data, including sensitive, biometric, and profiled data. Some of the older ones had a strong grasp of how data profiling is performed and the data economy which profiling is one of the components. Because they had previously searched for something and then received relevant advertisements. Some teenagers are also asked about advanced privacy issues, such as data transfers, data retention periods, and age verification methods. At the end, when they learned about the extensive collecting of their personal data from the research's authors, they were angered and confused; nevertheless, this is paradoxically the business model of social networking sites and advertising firms.⁶⁵⁴

This study demonstrates that data and privacy education should be tailored to the age of children, beginning with interpersonal privacy and data given for comparatively younger children and proceeding to institutional and commercial privacy and data taken and inferred (i.e., profiling) as children grow and develop. This study's findings also imply that parents usually know little about privacy and the digital world, citing instances of parents' comments when asked what they think about online experiences and Internet dangers:

“I don't know,” one of the mothers said, “I haven't really thought about it.”⁶⁵⁵ After describing the Internet's potential risks, one of the fathers stated, “that’s just the nature of the internet,” and “it’s a scary world.”⁶⁵⁶

⁶⁵³ Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri: Data and privacy literacy: The role of the school in educating children in a datafied society, *The handbook of media education research* (2020), 418.

⁶⁵⁴ Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri: Data and privacy literacy: The role of the school in educating children in a datafied society, *The handbook of media education research* (2020), 417-419.

⁶⁵⁵ Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri: Data and privacy literacy: The role of the school in educating children in a datafied society, *The handbook of media education research* (2020), 421.

⁶⁵⁶ Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri: Data and privacy literacy: The role of the school in educating children in a datafied society, *The handbook of media education research* (2020), 421.

One of the fathers asserted that schools should teach children about digital skills, adding, “I think that should be part of citizenship, that they’re learning in schools about how all of this impacts. Because, I don’t know much about profiling, to be honest.”⁶⁵⁷

Parents, who are unfamiliar with the internet world, expect the school and instructors to teach their children about it. Whereas teachers believe that parents should take greater responsibility in raising their children to be aware of potential dangers of Internet and be careful with their online presence and activities. Teachers also believe that the curriculum does not teach students the necessary digital literacy abilities, and that the digital literacy skills taught in schools are not transferrable into practise.⁶⁵⁸

According to all of the above-mentioned considerations, it is not unexpected that people, especially parents and teachers, believe they are lagging behind in the development of new technology.⁶⁵⁹ Therefore, governments and other stakeholders must take responsibility and make more investments to help parents and teachers improve their digital skills so that they can better support children's learning and growth in the digital era.⁶⁶⁰ The government should invest in competent instructors to consistently teach digital literacy to parents and children in schools. There may be lessons in the official curriculum designed to help children improve their digital abilities and get a deeper understanding of digital privacy and data protection. Besides, there may be evening or weekend courses for parents that the government funds for the same aim. Consequently, they will be able to assist their children much effectively with greater knowledge.

In conclusion, law makers, law enforcements, data controllers, researchers, schools, and parents should work to solve unforeseen difficulties and unknown repercussions related to the security and privacy of children's data in the digital world. Given the shortcomings in parental and child education in the current context, greater focus must be placed on enacting restrictive legislation. This will also drive social media platforms to implement more restricted and child-friendly content policies. As a long-term solution, however, the government foundation should implement digital literacy programmes in schools or courses

⁶⁵⁷ Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri: Data and privacy literacy: The role of the school in educating children in a datafied society, *The handbook of media education research* (2020), 421.

⁶⁵⁸ Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri: Data and privacy literacy: The role of the school in educating children in a datafied society, *The handbook of media education research* (2020), 422.

⁶⁵⁹ Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri: Children’s data and privacy online: Growing up in a digital age. An evidence review, London: London School of Economics and Political Science (2019), 35.

⁶⁶⁰ Sonia Livingstone and Jasmina Byrne: Challenges of parental responsibility in a global perspective. In: Urs Gasser (ed.): *Digitally Connected: Global Perspectives on Youth and Digital Media* (2015), 26-29. Cambridge: Berkman Center for Internet and Society, Harvard University.

for children and their parents. Last but not least, courts in the EU and the US should interpret the law in a manner that protects the privacy of children. Because they are two of the world's leading jurisdictions in terms of data security and privacy, their legal requirements and educational techniques will surely serve as models for the rest of the world's legal systems.⁶⁶¹

7.1 Short Summary

In this chapter, we examined the data policies and practises relevant to the safety and privacy of children's data on the three most prominent social networks (Facebook, Instagram, and YouTube) in the world to illustrate the discrepancies between law in text and law in practise. Our conclusions were supported by studies, surveys, and statistics.

We have seen that the COPPA and GDPR, which hold parents accountable for their children's internet actions, are an improvement against ignoring their existence. Yet, although children under the age of consent are limited in their ability to disclose information online, parents are free to do so at any time. We have suggested, however, that it is not a wise move, given that several parents lack digital literacy and may not foresee the ramifications and possible hazards of disclosing their children's information online.

Thus, we have indicated that parental freedom of speech and right to informational self-determination (on behalf of their children) is not absolute and should be balanced; when it comes to conflicting interests, we should prioritise the child's right to privacy, dignity and reputation.

In such instances, we stated that the right to be forgotten is a vital right for restoring children's power and control over their data, which they lost due to parental sharing. Although freedom of expression is an exception to the right to be forgotten under the GDPR, we claimed that where the data subject is a child, freedom of expression must be interpreted much more narrowly, and this exemption should not be utilised.

The COPPA does not offer children with this vital right to be forgotten; rather, it allows parents the ability to seek the removal of their children's information. We considered that it would have been preferable to extend this right to children and even individuals who are no longer children.

⁶⁶¹ Asli Alkis Tümtürk: Implications of Parental Sharing of Children's Personal Data Online, *ArsBoni Jogi Folyoirat*, X. evfolyam 2022/1-2 (2022), 13 available at https://arsboni.hu/wp-content/uploads/2022/09/Arsboni-foly%C3%B3irat_2022_1_2.pdf (last visited 10 March 2023).

Despite the fact that there are no legal limitations on parental sharing, social media platforms have imposed restrictions on harmful content relevant to children. However, it is still possible to locate restricted content on social networking platforms, as demonstrated by the real-life examples provided in this chapter. We stated that it would have been preferable to adopt an AI and ML system that they could detect potentially hazardous information before parents or other adults share it and prohibit it before it reaches the Internet environment and malevolent individuals.

We have determined that GDPR and COPPA should restrict the content that the parents can disclose about children. Only content that should be shared is reasonable family portraits or content that does not reveal any personal and/or sensitive information about children (e.g., a typical photo of family members celebrating Christmas/New Year). We emphasised that certain photographs shot from behind, blurred images, or the insertion of emojis to the children's faces can potentially act as a small type of censorship.

After that ultimately, we offered a long-term and more successful remedy whereby the teaching of children and parents regarding the digital literacy abilities. The government should thus take on responsibility and invest in digital literacy in schools, subsidise the assignment of instructors to schools, include digital literacy teachings into official curriculums, and provide free courses for parents. Therefore, parents and schools will have a clearer understanding of the notion of digital privacy and will be able to assist children/students much more effectively.

This chapter concluded by arguing that states, parents, schools, and data controllers should collaborate to overcome the unanticipated potential challenges of the digital world. Moreover, we suggested that the application of the law should also be child-friendly, and courts in the EU and the US should interpret the law in the best interest of children. In this regard, they can also serve as examples for other countries, given that they have the leading legal systems in data protection and privacy.

8. Conclusions

In Chapter 2 of this thesis, we began with a background analysis of the COPPA rule and Article 8 of the GDPR. Using a historical perspective, we analysed the emergence and evolution of the concepts of privacy and data protection. We claimed that privacy is not a contemporary issue but has been a concern since ancient empires and their laws, including Babylonian, Ancient Greek, and Roman. Although, there were similarities like one's home has always accepted as a private place, the concept of privacy was different than what we recognised today. The foundations of today's concept were laid in the 19th century. Especially as a result of urbanisation, cultures encountered a new concept of privacy that arose from the loss of space caused by the migration to the crowded cities and the development of press technology.

We added that these new advances contributed to the existing fundamental right to privacy, as journalism was the primary impetus behind Warren and Brandeis's famous article. Even today, this article's definition of privacy as the “right to be let alone” is widely accepted. Subsequently, technological advancements and computer developments led to the establishment of a new right known as the right to data protection, whose subject matter is protection of individuals (natural persons). Since the historical legislative developments of privacy and data protection started in the US, the EU followed in their footsteps but built a protection that was more comprehensive.

In contrast to the US, we stated, data protection became a fundamental right in the EU. Convention 108 of the Council of Europe was the first legislative framework related to data protection, but it was ineffective in harmonising the legislation of the Member States. Therefore, Directive 95/46/EC established by the European Parliament and the Council of the European Union came into effect. However, due to its nature, it enabled EU Member States to have varying domestic data protection rules, and it was unsuccessful in establishing a uniform legal framework across the Union. Consequently, the GDPR was established, and it became uniformly (except the facultative specifications clauses⁶⁶²) and entirely applicable in all Member States upon its entry into force.

⁶⁶² “The GDPR gives Member States the possibility to further specify its application in a limited number of areas.” See the list of the clauses for facultative specifications: European Commission, Commission Staff Working Document, Accompanying the document Communication from the Commission to the European Parliament and the Council Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation, Brussels, 24.6.2020, SWD(2020) 115 final, pp. 1-52, 50, Annex I.

We suggested that after becoming aware of children's internet presence, it became necessary to develop specific rules for them. First, the COPPA was created in the US to safeguard the online privacy of children. The EU then followed suit and incorporated Article 8 into the GDPR. The GDPR transplanted the COPPA's requirements concerning the age threshold and parental consent. However, the overreliance on parental consent in both pieces of legislation was criticised since the responsibility of processing personal data of children should be shared at least with the data controllers.

In Chapter 3, we defined consent and underlined that it is a concept that grants data subjects control over their data. We noted that consent must be freely provided, explicit, informed, and unequivocal for the processing of personal information concerning data subjects. We continued by comparing the concept of parental consent of the GDPR with the COPPA. The most notable distinctions between these two legislations are the age thresholds for obtaining parental consent (13-16 under the GDPR and 13 under the COPPA) and the methods for obtaining parental consent.

In Subchapter 3.3, concerning the first difference, we discussed the first research question of this thesis which is whether threshold ages for parental consent have any logical basis. Accordingly, we criticised the fact that the age of digital consent is neither standardised nor well-justified between Member States. It was transplanted for economic reasons and to lessen the burden on data controllers, but because to the variable threshold ages, it should now put a more burden on data controllers. Hence, we suggest the following:

Policymakers should review whether imposing age limits is useful or whether there are other solutions to provide children with a safe online environment. One important alternative is education and awareness-raising. Other solutions include a combination of parental supervision with software solutions, and ethical design principles for online service providers (including creating more child-friendly content and platforms). However, since age restrictions currently exist under both legislation, it is important to establish a uniform threshold age for online consent under the GDPR across Member States. This is particularly important due to data transfer within the EU and to the US. Besides, a uniform age threshold for digital consent online would offer clarity, consistency, and simplicity of compliance inside the EU for both individuals and companies. The uniform threshold age should also be well-justified. For instance, comparisons with other legal disciplines could help determine a consistent and reasonable age for all Member States.

Regarding the second difference, we noted that the COPPA covers non-exhaustive approaches, but the GDPR does not mention any methods. We criticised the fact that the GDPR did not transplant any methods for validating parental consent from COPPA. It would have been ideal to involve at least some of them in order to provide guidance to data controllers.

Then, the second research question of this thesis was how the threshold ages are applied in practise and if they are effective on children's internet activity habits and behaviours. To answer this question, we compared the age of digital consent to other ages of consent in a variety of circumstances, including entering the workforce, receiving medical care, including diagnosis and surgery, and participating in lawful sexual behaviour with others.

We found out that the correlations between various consent ages in different contexts are illogical and may confuse children. A 16-year-old child in Hungary, for instance, cannot see a doctor (who respects physician-patient privilege) on his or her own, but he or she may download a health app that gathers and processes sensitive data and the data controllers of this app may even sell this information for profit. In Hungary or Germany, for example, a child of 14 can have sexual intercourse, but without parental consent, he or she cannot create a social media account. In the Netherlands, a child of thirteen can opt to work part-time after school and earn his or her own money but cannot open an e-mail account without parental consent.

We analysed the surveys done by the Pew Research Center and the EU Kids Online studies to see whether there is any evidence that lowering the minimum age for accessing specific online services has any practical effect. However, decreasing (or raising) the threshold age has no influence on the outcomes. In Germany, the minimum age for parental consent is 16, although in Spain it is 14. However, children ages 12 to 14 and 15 to 16 are less likely to use social media networks in Spain than in Germany. It indicates that increasing the age threshold in Germany did not deter children under 16 from using social media platforms.

On one hand, Member States who oppose lowering the age of consent online assert that they do so to protect children. On the other hand, those who advocate lowering the age of consent on the Internet (to as low as 13) argue to support children's freedom of speech and press. Considering all the findings mentioned in Subchapter 3.3 regarding the second research question, this thesis claims as follows:

These regulatory standards do not have sufficient response in practise. In other words, these findings imply that differences in the digital age of consent have no direct

impact on use or internet safety in practise. Besides, it seems that lowering the age barrier has no direct impact on the motivation of children to engage in online activities. Moreover, the likelihood of children experiencing injury is not directly proportionate to their age.

Additionally, in Subchapter 3.3, we argued that there is a discrepancy between the law in text and the law in practise, and that this discrepancy is a result of age verification procedures that are easily deceived, particularly the widely used self-verification methods, and as we can see from the aforementioned surveys, children have, for example, social media or Gmail accounts before the age of consent.

Following that, we addressed age verification systems in Subchapter 3.4, which would use technology to ensure that only individuals of a certain age may access age-restricted information online. However, one should be aware that age verification systems include imperfections and cannot be depended upon to protect children from all potentially harmful content. In Subchapter 3.4, we addressed the third research question of this thesis, which is whether commonly deployed methods of age verification for preventing children's access to inappropriate online content be both trustworthy and respecting children's privacy and data protection rights.

Accordingly, self-verification, peer-based verification, using a credit card, debit card, or other online payment systems as an age verification method, providing personal identification documents such as a passport or driver's licence, knowledge-based authentication, and the use of biologically unique identifiers were covered.

We also addressed the outcomes of an ongoing EU-funded study called euCONSENT, which aims to improve age verification procedures. Based on the findings of this survey, face recognition is the most preferred way of age verification, while credit cards are the least used. Possible explanations for these results include the fact that facial recognition is very easy to use. However, we cannot infer the accuracy of facial recognition from the project's results. In our opinion, it should not be accurate to detect exact ages of children since a 16-year-old might appear to be an 18-years-old and simply could have access to adult consent.

It may be impractical to use a credit card when there is no monetary activity, which may explain why it is the least preferred payment option. In addition, it is difficult to identify a child from an adult because children might also have bank accounts, and the exact age cannot be determined from a bank account or credit card number. Therefore, the following proposed according to the findings of this thesis:

There are relatively accurate methods for estimating children's age, but they are not privacy-friendly, such as the personal ID or biometric features (e.g., fingerprint) scanning method. There are some methods that may violate data protection and still they are not useful to estimate the exact age, such as voice recognition or face ID tools. Besides, there are some which are privacy-friendly, however, useless because they are so easy to deceive, such as self-verified information. In addition, there is a knowledge-based authentication method that does not breach privacy and yet is useless at determining an individual's exact age. Therefore, we noticed that there is no method that simultaneously protect children from dangerous content and their personal data.

The EU, whereas, acknowledged this issue and urged Member States to develop age-verification systems in accordance with its eID plan. According to the European Commission, children can use their eIDs to verify their age without giving any further personal information (such as their name or address), which is compliant with the data minimization principle of the GDPR. Besides, it would be a reliable solution because it is based on reliable government databases. This technology, nonetheless, would raise security and privacy issues due to the large quantity of official papers and biometric user data that would be maintained. Thus, if the security and privacy issues (such as cyber-attacks and hacker activities) are mitigated, this eID solution will result in a trustworthy EU-wide age verification method that respects privacy.

Within the Chapter 4, we detailed the main rights of children and parents under the GDPR and COPPA. The fourth question of this thesis was whether data protection and privacy rights should be provided directly to children by law, or parents shall exercise them on their behalf.

Children have the same data protection rights as adults under the GDPR, including the right to be informed, the right of access, the right to rectification, the right to erasure (including the right to be forgotten), the right to processing restriction, the right to data portability, the right to object, and the right not to be subject to a decision based solely on automated processing, including profiling. We discovered, however, that neither the children nor their parents are provided with instructions on how to exercise these rights. Accordingly, this thesis advocates the following:

Some of the rights may be too complicated for children to exercise on their own; thus, it would be ideal if parents could do so on their behalf if necessary. Others, including as the right to access, rescission, and deletion, may be easier for children to exercise without parental consent if they are mature enough to understand the

repercussions of their online actions. At this point, the cooperation of data controllers and the service provider (e.g., third party suppliers) is also crucial because they can make these rights very clear and understandable for children, so that children are aware of their rights and may decide to exercise them or urge their parents to do so.

The COPPA, unlike the GDPR, does not identify any specific rights for children to exercise, but rather provides these rights to parents. It offers parents with notification and review rights, as well as the ability to seek the erasure of personally identifiable information belonging to their children. Likewise, this thesis recommends:

Under the COPPA, children should have at least the right to access, rectification, and deletion, and should not be subject to decisions based only on automated processing (especially profiling). And these rights should be given to children as soon as they can consent to the processing of their personal information. Children should not lose control over their data since it may lead to a variety of dangerous outcomes, as seen by Amanda Todd's suicide, which occurred because she lost control over her data and was unable to delete it herself.

Along with the legislative rights, we closed this chapter by emphasising the necessity of collaboration between data controllers, third-party service providers, and parents. Parents should provide their children with Internet access, secure their children's personal information from hazardous third parties by interacting, when necessary, without breaching their children's privacy, and be able to maintain this delicate balance.

In addition, data controllers and/or service providers must be able to explain and demonstrate these rights to children using colourful pictures or brief, entertaining, and easily understandable films, as well as clear and unambiguous language. In this circumstance, children will be more aware of their rights and will be able to comprehend the restrictions on how they may use those rights, as well as how much help they require from their parents, if necessary.

Following the rights of children and their parents, we discussed the interrelated obligations of data controllers and processors in Chapter 5. The fifth research question of this thesis was whether the GDPR and COPPA impose obligations specific to children on data controllers. The sixth question of this thesis was when and how data controllers could

directly engage with children (instead of their parents) and offer them more control over their data.

We have analysed all the obligations of the data controller under the GDPR and COPPA in detail. First obligation of the data controllers under the GDPR is to make it feasible and convenient for the data subjects to exercise their rights. In addition, data controllers identify the purposes and methods of processing personal data, and their primary responsibility is to adhere to the Regulation's standards and principles.

Protecting the confidentiality, security, and accuracy of the information gathered from children is another requirement. In addition, in compliance with the GDPR's purpose limitation, operators must only retain data for as long as is required for the original reason for which it was collected. If there will be an additional purpose, the data controller must re-obtain parental consent. For instance, a doctor should not divulge his/her patient list to a friend who owns a special education and rehabilitation centre in order to give special deals to the doctor's special education-needing patients.

Besides, they must protect the privacy and data protection rights of children and make all reasonable efforts, given the current level of technology, to get parental consent for processing children's data if the child is underage. They have extra responsibilities stemming from the principle of privacy by design and by default. Data protection by design involves adopting data protection principles from the design phase throughout the life cycle of a new project, product, or asset. Data protection by default entails that data controllers only process data that is required for their processing goals. It is also associated with the core concepts of data minimization and purpose limitation.

They also have additional duties related to working with the supervisory authority, especially in the event of data breaches. Within seventy-two hours of becoming aware of a personal data breach, the data controller is required to inform the supervisory authority. If the data in question belongs to children, data controllers must operate with heightened prudence, as a data breach may have far-reaching negative consequences for children than for adults.

Moreover, if the data breach is considered to pose a serious danger to the rights and freedoms of the data subject, they must notify the data subject without undue delay. This communication should be made in plain and clear language and w When children are under the age of consent, data controllers must inform their parents of a data breach.

Furthermore, data controllers have a major obligation to conduct a data protection impact assessment where a form of processing, especially one employing new technologies,

and the processing's goals pose a serious risk to the rights and freedoms of natural individuals. Data protection impact evaluations are an integral part of data protection by design and default. Using data protection impact assessments, for instance, data controllers can determine the technological and organisational measures to reduce the risks of the planned processing.

In GDPR Recital (75), there is a lengthy list of risks to the rights and freedoms of natural persons, including physical, material, and non-material damage, and it is explicitly stated that the risk may result from data processing, particularly when the personal data of vulnerable natural persons, such as children's personal data, is processed. Therefore, the data protection impact assessment should be conducted with special care when dealing with children's data, as the processing is likely to be high risk in this scenario.

Additionally, we underlined the operators' obligations under the COPPA. Several COPPA requirements pertain to facilitating the exercise of parental rights. It would be ideal, in our opinion, if the privacy policy, for example, featured engaging images that a child could grasp and be encouraged to read. There may be videos explaining information collection procedures and their consequences for younger children, allowing them to comprehend the operators' approach.

In compliance with the GDPR's data minimization principle, operators should not require children to provide more information than is strictly necessary to participate in an online activity. For instance, if the game requires only a nickname to join, the operators are prohibited from requesting more information such as the child's complete name, email address, or other identifying information. Comparing the two approaches, we claim:

It is evident that the GDPR is more comprehensive and detailed in terms of data controllers' duties and how they protect the personal data of data subjects by making it possible and easy for data subjects to exercise their rights, cooperating with supervisory authorities when necessary, and reducing the risks of processing by conducting data protection impact assessments. Nevertheless, regarding the obligations of data controllers to protect children's data, the GDPR falls behind. The GDPR draws a little distinction between data subjects as adults and data subjects as children, despite the fact that children require more specific protection due to their unique and more vulnerable status as data subjects. Therefore, it would be ideal to incorporate an article providing child-specific data controller obligations in the GDPR.

In contrast, all of the obligations of operators under COPPA concern the protection of children's privacy and how operators should ensure parental control over their

children's personal information. When children are young and unable to make decisions or realize the repercussions of personal data processing, it is plainly advantageous.

Nonetheless, if they are able and willing to do so, children should be allowed to participate in less dangerous actions such as deleting data from a website, unsubscribing, or restricting the transfer of personal data to other parties without parental consent in both legislations. Therefore, operators should give these options to children who choose to exercise control over their data and engage in less harmful online activities. Finally, given the significant risk associated with processing children's personal data, the COPPA should require operators to work with supervisory authorities and implement data protection/privacy impact assessments for such processing, as does the GDPR.

In Chapter 6, we examined free flow of personal data, a key component of the global digital economy. The GDPR makes it clear that data transfers between EU data controllers and third-country or international organisations are vital for international trade and collaboration. However, there has been no permanent and stable solution for EU-US data transfers due to fundamental inequalities in privacy and data protection. The seventh research question of this thesis was if the US will ever achieve the "adequate level" of data protection. Furthermore, the eighth research question was if there are any child-specific data transfer requirements under the GDPR, and if not, how the varying online consent ages for children across countries affect data transfers within the EU and to the US.

We observed that in the US, personal data regarded as a commodity, and a sector-specific approach restricts legislations to have certain objectives. Since different industries have different privacy and data protection standards, US privacy legislation are quite flexible. However, unregulated businesses in this scenario may be uncontrollable. On the contrary, the privacy and data protection are seen as fundamental rights that must be respected by the EU and GDPR was provided as a very comprehensive umbrella rule covering all the sectors.

We emphasised that neither the EU nor the US can afford to block personal data flow over the Atlantic, regardless of their different privacy and data protection approaches. Because the US is the EU's biggest trading partner, and they have the world's most interconnected economy. Therefore, for years, they have negotiated free data flow agreements.

This chapter reviewed the European Commission's partial adequacy decisions for the US. The Schrems I and II cases were also examined in order to understand how and why the

CJEU terminated the Safe Harbour and Privacy Shield. By doing so, we addressed the question of how third countries should offer EU data subjects with “essentially equivalent” level of data protection. The US lost its adequacy decisions with the CJEU's Schrems cases because it failed to address the crucial concepts, criteria, and requirements to provide essentially equivalent level of protection.

As we have indicated, US public authority access and surveillance were excessive and EU data subjects had no effective legal remedies, and there was no independent oversight mechanism, such as an independent Ombudsperson, to monitor public authority processing activities. The envisaged Transatlantic data privacy framework between the EU and the US should incorporate these principles and rules to avoid the potential Schrems III decision.

In the absence of adequacy decisions, SCCs and BCRs can be used to transfer data from the EU to the US. Besides, derogations can only be used in exceptional and specialised transfers. SCCs are utilised for recurring transfers from one EU data exporter company to a US data importer company, therefore they were commonly used. However, they need case-by-case consideration and inflict enormous burdens on data importers and exporters.

In most cases where the third country does not have an adequate level of data protection, data controllers should ensure that technical measures (e.g., encryption and pseudonymization), organisational measures (e.g., ISO certification, ENISA), and contractual measures (commitment to transparency, encouraging and assisting data subjects in exercising their rights) are in place. Those processes are expensive, especially for small and medium-sized businesses.

We added that data localisation may occur due to these issues and the unpredictable environment. In other words, data controllers may opt to keep their data within the Union and not transfer it outside. However, in that chapter, we explained why data localisation is not a proper solution. Over and above, the GDPR supports international data flow to enhance economic cooperation; hence, the so-called solution of data localisation conflicts with its objectives.

Thus, in order to provide a more stable and trustworthy data transfer environment, in March 2022, the EU and US agreed a new Transatlantic Data Privacy Framework. After this, *Biden* signed an Executive Order to implement the new EU-US Data Privacy Framework. They intend to improve the Safe Harbour and Privacy Shield systems with this new framework. Their goal is to create an agreement that the CJEU will not overturn.

We have argued that the implementation of this new framework will enhance the protection of EU data subjects' data from access by US national intelligence agencies. This

will be achieved through the establishment of a two-layered redress procedure. As we stated, this new framework promises to give stronger protection to EU data subjects than US people, as observed in Japan's adequacy decision, which also protects EU data subjects better than Japanese citizens and residents. We expect this arrangement to work in the US since it has worked between the EU and Japan for years.

The GDPR does not regulate the transfer of children's data, as we highlighted. We have advised that children's data should be treated differently and with more care than adult data transfers. We gave instances from online website practises. Instagram and Facebook do not even mention data transfer for children. However, Google and YouTube have relatively sophisticated data practises that declare they only disclose children's data with parental consent and also if their trusted processors process it on their behalf in line with their instructions, and for legal reasons.

We also attempted to raise awareness of the issue related to varying children's consent ages for digital platforms. For example, Hungary's online consent age is 16, whereas Finland's is 13. In this scenario, a 13-year-old Finnish child can consent to data transfer to Hungary. However, under Hungary's data protection laws, a child under 16 cannot consent to data transfer without parental consent. Thus, the consent provided by 13-year-old Finnish child to his/her personal data to be transferred to Hungary would be invalid according to Hungarian data protection. It would be the same between the EU Member States to US child data transfers since the age thresholds may also differ in their legislation. This issue is alarming, yet academics and lawmakers do not seem concerned. Consequently, we recommend the following:

The child data transfers from the EU to the US should be regulated in the upcoming Transatlantic Data Privacy Framework. It will also urge data controllers to include child-related data transfer requirements in their privacy policies. In order to provide a safe and stable environment for the transfer of children's personal data, Member States should agree on a uniform age of online consent. As national differences in legislation implementation and data protection authorities' interpretation raise EU legal compliance costs, consistent standards would aid data controllers in lowering the expenses associated with the transfer of children's data. Moreover, two-way approach seen in the Japan's adequacy decision and the two-layer redress and oversight mechanism appear promising this time. Nevertheless, the issues regarding the proportionality and necessity principles and bulk collection (including temporary bulk collection) should be addressed

adequately. *Max Schrems* or another individual would be failed in the third round if the practice will work as expected.

In the last chapter of this thesis, we discussed real-world examples such as social media sites, their privacy policies, child influencers, and parental sharing. We started this chapter with a discussion of the sociological and cultural changes caused by the development of social media platforms. In the past, sharing photographs and movies was limited to close family and friends through photo albums and videotapes. With the introduction of the Internet and social media platforms such as Facebook, Instagram, and YouTube, the situation has changed significantly. Due to the fact that individuals may now share their content online with millions of strangers, everyone has the potential to become so-called celebrities (i.e., influencers).

The ninth research question of this thesis was how the requirements of the GDPR and COPPA affect the practises of social media sites and the sharing activities of parents concerning their children. The last and the tenth research question was if excessive reliance on parental consent can protect the personal data and privacy of children. We answered these questions within Chapter 7.

Regarding the answer of the ninth research question, this thesis argues the following:

Given that the GDPR and COPPA restrict children under a specific age from revealing personal information online without parental consent, social media networks do not allow children under the age of consent to register accounts on their platform. However, neither of these legislations set restrictions on parental sharing. In other words, the GDPR and COPPA impose no penalties on parents who disclose personal information about their children on the Internet. However, social networking platforms prohibit the sharing of some types of information involving sexual abuse and violence against children.

For example, YouTube restricts the posting of nudity or sexual exploitation content, prank videos, content in the most private places of children (such as their bedroom and bathroom), and actions that may draw the attention of dangerous users. Both Instagram and Facebook restrict the content related to child exploitation and nudity.

Nevertheless, it is still possible to access restricted information on social networking sites, as illustrated by the real-world examples presented in this chapter. For example, you may discover an example of a barber pranking a child by pretending to cut off his ear and it is revealed that the boy's parents gave their consent for this content.

The parents of a very famous child influencer are sharing their daughter's bikini images with complete strangers, and there are several improper comments under the photos, which will disturb her when she is mature enough to comprehend them.

Notwithstanding, we appreciated Facebook's use of AI and ML technology to detect, and erase shared harmful data, such as nudity, violence, and sexual exploitation of children, in a manner similar to a suggestion we made in one of our previous publications. However, it would have been better to strengthen this system so that it could detect potentially harmful content before parents or other adults distribute it and prevent it from entering the Internet environment in the hands of malicious persons.

Some of the motivations of parents who share private moments of themselves and their children with strangers include feeling supported, being accepted by other parents, and creating a comfortable standard of life for their families with earning extra income. However, we debated if these benefits outweigh children's entitlement to data protection and privacy. On the one hand, parents can defend their internet sharing activities based on their right to free speech and right to informational self-determination (on behalf of their children). According to the EU Charter of Fundamental Rights and the first amendment to the US Constitution, everyone has the right to free expression.

According to the European Convention on Human Rights, on the other hand, freedom of expression must be limited so as not to harm the reputation of others. The US government also restricts free speech in some areas, including as invasion of privacy and the visual representation of children engaging in certain sexual actions or genital exposures in films or photographs. Taking toilet training and the first bath as examples, the sharing of naked photographs and the most intimate moments of children by millions of families is highly likely to harm the children's self-esteem, dignity, and privacy. We proposed that, in weighing these rather competing rights, we should favour the child's right to privacy, as was also urged in the decision of *Murray v. Express Newspapers Ltd (CA)*.

If children's privacy and data protection have already been infringed by their parents, as we illustrated with the Sidis case, we asserted that the right to be forgotten is essential for recovering the power and control over their data that they lost due to parental sharing. Freedom of speech is an exception to the right to erasure and right to be forgotten under the GDPR; however, where the data subject is a child, freedom of expression must be interpreted considerably more narrowly, and this exception should not be used.

In addition to preserving children's privacy, we addressed other reasons why the sharing of their personal information should be restricted, such as cyberbullying, identity theft, exposure to child pornography, prejudice and labelling, and even kidnapping. Because if malicious individuals obtain sensitive information about children's race, gender, and sexual orientation, they can bully or even blackmail them. Due to these sensitive details, a child may be labelled by his/her peers or subjected to discrimination by his/her teachers. Due to the permanence of the contents on the Internet, it may have a detrimental impact on their academic or professional careers.

We also stated regarding kidnapping that not only strangers, but also certain ill-intentioned relatives or acquaintances using the same social media platforms may use the provided information to persuade or deceive children to follow them, which can lead to kidnapping and the demand for ransom to release the children. Given that 76% of kidnappings and 90% of violent crimes against children are committed by relatives or friends, it is fair to be concerned about non-strangers.

Following a discussion of these potential concerns, we presented a survey indicating that eight out of ten parents share information about their children, despite the fact that only 16% of them are concerned that their children may be disturbed in the future as a result of their sharing. At that moment, we concluded that GDPR and COPPA should limit the information that parents may reveal about their children. Only reasonable family portraits or content that does not reveal any personal and/or sensitive information about children should be shared. We emphasised that some pictures taken from behind, blurred images, or the addition of emojis to the faces of children may constitute a small kind of censorship.

Livingstone et al. (2019) recently performed research on the data and privacy online of children growing up in the digital era, which yielded interesting findings regarding the perspectives of children's parents and teachers with regard to privacy and data protection. The study showed that children are less concerned with what social media sites do with their personal information and more worried about whether or if their family members or peers would bully them using this information. As a result, children may divulge personal information without being aware of potential data breaches or exploitative commercial operations, due to their lack of business awareness. For instance, a child can send a selfie to a friend by text message without realising that Instagram will also have access to this selfie. In this manner, sharing selfies is not just a social activity, but also a commercial one, as Instagram is involved.

This survey also revealed that parents have limited knowledge of digital privacy and, as a result, believe that their children should be taught digital privacy and literacy at school. Teachers, on the other hand, feel that parents should supervise and assist their children's internet activities more closely.

Accordingly, we recognised that parents and instructors lack the necessary skills to assist the children, which is why they pass the burden to one other. We proposed that the government should invest in digital literacy in schools, subsidise the deployment of instructors to schools, include digital literacy education into official curriculums, and offer free courses to parents. Therefore, parents and schools will have a better grasp of the concept of digital privacy and will be able to support children/students more efficiently.

As a consequence, the following is strongly suggested by this thesis as an answer to the tenth and the last research question:

The most effective way to protect children's privacy and data protection in the digital world is collaboration between governments, parents, schools and data controllers. Lawmakers should impose stricter restrictions on shared content that is relevant to children as an immediate solution, rather than relying excessively on parental consent. This is because neither parents nor children are always fully aware of the importance of privacy and data protection. These restrictions would also compel social media platforms to strengthen their privacy policies regarding hazardous or sensitive content related to children. As a long-term solution, the government can provide funding for schools to run seminars and lectures on digital literacy for both children and their parents. Furthermore, the legislations should be implemented in a child-friendly manner, and courts in the EU and the US should interpret them so as to protect the privacy and data protection rights of children. As such, they have the ability to serve as examples for other legal systems and jurisdictions.

Bibliography

Articles

- Adam D. Thierer: Social networking and age verification: Many hard questions; no easy solutions, Progress & Freedom Foundation Progress on Point Paper 14.5 (2007), 3.
- Adrienn Lukács: What is privacy? The history and definition of privacy, In: Gábor Keresztes (ed.): Tavaszi Szél 2016 Tanulmánykötet I., Budapest, Doktoranduszok Országos Szövetsége (2016), 259 <https://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf> (last visited 10 March 2023).
- Alan Watson: Legal transplants and European private law, Electronic Journal of Comparative Law, IV (2000), 13.
- Andrew Clearwater and J. Trevor Hughes: In the Beginning - An Early History of the Privacy Profession, Ohio State Law Journal 74, no. 6 (2013), 899.
- Anupam Chander: Is Data Localization a Solution for Schrems II?, Journal of International Economic Law, vol. 23.3, (2020), 781.
- Asli Alkis Tümtürk: Implications of Parental Sharing of Children's Personal Data Online, ArsBoni Jogi Folyoirat, X. evfolyam 2022/1-2 (2022), 3 available at https://arsboni.hu/wp-content/uploads/2022/09/Arsboni-foly%C3%B3irat_2022_1_2.pdf (last visited 10 March 2023).
- Asli Alkis Tümtürk: The Threshold Age for Children's Online Consent in Light of the Watson/Legrand Debate: Is Legal Transplant Possible in the Digital Era?, The Journal of Comparative Law vol. 17/1 (2022), 243.
- Asli Alkis, Investigating the usefulness of online age verification methods, Studia Iurisprudentiae Doctorandorum Miskolciensium, (2021) vol.1, 8.
- Asli Alkis: The impact of the Privacy Shield's invalidation on the EU-US dataflows, Studia Iurisprudentiae Doctorandorum Miskolciensium, (2022) vol.1, 34.
- Asli Alkis-Tümtürk: Uncertain future of transatlantic data flows: Will the United States ever achieve the 'adequate level' of data protection?, Hungarian Journal of Legal Studies, vol. 63 issue. 3 (2022) 294-311.
- Barbara Sandfuchs: The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18–Schrems II, GRUR International 70(3) (2021), 246.

- Ben Bratman: Brandeis and Warren's the Right to Privacy and the Birth of the Right to Privacy, *Tennessee Law Review* 69, no. 3 (2002), 629.
- Brooke Auxier, Monica Anderson, Andrew Perrin and Erica Turner: Children's engagement with digital devices, screen time, Pew Research Center, (2020), 2.
- Bunn Anna: Children and the 'Right to be Forgotten': What the right to erasure means for European children, and why Australian children should be afforded a similar right, *Media International Australia*, 170(1) (2019), 41.
- Business Europe, DIGITALEUROPE, the European Round Table for Industry, and European Automobile Manufacturers Association: Schrems II: Impact Survey Report, 2020, 1-14, <https://www.digitaleurope.org/resources/schrems-ii-impact-survey-report/> (last visited 10 March 2023).
- Carl Van der Maelen: The Coming-of-Age of Technology: Using Emerging Tech for Online Age Verifications, *Delphi 2* (2019), 115.
- Carrie MacMillan: COVID-19 Vaccine Authorized For Kids Ages 5 to 11: What Parents Need to Know, *Yale Medicine*, 20 May 2022, <https://www.yalemedicine.org/news/covid-vaccine-for-ages-5-to-11> (last visited 10 March 2023).
- Chelsea Wald: The secret history of ancient toilets, *Nature* 533, no. 7604 (2016), 457.
- CHOC (Children's Hospital of Orange County): The COVID-19 vaccine for kids under 12: What parents should know, last updated 11 November 2022, <https://health.choc.org/the-covid-19-vaccine-for-kids-under-12-what-parents-should-know/> (last visited 10 March 2023).
- Corien Prins: When Personal Data, Behavior and Virtual Identities Become a Commodity: Would a Property Rights Approach Matter, *SCRIPTed: A Journal of Law, Technology and Society* 3, no. 4 (2006), 280.
- Dan Svantesson: Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines, *OECD Digital Economy Papers*, No. 301, OECD Publishing (2020), 15.
- David Smahel, Hana Machackova, Giovanna Mascheroni, Lenka Dedkova, Elisabeth Staksrud, Kjartan Ólafsson, Sonia Livingstone, and Uwe Hasebrink: EU Kids Online 2020: Survey results from 19 countries (2020), *EU Kids Online*, 30.

- Emily A. Ivers: Using State-Based Adequacy Now, National Adequacy over Time to Anticipate and Defeat Schrems III, 62 BC L Rev. (2021) 2589-2591.
- Emily Linn: A Look into the Data Privacy Crystal Ball: A Survey of Possible Outcomes for the EU-US Privacy Shield Agreement, Vand. J. Transnat'l L. 50, (2017), 1312-1313.
- Eva Lievens and Valerie Verdood: Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation, Computer Law & Security Review 34, no. 2 (2018), 274.
- Fabio Nascimbeni and Steven Vosloo: Digital literacy for children: Exploring definitions and frameworks, UNICEF Office of Global Insight and Policy, Scoping Paper 1 (2019), 10.
- Flora Y. Wang: Cooperative Data Privacy: The Japanese Model of Data Privacy and the Eu-Japan GDPR Adequacy Agreement 33 Harv. JL & Tech. (2020) 690-691.
- Florent Thouvenin: Informational Self-Determination: A Convincing Rationale for Data Protection Law?, Journal of Intellectual Property, Information Technology and Electronic Commerce Law 12, no. 4 (2021), 248.
- Francesca Bignami and Giorgio Resta: Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance In Community Interests Across International Law (Eyal Benvenisti & Georg Nolte, eds., Oxford University Press, Forthcoming), GWU Law School Public Law Research Paper 2017-67 (2018), 10 and 18.
- Gaëlle Ouvrein and Karen Verswijvel: Sharenting: Parental adoration or public humiliation? A focus group study on adolescents' experiences with sharenting against the background of their own impression management, Children and Youth Services Review 99 (2019), 320.
- Haeji Hong: Dismantling the Private Enforcement of the Privacy Act of 1974: Doe v. Chao, Akron Law Review 38, no. 1 (2005), 76-77.
- Haley Keltie: Sharenting and the (Potential) Right to Be Forgotten, Ind. LJ, 95 (2020), 1006.
- Harry Kalven Jr.: Privacy in Tort Law--Were Warren and Brandeis Wrong, Law and Contemporary Problems 31, no. 2 (1966), 327.
- Holly Kathleen Hall: Oversharenting; Is It Really Your Story to Tell, John Marshall Journal of Information Technology and Privacy Law 33, no. 3 (2018), 132.

- James H. Barron: Warren and Brandies, the Right to Privacy, 4 Harv. L. Rev. 193 (1890): Demystifying a Landmark Citation, Suffolk University Law Review 13, no. 4 (1979), 910.
- James Lee: SB 568: Does California's Online Eraser Button Protect the Privacy of Minors, 48(3) U.C. Davis Law Review (2015), 1203.
- John C. Reitz: How to Do Comparative Law, American Journal of Comparative Law 46, no. 4 (Fall 1998), 621.
- John Selby: Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?, International Journal of Law and Information Technology, 25.3 (2017), 230.
- Jonah Force Hill: The growth of data localization post-snowden: Analysis and recommendations for us policymakers and business leaders, The Hague Institute for Global Justice, Conference on the Future of Cyber Governance (2014), 32.
- Jules Polonetsky: Online Age Verification for Our Children A Report on the Tools and Resources Available for Safeguarding the First Generation of Digital Natives. 31st International Conference of Data Protection and Privacy Commissioners in Madrid, Future of Privacy Forum, (2009), 3-4.
- Manu J. Sebastian: The European Union's General Data Protection Regulation: How Will It Affect Non-EU Enterprises, Syracuse Journal of Science and Technology Law 31 (2014-2015), 222-223.
- Margaret Jane Radin: Incomplete commodification in the computerized world In Niva Elkin-Koren and Neil Weinstock Netanel (eds.): The commodification of information, The Hague: Kluwer Law International (2002), 17-18.
- Marie-Anne Frison-Roche: Remarques sur la distinction de la volonté et du consentement en droit des contrats, RTD civ (1995), 574.
- Mark Van Hoecke: Methodology of comparative legal research, Law and method (2015), 13-16.
- Máté Dániel Szabó: Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival, Információs Társadalom: társadalomtudományi folyóirat 5, no. 2 (2005), 44.
- Matthew Newman, Mike Swift and Vesela Gladicheva: GDPR and CCPA Start to Bare Teeth as Privacy Protection Goes Global, 21(3) Business Law International (2020), 276.

- Milda Macenaite and Eleni Kosta: Consent for processing children’s personal data in the EU: following in US footsteps?, *Information & Communications Technology Law* 26, no. 2 (2017), 160.
- Neil M. Richards: The dangers of surveillance, *Harvard Law Review* 126, no. 7 (2013), 1952-1958.
- Nigel Cory, Ellyse Dick, and Daniel Castro: The Role and Value of Standard Contractual Clauses in EU-US Digital Trade, *Information Technology and Innovation Foundation* (2020), 13.
- Oliver Patel and Nathan Lea: EU-UK data flows, Brexit and no-deal: Adequacy or disarray?, *UCL European Institute, Brexit Insights*, (2019), 10.
- Paul M. Schwartz and Karl-Nikolaus Peifer: Transatlantic Data Privacy *Law 106 Geo. LJ.* (2017) 132-137 cited in Paul M. Schwartz: *Global Data Privacy: The EU Way* 94 *NYUL Rev.* (2019) 771-773.
- Paul M. Schwartz: *Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, the State, and New Technology*, *William and Mary Law Review* 53, no. 2 (2011), 368.
- Peter Mei: The EC Proposed Data Protection Law, *Law and Policy in International Business* 25, no. 1 (1993), 305.
- Philip Bontrager, Aditi Roy, Julian Togelius, Nasir Memon, and Arun Ross: Deepmasterprints: Generating masterprints for dictionary attacks via latent variable evolution, 2018 *IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, IEEE (2018), 1-9.
- Pierre Legrand: The impossibility of ‘legal transplants, *Maastricht journal of European and comparative law* 4, no. 2 (1997), 111.
- Raphael Gellert and Serge Gutwirth: The legal construction of privacy and data protection, *Computer Law & Security Review* 29, no. 5 (2013), 524.
- Samuel D. Warren and Louis D. Brandeis: Right to Privacy, *Harvard Law Review* 4, no. 5 (1890), 193-220.
- Shannon Sorensen: Protecting Children's Right to Privacy in the Digital Age: Parents as Trustees of Children's Rights, *Children's Legal Rights Journal* 36, no. 3 (2016), 156-157.
- Sheila Donovan: ‘Sharenting’: The Forgotten Children of the GDPR, *Peace Human Rights Governance* 4(1), (2020), 43.

- Simone van der Hof and Eva Lievens: The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR, *Communications law* 23.1 (2018), 20.
- Simone Van der Hof: I agree, or do I: a rights-based analysis of the law on children's consent in the digital world, *Wis. Int'l LJ* 34 (2016), 412-414.
- Sonia Livingstone and Jasmina Byrne: Challenges of parental responsibility in a global perspective. In: Urs Gasser (ed.): *Digitally Connected: Global Perspectives on Youth and Digital Media* (2015), 26-29. Cambridge: Berkman Center for Internet and Society, Harvard University.
- Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri: Children's data and privacy online: Growing up in a digital age. An evidence review, London: London School of Economics and Political Science (2019), 35.
- Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri: Data and privacy literacy: The role of the school in educating children in a datafied society, *The handbook of media education research* (2020), 415.
- Stacey B. Steinberg: Sharenting: Children's Privacy in the Age of Social Media, *Emory Law Journal* 66, no. 4 (2017), 876-877.
- Szilvia Váradi: Legal challenges of processing health data in the shadow of COVID-19 in the European Union, *Forum: Acta Juridica Et Politica*, Vol. 11. No. 4 (2021), 358-362.
- Tehila Minkus, Kelvin Liu, and Keith W. Ross: Children seen but not heard: When parents compromise children's online privacy, In *Proceedings of the 24th international conference on World Wide Web* (2015), 777.
- Vernon Valentine Palmer: Three Milestones in the History of Privacy in the United States, *Tulane European and Civil Law Forum* 26 (2011), 71.
- Karen Verswijvel, Michel Walrave, Kris Hardies, Wannes Heirman: Sharenting, is it a good or a bad thing? Understanding how adolescents think and feel about sharenting on social network sites, *Children and youth services review* 104 (2019) 104401, 7.
- Virginia A. M. Talley: Major Flaws in Minor Laws: Improving Data Privacy Rights and Protections for Children under the GDPR, *Indiana International & Comparative Law Review* 30, no. 1 (2019), 143.

Books

- Alan F. Westin: *Privacy and Freedom*, Atheneum New York (1967), 1-487.
- Alan Watson: *Introduction to Legal Transplants in Legal Transplants: An Approach to Comparative Law* (1974), 21.
- Niva Elkin-Koren and Neil Weinstock Netanel (eds.): *The commodification of information*, The Hague: Kluwer Law International (2002), 17-18.
- Paul Craig: *The Evolution of EU Law*, 2nd ed. Oxford: Oxford University Press (2011), 335.
- Samuel Dash: *The intruders: Unreasonable searches and seizures from King John to John Ashcroft*, Rutgers University Press (2004), 9.
- W. Page Keeton (et al.): *Prosser and Keeton on the Law of Torts*, West Publishing Co. St. Paul Minn. 5th ed. (1984), 850-851.

Legal Texts

- 16 CFR Part 312 Children's Online Privacy Protection Act; Final Rule, 15 U.S.C. §§ 6501–6506, Federal Register Vol. 64, No. 212, 03.11.1999, p. 59888-59915.
- 28 CFR 201 Data Protection Review Court; Final Rule, 28 U.S.C §§ 509, 510-512, Federal Register Vol. 87, No. 198, 14.10.2022, pp. 62303-62308.
- Article 29 Data Protection Working Party, Adequacy Referential, 18/EN 6 February 2018 WP 254 rev01.
- Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN WP251rev.01, last revised and adopted on 6 February 2018, p. 1-37, 26.
- Article 29 Data Protection Working Party, Opinion 03/2014 on Personal Data Breach Notification, 693/14/EN WP 213, 25 March 2014, p. 5-6.
- Article 29 Working Party, Guidelines on consent under Regulation 2016/679 17/EN WP 259 rev.01, 10 April 2018, 1-31.
- Assembly, UN General, Convention on the Rights of the Child, United Nations, Treaty Series 1577, no. 3 (1989), pp. 1-23.

- Berliner Beauftragte für Datenschutz und Informationsfreiheit: Nach „Schrems II“: Europa braucht digitale Eigenständigkeit, Pressemitteilung, 711.424.1, 17 Juli 2020.
https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2020/20200717-PM-Nach_SchremsII_Digitale_Eigenstaendigkeit.pdf (last visited 10 March 2023).
- Biometric Information Privacy Act (BIPA) of 2018, 740 ILL. COMP.STAT. 14/1-99.
- California Consumer Privacy Act (CCPA) of 2018, CAL. CIV.CODE §§ 1798.100-1798.199.100.
- Charter of Fundamental Rights of the European Union, OJ C 326, 26.12.2012, p. 391-407, Article 7: “Everyone has the right to respect for his or her private and family life, home and communications.”
- Charter of Fundamental Rights of the European Union, OJ C 326, 26.12.2012, p. 391-407, Article 7-8.
- Charter of Fundamental Rights of The European Union, OJ C 364, 18.12.2000, pp. 1-22, Article 11.
- CJEU, Judgment in Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, Press Release No 91/20, 16 July 2020, p. 1-3.
<https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf> (last visited 10 March 2023).
- Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215, 26.07.2000, p. 7-47.
- Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 OJ L 344/ 100, 17.12.2016, p. 100-101.
- Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207/1, 12.07.2016, 1-112.

- Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/ 679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, OJ L 76, 19.3.2019, p. 1–58.
- Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom under the Act on the Protection of Personal Information, OJ L 360, 11.10.2021, p. 1-68.
- Commission Staff Working Paper, Impact Assessment, SEC (2012) 72 final, p. 68, https://www.europarl.europa.eu/cmsdata/59702/att_20130508ATT65856-1873079025799224642.pdf (last visited 10 March 2023).
- Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, p. 47–390, Article 288.
- Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union Consolidated version of the Treaty on European Union Consolidated version of the Treaty on the Functioning of the European Union Protocols Annexes to the Treaty on the Functioning of the European Union Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007 Tables of equivalences, OJ C 202, 7.6.2016, p. 1–388, Article 5(4).
- Council of Europe, Convention 108+ Convention for the protection of individuals with regard to the processing of personal data, ETS No. 108 (2018) https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf (last visited 10 March 2023).
- Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 28.01.1981, ETS No. 108.
- Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, https://www.echr.coe.int/documents/convention_eng.pdf (last visited 10 March 2023).
- Court of Justice of the European Union, The Court of Justice declares that the Commission’s US Safe Harbour Decision is invalid, Press Release, 117/15, Judgment in

Case C-362/14 Maximilian Schrems v Data Protection Commissioner, 6 October 2015, 1-3.

- Data Protection Commission Ireland, Children Front and Centre, Fundamentals for a Child-Oriented Approach to Data Processing-Draft Version for Public Consultation, December 2020, 33.
- Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services OJ L 241, 17.9.2015, pp. 1-15.
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31, 23.11.1995, pp. 31–50.
- EDPB, Guidelines 04/2021 on codes of conduct as tools for transfers, 2021, 1-14. https://edpb.europa.eu/system/files/2021-07/edpb_guidelinescodesconducttransfers_publicconsultation_en.pdf (last visited 10 March 2023).
- EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 2.1 Adopted on 07 July 2021, pp. 1-51. https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf (last visited 10 March 2023).
- EDPB, Guidelines 07/2022 on certification as a tool for transfers, version 1.0, 14 June 2022, 1-19. https://edpb.europa.eu/system/files/2022-06/edpb_guidelines_202207_certificationfortransfers_en_1.pdf (last visited 10 March 2023).
- EDPB, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework (28 February 2023), pp. 1-54, https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf (last visited 10 March 2023).
- EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0, 18.06.2021, 3. <https://edpb.europa.eu/system/files/2021->

[06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf](https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/response_s_to_edpb_recommendations.pdf)

(last visited 10 March 2023).

- EDPB, Why a good additional technical safeguard is hard to find- A response to the consultation on the EDPB draft recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 2 https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/response_s_to_edpb_recommendations.pdf (last visited 10 March 2023).

- EDPS, The History of the General Data Protection Regulation,
- European Commission, Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Preamble, COM(92) 422 final - SYN 287, OJ C 311/30, 27.11.1992, pp. 30-61.

- European Commission, Annex to the Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, Brussels, 4.6.2021, C(2021) 3972 final, 6, Clause 8.6 “Sensitive Data”.

- European Commission, Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council, OJ L 199/18, 7.6.2021, p. 18-30.

- European Commission, Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, OJ L199/31, 7.6.2021, p. 31-61.

- European Commission, Commission Staff Working Document, Accompanying the document Communication from the Commission to the European Parliament and the Council Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation, Brussels, 24.6.2020, SWD(2020) 115 final, pp. 1-52, 17.

- European Commission, Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions a Digital Decade for children and youth: the new European

strategy for a better internet for kids (BIK+), Brussels, 11.5.2022 COM (2022) 212 final, 6.

- European Commission, Communication from the Commission to the European Parliament and the Council Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, Brussels, 24.6.2020, COM (2020) 264 final, pp. 1-18.
- European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, Brussels, 3.6.2021 COM (2021) 281 final 2021/0136 (COD).
- European Commission: Communication from the Commission to the European Parliament and the Council Exchanging and Protecting Personal Data in a Globalised World, COM/2017/07 final, 10.01.2017, 7.
- [European Data Protection Board, Approved Binding Corporate Rules, https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en?page=1](https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en?page=1) (last visited 28 February 2023).
- European Data Protection Supervisor (EDPS), Data Protection, https://edps.europa.eu/data-protection/data-protection_en (last visited 13 January 2023).
- Executive Order No. 14086, vol. 87 no. 198 Federal Register, 14.10.2022, pp. 62283-62297, Section 2(c)(i)(B).
- Executive Order No. 14086, vol. 87 no. 198 Federal Register, 14.10.2022, pp. 62283-62297, Section 2(c)(i)(B).
- Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (1974).
- Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-1885, 25.10.1978, §1801(h) "Minimization procedures".
- Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-1885, 25.10.1978, §1801(h) "Minimization procedures".
- GDPR.EU, What is GDPR, the EU's new data protection law?: History of GDPR: <https://gdpr.eu/what-is-gdpr/> (last visited 22 January 2023).
- Guidelines 2/2018 of the European Data Protection Board (EDPB) on derogations of Article 49 under Regulation 2016/679 7 (May 25, 2018), 4-5.

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf (last visited 10 March 2023).

- Health Insurance Portability and Accountability Act. Pub. L. No. 104-191, 110 Stat.1936 (1996).
- https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (last visited 18 January 2023).
- N.Y. Sess. Laws 1903, ch. 132, §§ 1-2, amended by N.Y. Civ. Rights Law, §§ 50-51 (McKinney 1909).
- Personal Information Protection Commission: Amended Act on the Protection of Personal Information (Tentative Translation) (June 2020)
https://www.ppc.go.jp/files/pdf/APPI_english.pdf (last visited 10 March 2023).
- Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896, as amended 5 U.S.C. § 552a.
- 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), OJ 2016 L 119, 04.05.2016, pp. 1-88.
- S.B. 568, 2013 LEG. 2013-14 SESS. (Cal. 2013),
https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568 (last visited 10 March 2023).
- Telephone Consumer Protection Act of 1991, 47 U.S. Code § 227 (1991).
- The White House: Fact Sheet: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework (7 October 2022),
<https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/> (last visited 10 March 2023).
- U.S. Const. amend. I: “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.”
- U.S. Const. amend. XIV section 1.1: “All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall

abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.”

- U.S. Government Publishing Office (GPO): The Constitution of the United States of America Analysis and Interpretation Centennial Edition Interim Edition: Analysis of Cases Decided by the Supreme Court of the United States to June 27, 2016, 112th Congress 2nd Session, Document No: 112-9, pp. 1-2835, 1285 et seq.
- UN Commission on Human Rights, Convention on the Rights of the Child, E/CN.4/RES/1990/74, 07.03.1990.
- United Nations Committee on the Rights on the Child (2013) General Comment No. 14 on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1). CRC/C/GC/14, p. 18, para. 84.
- William Blackstone and William Carey Jones (Editor): Commentaries on the Laws of England, San Francisco, Bancroft-Whitney Co. (1916), 2430-2431. European Council of Medical Orders, Principles of European medical ethics, Article 7. <http://www.ceom-ecmo.eu/en/view/principles-of-european-medical-ethics> (last visited 10 March 2023).
- Working Party’s Working Document on the Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU Data Protection Directive, DG XV 1998 D/5025/98 WP12.

Legal Cases

- BVerfG, Order of the First Senate of 15 December 1983 - 1 BvR 209/83 -, paras. 1-214, BVerfGE 65, 1 - 71 Volkszählung.
- Case 113 F.2d 806, Sidis v. F-R Pub. Corporation (No. 400), Judgement of the Court of Appeals for the Second Circuit, New York, 22 July 1940.
- Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González EU:C:2014:317.
- Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems EU:C:2020:559.
- Case C-362/14 Maximillian Schrems v Data Protection Commissioner EU:C:2015:650.
- Case C-450/06 Varec [2008] ECR I-581, EU:C:2008:91, para. 48.

- Case C-507/17 Google LLC v Commission nationale de l'informatique et des libertés (CNIL) EU:C:2019:772.
- Case C-80/06, Carp v. Electricité de France (EDF) [2007] ECR I-4473, EU:C:2007:327, para. 20.
- Case EWCA Civ446, Murray v Express Newspapers plc and another, Judgement of the Court of Appeal, England and Wales, 7 May 2008, 512.
- Dudgeon v. the United Kingdom judgment on 22 October 1981, no. 7525/76 para. 40-41.
- Griswold v. State of Connecticut, 381 U.S. 479 (1965), 484-486.
<https://tile.loc.gov/storage-services/service/ll/usrep/usrep381/usrep381479/usrep381479.pdf> (last visited 9 January 2023).
- Klass and Others v. Germany judgment on 6 September 1978, no. 5029/71 para. 41.
- Leander v. Sweden judgment of 26 March 1987, no. 9248/81 para. 46-48.
- Niemietz v. Germany judgment on 16 December 1992, no. 13710/88 par. 28-33.
- Powell and Rayner v. the United Kingdom judgment of 21 February 1990, no. 9310/81, para. 41.
- Szabó and Vissy v. Hungary judgment 12 January 2016, no. 37138/14 para. 73.

Websites

- A Parent and Carer's Guide to Instagram: Manage Privacy, 15-16
https://www.internetmatters.org/wp-content/uploads/2021/11/UK_Instagram_-_parent_and_carer_guide_to_instagram.pdf (last visited 10 March 2023).
- Apple, Siri: <https://www.apple.com/siri/> (last visited 10 March 2023).
- Apple, Use Face ID on your iPhone or iPad Pro: <https://support.apple.com/en-us/HT208109#:~:text=Tap%20Set%20Up%20Face%20ID,your%20head%2C%20tap%20Accessibility%20Options>. (last visited 10 March 2023).
- BBC News, Edward Snowden: Leaks that exposed US spy programme, 17 January 2014, <https://www.bbc.com/news/world-us-canada-23123964> (last visited 10 March 2023).
- BBC News: Amanda Todd: Dutchman sentenced for fatal cyber-stalking (15 October 2022) <https://www.bbc.com/news/world-us-canada-63218797> (last visited 10 March 2023).

- BEUC, Making European Digital Identity as Safe as It Is Needed, https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-016_eidas_position_paper.pdf , 1 (last visited 10 March 2023).
- Britannica, Joe Biden, <https://www.britannica.com/biography/Joe-Biden> (last visited 28 February 2023).
- Brooke Auxier, Monica Anderson, Andrew Perrin and Erica Turner, Children’s engagement with digital devices, screen time, Pew Research Center, (2020). 2. <https://www.pewresearch.org/internet/2020/07/28/childrens-engagement-with-digital-devices-screen-time/> (last visited 23 January 2023).
- CBC News: Amanda Todd's parents recall teenager's anguish at recurring social media torment (7 June 2022) <https://www.cbc.ca/news/canada/british-columbia/todd-sextortion-trial-coban-1.6480477> (last visited 10 March 2023).
- CBC News: Parents, Dutch police investigator testify in trial of man accused of cyberbullying Amanda Todd, (11 June 2022) <https://www.cbc.ca/news/canada/british-columbia/amanda-todd-week-one-1.6485200> (last visited 10 March 2023).
- Children may also have bank accounts with the consent of their parents or guardians. For instance: HSBC, Children’s Bank Accounts: <https://www.hsbc.co.uk/current-accounts/products/children/> (last visited 10 March 2023).
- Complying with COPPA: Frequently Asked Questions, Why does COPPA apply only to children under 13? What about protecting the online privacy of teens?: <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions> (last visited 10 March 2023)
- Council of Europe, Chart of signatures and ratifications of Treaty 108, <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty=108> (last visited 13 January 2023).
- Deutsche Welle: The sixth eye?, 22 November 2013, <https://www.dw.com/en/us-lawmakers-push-for-german-entrance-to-five-eyes-spy-alliance/a-17246049> (last visited 10 March 2023).
- EPRS, Update on the state of play of the EU-US data transfer rules, Members' Research Service, 14-20. [https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/625151/EPRS_IDA\(2018\)625151_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/625151/EPRS_IDA(2018)625151_EN.pdf) (last visited 10 March 2023).

- euCONSENT, A summary of the achievements and lessons learned of the euCONSENT project and what comes next (7 December 2022) <https://euconsent.eu/a-summary-of-the-achievements-and-lessons-learned-of-the-euconsent-project-and-what-comes-next/> (last visited 21 January 2023).
- EuConsent, Digital Age of Consent under the GDPR: <https://euconsent.eu/digital-age-of-consent-under-the-gdpr/#:~:text=As%20per%20Article%208%20of,at%20least%2016%20years%20old>. (last visited 10 March 2023)
- euCONSENT, euCONSENT's first large scale pilot (18 March 2022) <https://euconsent.eu/euconsents-first-large-scale-pilot/> (last visited 21 January 2023).
- euCONSENT, euCONSENT's first large scale pilot: What did the participants have to do? (18 March 2022) <https://euconsent.eu/euconsents-first-large-scale-pilot/> (last visited 21 January 2023).
- euCONSENT, FAQ: What is euCONSENT?, <https://euconsent.eu/faq/> (last visited 21 January 2023).
- European Commission, Binding Corporate Rules (BCR), https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en (last visited 10 March 2023).
- European Commission, New European strategy for a Better Internet for Kids – Questions and Answers, 11 May 2022, 12. How will the new strategy address age verification?: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_2826 (last visited 10 March 2023).
- European Commission, Standard Contractual Clauses, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (last visited 10 March 2023).
- European Commission, Study on the impact of marketing through social media, online games and mobile applications on children's behaviour (1 March 2016) https://commission.europa.eu/publications/study-impact-marketing-through-social-media-online-games-and-mobile-applications-childrens-behaviour_en (last visited 10 March 2023).
- European Commission, Trade, EU trade relationships by country/region, Countries and Regions, United States: <https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/united->

[states_en#:~:text=The%20European%20Union%20and%20the,and%20investment%20partner%20by%20far](#)(last visited 10 March 2023)

- European Commission, Types of EU law, Types of EU legal acts: Directives, [Types of EU law \(europa.eu\)](#) (last visited 13 January 2023).
- European Commission, Types of EU law, Types of EU legal acts: Regulations, https://commission.europa.eu/law/law-making-process/types-eu-law_en (last visited 18 January 2023).
- European Commission: Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection' (13 January 2018): https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited 10 March 2023).
- European Commission: Data protection: Commission adopts adequacy decisions for the UK (28 June 2021): https://ec.europa.eu/commission/presscorner/detail/ro/ip_21_3183 (last visited 10 March 2023).
- European Commission: European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework (25 March 2022) https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087 (last visited 10 March 2023).
- European Commission: Questions & Answers: EU-U.S. Data Privacy Framework (7 October 2022) https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_6045 (last visited 10 March 2023).
- European Commission: Trans-Atlantic Data Privacy Framework (25 March 2022), https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100 (last visited 10 March 2023).
- European Data Protection Supervisor (EDPS), Data Protection: Privacy- a fundamental right, https://edps.europa.eu/data-protection/data-protection_en (last visited 22 January 2023).
- European Data Protection Supervisor (EDPS), Data Protection: What is data protection?, https://edps.europa.eu/data-protection/data-protection_en (last visited 22 January 2023).

- European Data Protection Supervisor (EDPS), Data Protection: What is privacy?, https://edps.europa.eu/data-protection/data-protection_en (last visited 22 January 2023).
- Facebook data policy includes Instagram terms as well, but you may also check it here: Instagram, Help Centre, Data Policy: How do we operate and transfer data as part of our global services? <https://help.instagram.com/155833707900388> (last visited 10 March 2023).
- Facebook Help Center, How to Report Things, How do I report a child under the age of 13 on Facebook?: https://www.facebook.com/help/157793540954833/?helpref=uf_share (last visited 10 March 2023).
- Facebook, Data Policy: How do we operate and transfer data as part of our global services? <https://m.facebook.com/privacy/policy/version/20220104/> (last visited 10 March 2023).
- Facebook, Help Centre, Safety Resources for Parents: How to request data from your underage child's Facebook account? https://www.facebook.com/help/173734372685099/?helpref=uf_share (last visited 10 March 2023).
- Facebook, Help Centre: How do I report a child under the age of 14 on Facebook in South Korea or Spain?, https://www.facebook.com/help/100532533374396/?helpref=uf_share (last visited 10 March 2023). See the reporting form only for Spain and South Korea: <https://www.facebook.com/help/contact/1408156889442791> (last visited 10 March 2023).
- Facebook, Privacy Centre: Where is information transferred? <https://www.facebook.com/privacy/policy/?subpage=9.subpage.2-WhereIsInformationTransferred> (last visited 10 March 2023).
- Facebook, Safety Centre, Online Child Protection: Our Policies <https://www.facebook.com/safety/onlinechildprotection> (last visited 10 March 2023).
- Facebook, Sign Up: <https://www.facebook.com/signup> (last visited 10 March 2023).
- Federal Trade Commission, Complying with COPPA: Frequently Asked Questions, Verifiable Parental Consent, How do I get parental consent?: <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked->

[questions#I.%20Verifiable%20Parental%20Consent](#), FAQ I.4. (last visited 10 March 2023).

- Federal Trade Commission, Verifiable Parental Consent and the Children's Online Privacy Rule: <https://www.ftc.gov/business-guidance/privacy-security/verifiable-parental-consent-childrens-online-privacy-rule> (last visited 10 March 2023).
- Federal Trade Commission: Complying with COPPA: Frequently Asked Questions, Why does COPPA apply only to children under 13? What about protecting the online privacy of teens?, <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions> (last visited 10 March 2023).
- For more information about OneTrust platform and their automated data protection impact assessment system: OneTrust, products> PIA and DPIA Automation, <https://www.onetrust.com/products/pia-and-dpia-automation/> (last visited 10 March 2023).
- FRA (European Union Agency for Fundamental Rights), Minimum age requirements related to rights of the child in the EU, Social rights; Employment; Education; Alternative care; LGBTI and Mobility: https://fra.europa.eu/en/publications-and-resources/data-and-maps/minag?dataSource=MINAG_en_62756&media=png&width=740&topic=group05&question=MINAG_HE01&plot=MAP&subset=NONE&subsetValue=NONE&answer=MINAG_HE01&year=2017 (last visited 10 March 2023).
- FRA, Consenting to medical treatment without parental consent: <https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements-concerning-rights-child-eu/consenting-medical-treatment-without-parental-consent#:~:text=However%2C%20where%20a%20medical%20intervention,is%20set%20at%2015%20years.> (last visited 10 March 2023).
- FRA, Minimum age requirements related to rights of the child in the EU, Marriage and sexual consent; Citizenship; Political Participation; Religion; Health: https://fra.europa.eu/en/publications-and-resources/data-and-maps/minag?dataSource=MINAG_en_62756&media=png&width=740&topic=group05&question=MINAG_HE01&plot=MAP&subset=NONE&subsetValue=NONE&answer=MINAG_HE01&year=2017 (last visited 10 March 2023).
- Fun Brain, Privacy Policy: <https://www.funbrain.com/privacy-policy> (last visited 10 March 2023).

- Fun Brain: <https://www.funbrain.com/> (last visited 10 March 2023).
- Global News: Exclusive: Mountie who worked Amanda Todd case speaks for first time (10 August 2022) <https://globalnews.ca/news/9050914/amanda-todd-officer-speaks/> (last visited 10 March 2023).
- Google Family Link <https://families.google/familylink/> (last visited 10 March 2023).
 - Google Family Link, Privacy Notice for Google Accounts and Profiles Managed with Family Link, for Children under 13 (or applicable age in your country) (“Privacy Notice”): Information Google Shares <https://families.google.com/familylink/privacy/child-policy/> (last visited 10 March 2023).
 - Google, Help Centre: Age requirements on Google Accounts, Find your country’s age requirement, <https://support.google.com/accounts/answer/1350409?hl=en#zippy=%2Ceurope> (last visited 10 March 2023).
 - Google, Privacy & Terms: Data transfers <https://policies.google.com/privacy?hl=en-US#infosharing> (last visited 10 March 2023).
 - Google, Sign Up: <https://accounts.google.com/signup/v2/webcreateaccount?flowName=GlifWebSignIn&flowEntry=SignUp> (last visited 10 March 2023).
 - Happify, Legal, Happify™ Privacy Policy: Last Updated July, 2020, <https://www.happify.com/public/legal/#legal> (last visited 10 March 2023).
 - HSBC Voice ID: <https://www.hsbc.com.hk/ways-to-bank/phone/voice-id/> (last visited 10 March 2023).
 - ICO, Data protection by design and default, at What is data protection by design?, and at What is data protection by default?: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/#dpd3> (last visited 10 March 2023).
 - ICO, Data protection by design and default, How does data protection by design and by default link to data protection impact assessments (DPIAs)?: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/#dpd3>

and-

[default/#:~:text=A%20DPIA%20is%20a%20tool,by%20design%20and%20by%20default. \(last visited 10 March 2023\).](#)

- If we search on LinkedIn or other job search platforms, we may come across several announcements for open positions such as data protection/privacy officer, data privacy specialist, privacy operations specialist, and so on: LinkedIn, Privacy Officer jobs in Hungary:

<https://www.linkedin.com/jobs/search/?geoId=100288700&keywords=privacy%20officer&location=Hungary> (last visited 10 March 2023).

- Information Commissioner's Office (ICO), The benefits of data protection laws, [- Information Commissioner's Office \(ICO\), What rights do children have?, When may a child exercise these rights on their own behalf?: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/what-rights-do-children-have/> \(last visited 10 March 2023\).](https://ico.org.uk/for-organisations/sme-web-hub/the-benefits-of-data-protection-laws/#:~:text=And%20you%20have%20to%20protect,discrimination%20or%20even%20physical%20harm. (last visited 23 January 2023).</div><div data-bbox=)

- Instagram Help Centre, How to Report Things, How do I report a child under the age of 13 on Instagram?: https://help.instagram.com/2922067214679225/?helpref=hc_fnav (last visited 10 March 2023).

- Instagram Help Centre, Sharing to other social networks, <https://help.instagram.com/169948159813228> (last visited 1 March 2023).

- Instagram, Help Centre, Tips for Parents: How do I report a child under the age of 13 on Instagram? https://help.instagram.com/517920941588885/?helpref=uf_share (last visited 10 March 2023).

- Instagram, Help Centre: Community Guidelines, https://help.instagram.com/477434105621119/?helpref=uf_share (last visited 10 March 2023).

- Instagram, Kids Diana Show (image posted on 21 August 2021) <https://www.instagram.com/p/CSeZgdHjkVF/?hl=tr> (last visited 10 March 2023).

- Johnson & Johnson Privacy Policy: Crossborder Transfers
<https://www.jnj.com/corporate/privacy-policy#:~:text=Unless%20we%20specifically%20request%20or,life%20or%20sexual%20orientation%2C%20criminal> (last visited 10 March 2023).
- Johnson & Johnson, Privacy Policy: Contacting us
<https://www.jnj.com/corporate/privacy-policy> (last visited 10 March 2023).
- Johnson & Johnson, Privacy Policy: Use by Minors
<https://www.jnj.com/corporate/privacy-policy> (last visited 10 March 2023).
- Meta Newsroom: What Our Research Really Says About Teen Well-Being and Instagram (26 September 2021) <https://about.fb.com/news/2021/09/research-teen-well-being-and-instagram/> (last visited 10 March 2023).
- Meta, Child sexual exploitation, abuse and nudity, https://transparency.fb.com/en-gb/policies/community-standards/child-sexual-exploitation-abuse-nudity/?source=https%3A%2F%2Fwww.facebook.com%2Fcommunitystandards%2Fchild_nudity_sexual_exploitation (last visited 26 January 2023).
- Meta, Facebook Community Standards, <https://transparency.fb.com/en-gb/policies/community-standards/?source=https%3A%2F%2Fwww.facebook.com%2Fcommunitystandards> (last visited 10 March 2023).
- Mr. Alkohol (Coctails&Drinks): <https://mralkohol.hu/> (last visited 10 March 2023).
- My story: Struggling, bullying, suicide, self-harm, *Thesomebodytoknow* videos, available at: <https://www.youtube.com/watch?v=vOHXGNx-E7E>, (last visited 10 March 2023).
- MyFitnessPal Privacy Policy, <https://www.myfitnesspal.com/privacy-policy> (last visited 10 March 2023)
- MyFitnessPal, Sign Up: <https://www.myfitnesspal.com/account/create> (last visited 10 March 2023).
- NBC News, Hackers are leaking children’s data — and there’s little parents can do, 10 September 2021, by Kevin Collier: <https://www.nbcnews.com/tech/security/hackers-are-leaking-childrens-data-s-little-parents-can-rcna1926> (last visited 10 March 2023).
- Pew Research Center, Children’s engagement with digital devices, screen time: <https://www.pewresearch.org/internet/2020/07/28/childrens-engagement-with-digital-devices-screen-time/> (last visited 10 March 2023).

- Pew Research Center, Connection, Creativity and Drama: Teen Life on Social Media in 2022 (16 November 2022)
<https://www.pewresearch.org/internet/2022/11/16/connection-creativity-and-drama-teen-life-on-social-media-in-2022/> (last visited 10 March 2023).
- Pew Research Center, Parenting Children in the Age of Screens: Parents' attitudes – and experiences – related to digital technology (28 July 2020)
<https://www.pewresearch.org/internet/2020/07/28/parents-attitudes-and-experiences-related-to-digital-technology/> (last visited 10 March 2023).
- Pew Research Center, Teens' views about social media: In their own words: Teens explain what they think social media companies do with their data (16 November 2022)
<https://www.pewresearch.org/internet/2022/11/16/2-teens-views-about-social-media/> (last visited 10 March 2023).
- Privacy International, Five Eyes, <https://privacyinternational.org/learn/five-eyes> (last visited 28 February 2023).
- Rachel Sandler: CDC Will Collect Personal Data On Vaccine Recipients, Raising Privacy Concerns, Forbes, 8 December 2020,
<https://www.forbes.com/sites/rachelsandler/2020/12/08/cdc-will-collect-personal-data-on-vaccine-recipients-raising-privacy-concerns/?sh=2ac8021d50ec> (last visited 10 March 2023).
- Spiegel International: German Intelligence Used NSA Spy Program, 20 July 2013,
<https://www.spiegel.de/international/germany/german-intelligence-agencies-used-nsa-spying-program-a-912173.html> (last visited 10 March 2023).
- Spotify Privacy Policy: Transfer to other countries
<https://www.spotify.com/us/legal/privacy-policy/#7-transfer-to-other-countries> (last visited 10 March 2023).
- Statista, Global number of child nudity and sexual exploitation-related content items removed by Facebook from 3rd quarter 2018 to 2nd quarter 2022 (in millions),
<https://www.statista.com/statistics/1013776/facebook-child-exploitation-removal-quarter/> (last visited 10 March 2023).
- Statista: Most popular social networks worldwide as of January 2022, ranked by number of monthly active users (in millions),
<https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/> (last visited 10 March 2023).

- The Guardian, Boy, 12, Steals Credit Card and Goes on Bali Holiday after Fight with Mother (23 April 2018): <https://www.theguardian.com/australia-news/2018/apr/23/boy-12-steals-credit-card-and-goes-on-bali-holiday-after-fight-with-mother> (last visited 10 March 2023).
- The Guardian, Fake fingerprints can imitate real ones in biometric systems – research, 15 November 2018: <https://www.theguardian.com/technology/2018/nov/15/fake-fingerprints-can-imitate-real-fingerprints-in-biometric-systems-research> (last visited 10 March 2023).
- The Guardian: Couple who screamed at their kids in YouTube 'prank' sentenced to probation (12 September 2017) <https://www.theguardian.com/us-news/2017/sep/12/youtube-parents-children-heather-mike-martin> (last visited 10 March 2023).
- The Guardian: US and UK struck secret deal to allow NSA to 'unmask' Britons' personal data, 20 November 2013, <https://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data> (last visited 10 March 2023).
- The New York Times, Alan F. Westin, Who Transformed Privacy Debate Before the Web Era, Dies at 83 (22 February 2013) <https://www.nytimes.com/2013/02/23/us/alan-f-westin-scholar-who-defined-right-to-privacy-dies-at-83.html> (last visited 7 January 2023).
- The Wall Street Journal, Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show (14 September 2021) https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739?mod=hp_lead_pos7 (last visited 10 March 2023).
- The Wall Street Journal, Julie Jargon, How 13 Became the Internet's Age of Adulthood? (18 June 2019): <https://www.wsj.com/articles/how-13-became-the-internets-age-of-adulthood-11560850201> (last visited 10 March 2023).
- Today: Have a social media account for your baby? 40 percent of millennial moms do (18 October 2014) <https://www.today.com/parents/have-social-media-account-your-baby-40-percent-millennial-moms-%201D80224937> (last visited 10 March 2023).
- Twitter, BlogHer: “So I Posted Photos of My Kid Online and This is Where They Ended Up <http://ow.ly/2uSjRn>” (14 February 2013) <https://twitter.com/blogher/status/302079107901046784> (last visited 10 March 2023).

- Ügyfélkapu: <https://ugyfelkapu.gov.hu/> (last visited 10 March 2023).
- UNICEF, More than 175,000 children go online for the first time every day, tapping into great opportunities, but facing grave risks (6 February 2018), <https://www.unicef.org/press-releases/more-175000-children-go-online-first-time-every-day-tapping-great-opportunities> (last visited 23 January 2023).
- United Nations, Children’s right to privacy in the digital age must be improved (15 July 2021) <https://www.ohchr.org/en/stories/2021/07/childrens-right-privacy-digital-age-must-be-improved> (last visited 23 January 2023).
- United Nations, Office of the United Nations High Commissioner for Human Rights (OHCHR): Children’s right to privacy in the digital age must be improved (15 July 2021) <https://www.ohchr.org/en/stories/2021/07/childrens-right-privacy-digital-age-must-be-improved> (last visited 10 March 2023).
- UpcoMinds, AgeCheck, JusProg, Lisal Expert, Revealing Reality, AGEify, Aston University, London School of Economics and Political Science, Leiden University, Digie, AVPA, John Carr. <https://euconsent.eu/partners/> (last visited 21 January 2023).
- Vodafone Privacy and Cookie Policy: International data transfer <https://www.vodafone.com/cookie-policies> (last visited 10 March 2023).
- Vodafone, Child rights and online safety: Privacy and Product Safety <https://www.vodafone.com/sustainable-business/operating-responsibly/child-rights-and-online-safety> (last visited 10 March 2023).
- YouTube help, Manage privacy settings: [Understanding the basics of privacy on YouTube apps](https://support.google.com/youtube/answer/10364219?hl=en#:~:text=YouTube%20does%20not%20sell%20your,results%2C%20and%20serving%20relevant%20ads) <https://support.google.com/youtube/answer/10364219?hl=en#:~:text=YouTube%20does%20not%20sell%20your,results%2C%20and%20serving%20relevant%20ads>. (For their privacy policy they direct you to the above-mentioned Google Privacy Policy) (last visited 10 March 2023).
- YouTube Help, YouTube Policies: Child Safety Policy, https://support.google.com/youtube/answer/2801999?hl=en&ref_topic=9282679#zippy=%2Ckorhat%C3%A1ros-tartalom%2Ckiskor%C3%BAakat-megc%C3%A9lz%C3%B3-tartalom%2Ccontent-featuring-minors (last visited 10 March 2023).

- YouTube Kids Privacy Notice: Information we share
<https://kids.youtube.com/t/privacynotice> (last visited 10 March 2023).
- YouTube Kids: An application specially designed for children
<https://www.youtube.com/kids/> (last visited 10 March 2023).
- YouTube, Simply Allie Channel: Night Time Routine of a Mom 2021 // Mom Of 3 // Preschooler, Toddler and Infant, <https://www.youtube.com/watch?v=Dx7Ty0Yg2-k> (last visited 10 March 2023).
- YouTube, Storyhive Channel: Yoga for Kids!,
<https://www.youtube.com/watch?v=X655B4ISakg> (last visited 10 March 2023).
- YouTube, Terms of Service, General Terms and Conditions: Who can use the service?, Age requirements <https://kids.youtube.com/t/terms> (last visited 10 March 2023).