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

Doctoral (Ph.D.) Dissertation

Aslı Alkış Tümtürk

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

University of Szeged
Faculty of Law and Political Sciences
Doctoral School

Szeged
2023

Table of Contents

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
DPA	Data Protection Authority
DPF	Data Privacy Framework
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
EPRS	European Parliamentary Research Service
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
ITA	International Trade Administration
ML	Machine Learning
NAIH	Nemzeti Adatvédelmi és Információszabadság Hatóság (Hungarian Data Protection Authority)
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, Charts and Schemas

Acknowledgement

I would like to express my gratitude to Tempus Public Foundation for their generous sponsorship of my doctoral studies, which has afforded me a remarkable opportunity. I also express my sincere appreciation to the University of Szeged, namely the Faculty of Law and Political Science, as well as our Institute of Comparative Law, for graciously hosting me during my studies.

Additionally, I would like to express my sincere gratitude to my supervisors, Dr. Szilvia Váradi Dr. Kertészné and Dr. Zsolt Nagy, for their unwavering support and valuable input during my academic journey. This thesis would not have been achievable without the precious input and recommendations they provided.

Besides, I would like to express my gratitude towards Prof. Dr. Attila Badó, the director of the Institute of Comparative Law, for his kind encouragement, guidance and fatherly attitude throughout my Ph.D. studies. I owe my ability to embark on this Ph.D. journey to his inestimable support.

Furthermore, I express my sincere appreciation to my respected reviewers, Dr. Julien Rossi and Dr. Dániel Eszteri, for their precious contributions in terms of knowledge and insights, which have greatly enhanced the quality and readiness of my doctoral thesis. The thesis saw significant improvement as a result of their generous contributions.

Moreover, I would like to express my gratitude towards my beloved family. Without the spiritual and material support of my dear late father, may he rest in peace, I would not have had the opportunity to pursue my education abroad. I am very grateful for the constant and unconditional love and support provided by my beloved mother. Regrettably, the confines of this restricted area prevent me from adequately conveying the depth of my appreciation for them. I am also grateful to my brother, who was always there for me when I lost motivation throughout the most difficult stages of my Ph.D. studies. I express my gratitude for the presence of my husband who exhibits exceptional qualities of help, compassion, and empathy. His continuous affection, inspiration and support were invaluable in navigating the challenging phases encountered throughout the process of researching and composing this Ph.D. thesis. During my most challenging moments, they consistently showed unwavering faith in my capabilities. İyi ki varsınız, canım ailem.

I express my gratitude towards my dear friends who have always provided me with encouragement through times of adversity and have also been there to celebrate my accomplishments.

Ultimately, I feel honoured and delighted to have completed my thesis when celebrating the centenary of the Turkish Republic. I greatly appreciate Mustafa Kemal Atatürk, the visionary behind the establishment of the Turkish Republic, to whom I may owe my independence and career as a Turkish woman. During my research, Atatürk's resolute commitment to women's rights, education, and the elevation of science above personal beliefs has served as a significant guidance. While being satisfied with my academic achievements, I am motivated to consistently follow Atatürk's heritage by embodying the principles of science, logic, and progress. I am enthusiastically looking forward to making further efforts that will help create a brighter future.

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 29 September 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 29 September 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 29 September 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.

The contemporary culture exhibits a pervasive reliance on data, which compels individuals to provide personal data in order to get 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 and most likely credit/debit card information to pay for the service if it is not free) 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 29 September 2023).
[11] Bart Custers, Alan M. Sears, Francien Dechesne, Ilina 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 29 September 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 29 September 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 will thus 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 children[20] 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[22], over protecting vulnerable data subjects who may not contribute as much to the Digital Single Market economically.[23] 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.[24]

The second issue identified is the limited number of academics who exhibit interest in the online activities of children. Consequently, there exists a limited amount of academic literature pertaining to this subject matter. One of the obstacles encountered throughout the research for our thesis was the scarcity of scholarly material available. However, we successfully addressed this challenge by carefully picking research questions that are in accordance with the existing sources and using a multidisciplinary approach. The latter was achieved by including case studies from civil law and doing comparative analyses to explore specific concerns within different legal disciplines. Furthermore, our statements have been supported by sociological sources including surveys and studies. Therefore, it is our contention that this doctoral thesis has the potential to provide a unique and advantageous contribution to the realm of academia and the body of knowledge within the field.

---

[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 29 September 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 29 September 2023).

[22] 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".
GDPR, Article 4(4).

[23] 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.

[24] 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 29 September 2023).

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.[25] This was a milestone factor that prompted us to conduct extensive study on this issue.

The fourth 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 impose any restrictions with respect to parental sharing.

The difference between the legal text and its application in practice is the fifth problem we have identified. Because, for example, *"child"* is defined as *"an individual under the of 13"* under COPPA,[26] 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.[27] 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.

The General Data Protection Regulation (GDPR) of the European Union[28] and the Children's Online Privacy Protection Act (COPPA) of the US[29] took vital measures since, rather than disregarding the internet presence of children, they created provisions mentioning them.[30] However, the last and most significant issue that will be addressed in this thesis is the

[25] YouTube, Thesomebodytoknow channel: My story: Struggling, bullying, suicide, self-harm, available at: https://www.youtube.com/watch?v=vOHXGNx-E7E (29 September 2023).
[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, 312.2 "Child".
[27] 16 CFR 312.2 "Web site or online service directed to children".
[28] 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.
[29] 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.
[30] 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

overreliance on parental consent and responsibility under both legislations. In situations when parents lack awareness regarding the potential hazards and repercussions associated with their children's online activities, depending only on parental accountability may exacerbate the well-being concerns regarding children.

Nonetheless, it is possible that the final three problems listed have not yet become readily apparent. 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 legal 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 historical background of the GDPR Article 8 and the COPPA involving the recent history of transatlantic data transfers, 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 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 the COPPA hold parents/legal guardians[31] accountable for their children's online actions and require parental consent for sharing children's personal data online. Additionally, they also implement a similar age of digital

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.

[31] GDPR employs the phrase "the holder of parental responsibility over the child." In this study, the word "parent" will be employed henceforth, as it represents the usual scenario. Nevertheless, it is important to note that any of these terms might be substituted with the phrase "legal guardians or holders of parental responsibility."

consent for children.[32] 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.

The primary objective of this thesis is to highlight the importance of protecting children's online data and privacy. Additionally, it aims to examine the potential limitations associated with relying heavily on parental consent for protecting online data and the privacy of children. We aim to make a valuable contribution to the existing body of literature by addressing this significant and broad research question.

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 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, data controllers (particularly online service providers in the context of our thesis), and even schools.

[32] 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.

1.3 Research Design

We will begin this thesis by analysing the background of the COPPA 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. Besides, in Chapter 2.1, 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.

The robust economic cooperation of the EU and the US may also justify the comparison of their relevant legislation in this thesis. Subchapter 2.2 will examine the history of transatlantic transfer of data because facilitating data sharing between these two jurisdictions is vital to their economic collaboration. The GDPR makes it abundantly obvious that the transfer of data between data controllers in the EU countries and data controllers in third countries or international organisations is necessary for the expansion of international trade and cooperation.[33]

The transfer of data to third countries and international organisations should be conducted in strict adherence to the provisions outlined in this Regulation. The most optimal course of action entails obtaining an adequacy decision granted by the European Commission. Subchapter 2.2.1 aims to present a comprehensive analysis of the EU-US free flow of personal data agreements (on those for which adequacy decisions have been adopted by the European Commission), namely Safe Harbour, Privacy Shield, and the EU-US Data Privacy Framework, from a historical standpoint.

Since there are no specific requirements for the transfer of children's data, we will not mention any child-related matters in Subchapter 2.2. However, we will examine briefly in Chapter 5 whether children should have control over the transfer of their personal data to third countries prior to the age of digital consent.

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.[34] Consent, as defined by the GDPR as the freely expressed, precise, informed, and clear wishes of the

[33] GDPR, Article 1 and Recital 101.

[34] 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.

data subjects, indicates consent to the use of their personal data.[35] 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.[36] 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 (from 13 to 16 depending on the Member States).[37] Similarly, according to the COPPA, the process of obtaining parental consent involves employing reasonable efforts, taking into account the technological resources at hand, to inform parents about the collecting, use, and/or sharing of their children's personal information. It is essential to obtain parental consent before gathering, utilising, and/or disclosing personal information of children under the age of thirteen.[38]

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?

---

[35] GDPR, Article 4(11).
[36] Marie-Anne Frison-Roche: Remarques sur la distinction de la volonté et du consentement en droit des contrats, RTD civ (1995), 574.
[37] GDPR, Article 8(1).
[38] 16 CFR 312.2 “Obtaining verifiable consent”.

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 Online[39] and the Pew Research Center in the US.[40]

By answering these questions, we will determine whether the threshold ages for parental consent are implemented properly in real-life cases or if there is a gap between real-life 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 the GDPR. The parents of a child, however, cannot be expected to keep a close eye on them all the time. Therefore, there are internet technologies that make it easier to keep an eye on children while their parents are not available.[41] 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

[39] 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.

[40] 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 29 September 2023).

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

policy.[42] 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.[43] 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 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.[44] We intend to finalise Chapter 3.4 with an analysis of the European Commission's proposal for European Digital Identities (eIDs).[45] Using the eIDs for age verification purposes might raise concerns about privacy and security. Thus, 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.

---

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

[43] 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.

[44] euCONSENT, euCONSENT's first large scale pilot (18 March 2022) https://euconsent.eu/euconsents-first-large-scale-pilot/ (last visited 29 September 2023).

[45] 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).

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)[46] 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:

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.[47] Moreover, data controllers specify the aims and

[46] 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.

[47] 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."

means of processing personal data, and their most important task is to comply with the Regulation's norms and principles.[48] 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.[49] They have additional obligations originating from the concept of privacy by design and by default[50], as well as additional requirements connected to cooperating with the supervisory authority, particularly in the case of data breaches.[51] 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.[52]

Additionally, we will discuss the transfer of personal data to third countries, which is another important responsibility of data controllers and one of the most important aspects of the global digital economy. We will also debate the existing situation of the transfer of EU children's data to third countries. 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 within the EU 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 briefly draw attention to this issue.

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.[53] Other obligations include protecting the confidentiality, security, and accuracy of the information collected from children.[54]

[48] GDPR, Article 24(1).
[49] GDPR, Article 8(2).
[50] GDPR, Article 25.
[51] GDPR, Article 31 and Article 33.
[52] GDPR, Article 35.
[53] 16 CFR 312.4(a)(b), 16 CFR 312.5(a)(2), 16 CFR 312.6(a) and 16 CFR 312.3(c).
[54] 16 CFR 312.8.

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 will analyse the scenarios in which data controllers may actively involve children and offer them with more control over their personal data.

In Chapter 6, 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. In the recent 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. Since individuals now have the opportunity to share their material online with millions of random strangers, everyone has the potential to become celebrities or, as the term has evolved, influencers.[55] 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.[56] Nevertheless, the frameworks do not impose restrictions on parents regarding the disclosure of their children's personal information on the Internet. This chapter addresses our seventh 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?

To answer the seventh 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 attempt to determine whether the prohibited content specified in the data protection and privacy policies of these social media sites as a consequence of the GDPR and the COPPA requirements, as well as whether these social media sites' policies are reflected in practice.

---

[55] 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.

[56] Instagram Help Center, How to Report Things, Report a child under 13 on Instagram, https://help.instagram.com/2922067214679225/?helpref=hc_fnav (last visited 29 September 2023); YouTube, Terms of Service, General Terms and Conditions: Who can use the service?, Age requirements https://kids.youtube.com/t/terms (last visited 29 September 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 29 September 2023).

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.[57]

In addition to privacy concerns, the sharing of personal data of children on the Internet poses other hazards, including but not limited to cyberbullying, identity theft, exposure to child pornography, discrimination and labelling, and the potential for kidnapping.[58] In conjunction with the various scenarios, these potential risks will be examined in detail. Instead of completely prohibiting the sharing of child-related information, we will explore the optimal approach and restrictions that can be implemented.

Finally, in this chapter, we will also answer the overarching question of this thesis:

Does an excessive reliance on parental authorisation and consent effectively protect the personal data and privacy of children?

In order to address this inquiry, we will investigate the level of comprehension among children and parents about the significance of privacy and data protection for children. This investigation will be enhanced by the utilisation of studies and surveys, together with the analysis of replies to the previously stated research questions. We will ascertain the degree to which they are aware of the potential hazards associated with relinquishing control over children's personal data. It is important to consider the insights gained from the preceding chapters in order to address the extent of parental awareness of the privacy and data protection rights of children, together with their ability to effectively exercise these rights. Additionally, it is crucial to examine the knowledge of parents about the responsibilities of data controllers in relation to safeguarding these rights. Ultimately, we will address the mentioned overarching question. In the event of an unfavourable outcome, we will also put forward prompt and enduring measures to attain optimal practices for protecting the personal data and privacy of children.

---

[57] 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 29 September 2023).

[58] 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.

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"[59], whereas the COPPA defines "operator" as the one "who collects or maintains personal information"[60]. Another difference between the COPPA and the GDPR terminology is that the former refers to any identifiable information related to an individual as "personal information,"[61] while the latter refers to the same as "personal data".[62] 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.[63]

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 literature, and social media examples in order to better comprehend the implementation of legal text into practise.[64]

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

[59] GDPR, Article 4(7).
[60] 16 CFR 312.2 "Operator".
[61] 16 CFR 312.2 "Personal information".
[62] GDPR, Article 4(1).
[63] John C. Reitz: How to Do Comparative Law, American Journal of Comparative Law 46, no. 4 (Fall 1998), 621.
[64] John C. Reitz: How to Do Comparative Law, American Journal of Comparative Law 46, no. 4 (Fall 1998), 626-631.

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.[65]

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."[66] 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.[67] 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,[68] while Legrand contends that the application of a legal transplant is impossible due to the historical and cultural diversity of each society and legal system.[69] 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:

---

[65] The right to be forgotten of children will be analysed in depth in the Chapter 4 and Chapter 7.
[66] For more information about analytical method see: Mark Van Hoecke: Methodology of comparative legal research, Law and method (2015), 13-16.
[67] Alan Watson: Introduction to Legal Transplants In Legal Transplants: An Approach to Comparative Law (1974), 21.
[68] Alan Watson: Introduction to Legal Transplants In Legal Transplants: An Approach to Comparative Law (1974), 21.
[69] Pierre Legrand: The impossibility of 'legal transplants, Maastricht journal of European and comparative law 4, no. 2 (1997), 111.

> "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."[70]

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. Furthermore, this chapter examines the significance of transatlantic data transfers and provides a historical analysis of the agreements pertaining to the free movement of data that have been established between the EU and the US. 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 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 by parents and children, in order to determine how legal texts manifest themselves in online practise.

[70] 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.

2. The historical context and evolution of the current standards, definitions, data transfers 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*."[71]

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.[72] 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.[73] 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.[74]

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

[71] Samuel Dash: The intruders: Unreasonable searches and seizures from King John to John Ashcroft, Rutgers University Press (2004), 9.
[72] 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 29 September 2023).
[73] Chelsea Wald: The secret history of ancient toilets, Nature 533, no. 7604 (2016), 457.
[74] 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.[75]

In 1890, the "most influential law review article of all"[76] titled "Right to Privacy",[77] 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 […]"[78]

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.[79] Nonetheless, it is widely accepted that Warren's dislike of Boston's

---

[75] 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 29 September 2023).

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

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

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

[79] "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-

print media in general and his perception of its invasion of social privacy inspired this article 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.[80]

The introduction of personal computers during the 1970s[81] prompted inquiries into the adequacy of the right to privacy in protecting private life.[82] Consequently, advancements in technology led to the emergence of a new right known as the right to data protection, which also encompasses the protection of private life.[83]

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."[84] *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."[85] Moreover, *Marc Rotenberg*, the executive director of the Electronic Privacy Information Centre in Washington, remarked, "This concept[86] became the cornerstone of our modern right to privacy."[87] Hence, Privacy and Freedom became the

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.

[80] 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.

[81] Paul Ceruzzi: From scientific instrument to everyday appliance: The emergence of personal computers, 1970–77, History and Technology: An International Journal 13, no. 1 (1996), 1-31.

[82] 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 28 September 2023).

[83] 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 28 September 2023).

[84] Alan F. Westin: Privacy and Freedom, Atheneum New York (1967), 1-487.

[85] 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 29 September 2023).

[86] Marc Rotenberg uses "this concept" to refer to Alan Westin's definition of privacy.

[87] 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 29 September 2023).

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.[88]

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.[89] Hence, a comparative analysis of these two jurisdictions on each side of the Atlantic will be conducted in this thesis, with a focus on their respective historical developments as a starting point for enhanced clarity and understanding.

Besides this, it is crucial to provide more clarification on another reason that justifies a comparison between the EU and the US, which is their robust economic partnership. The facilitation of data sharing between these two jurisdictions is widely seen as a pivotal factor in promoting and strengthening their collaborative endeavours. Therefore, the subsequent subsection, Subchapter 2.2, will delve into the analysis of the historical context related to transatlantic data transfers.

2.1 The historical background of the GDPR Article 8 and the COPPA

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.[90] 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."[91]

[88] 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.
[89] Máté Dániel Szabó: Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival, Információs Társadalom: társadalomtudományi folyóirat 5, no. 2 (2005), 44.
[90] 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.
[91] N.Y. Civ. Rights Law, §§ 50 (McKinney 1909).

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 […]"[92] 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.[93]

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.[94] 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.[95]

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

[92] 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."

[93] Griswold v. State of Connecticut, 381 U.S. 479 (1965) 484-86. https://tile.loc.gov/storage-services/service/ll/usrep/usrep381/usrep381479/usrep381479.pdf (last visited 29 September 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.

[94] 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.

[95] 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.

Accountability Act (HIPPA),[96] the Family Educational Rights and Privacy Act (FERPA),[97] Telephone Consumer Protection Act of 1991 (TCPA)[98] and most significantly for our research, the Children's Online Privacy and Protection Act (COPPA)[99].[100]

In May 1996, a consumer watchdog group known as the Centre for Media Education filed a complaint with the FTC regarding the KidsCom.com (KidsCom) conduct because the KidsCom acquired children's information without correctly disclosing the purpose of collection. Moreover, KidsCom sold the collected personal information such as name, email address, home address or phone numbers of children to third parties without giving the adequate notice to the parents and providing them with the opportunity to control over their children's personal information.[101]

In 1997, the FTC investigated and published its findings in a letter that involves several principles. They suggested that those principles should apply generally to the collection of personal information from children online. In this letter, the FTC staff argued that KidsCom's information gathering practises violated Section 5 of the Federal Trade Commission Act[102] due to its practices were deceptive or unfair. Furthermore, this letter states that parental approval should be obtained before disclosing children's information to any third party.[103]

For the first time, the FTC announced its criteria for collecting personal information from children in this letter.[104] Following these developments, the FTC delivered its Privacy

[96] Health Insurance Portability and Accountability Act. Pub. L. No. 104-191, 110 Stat.1936 (1996).
[97] Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (1974).
[98] Telephone Consumer Protection Act of 1991, 47 U.S. Code § 227 (1991).
[99] 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.
[100] 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.
[101] Joshua Warmund: Can COPPA Work - An Analysis of the Parental Consent Measures in the Children's Online Privacy Protection Act," Fordham Intellectual Property, Media &Entertainment Law Journal 11, no. 1 (2000), 192-193.
[102] 15 U.S.C. § 45(a)(1) (1994): "Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."
[103] Federal Trade Commission, FTC Staff Sets Forth Principles For Online Information Collection From Children, July 1997, https://www.ftc.gov/news-events/news/press-releases/1997/07/ftc-staff-sets-forth-principles-online-information-collection-children (last visited 29 September 2023).
[104] Joshua Warmund: Can COPPA Work - An Analysis of the Parental Consent Measures in the Children's Online Privacy Protection Act," Fordham Intellectual Property, Media &Entertainment Law Journal 11, no. 1 (2000), 193.

Online Report to Congress in 1998 concerning the online collection of children's personal information.[105]

In light of the survey results in this report, the FTC informed Congress of the necessity for parental consent while collecting children's personal information. This report suggests that consent from parents should be obtained for the collecting of personal information from children aged 12 and younger due to their vulnerability to overreaching by the marketers.[106] In reaction to this report, Congress established the COPPA[107], the first federal law protecting children's online privacy, in 1998.[108] Recognising the analysis of the report, Congress decided that the act's provisions would only apply to children under the age of 13.[109]

In the meantime, 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,[110] 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.[111]

Yet, before delving into those international treaties, we shall note the world's first data protection law, the *Hessisches Datenschutzgesetz* of 1970.[112] This law was enacted by the German federal state of Hesse in order to protect personal information stored in public

[105] Federal Trade Commission, Privacy Online: A report to Congress, June 1998, https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf (last visited 29 September 2023).
[106] Federal Trade Commission, Privacy Online: A report to Congress, June 1998, 42 https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf (last visited 29 September 2023).
[107] 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.
[108] Joshua Warmund: Can COPPA Work - An Analysis of the Parental Consent Measures in the Children's Online Privacy Protection Act," Fordham Intellectual Property, Media &Entertainment Law Journal 11, no. 1 (2000), 194.
[109] Federal Trade Commission, Complying with COPPA: Frequently Asked Questions, Q9. 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#A.%20General%20Questions (last visited 29 September 2023).
[110] 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 29 September 2023).
[111] 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.
(*) 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.
[112] Hessisches Datenschutzgesetz of 7 October 1970, Gesetz- und Verordnungsblatt für das Land Hessen Teil I, No. 41, 625 of 12 October 1970.

bodies' files. However, the right to private and family life provided by Article 8 of the ECHR was not included in the *Hessisches Datenschutzgesetz.*[113]

According to Article 8 of the ECHR, "Everyone has the right to respect for his private and family life, his home and his correspondence."[114] 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".[115]

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.[116]

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.[117] 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,[118] wiretapping,[119] sexual life,[120] profession or domicile,[121] and the protection against the environmental nuisances (e.g., noise nuisance).[122] 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.[123]

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

[113] Tobias Naef: The Global Reach of the Right to Data Protection. In: Data Protection without Data Protectionism. European Yearbook of International Economic Law, vol 28. Springer (2023), 21.
[114] 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 29 September 2023).
[115] Charter of Fundamental Rights of The European Union, OJ C 364, 18.12.2000, pp. 1-22, Article 7.
[116] Raphael Gellert and Serge Gutwirth: The legal construction of privacy and data protection, Computer Law & Security Review 29, no. 5 (2013), 524.
[117] 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"[...]"
[118] Leander v. Sweden judgment of 26 March 1987, no. 9248/81 para. 46-48.
[119] Klass and Others v. Germany judgment on 6 September 1978, no. 5029/71 para. 41.
[120] Dudgeon v. the United Kingdom judgment on 22 October 1981, no. 7525/76 para. 40-41.
[121] Niemietz v. Germany judgment on 16 December 1992, no. 13710/88 par. 28-33.
[122] Powell and Rayner v. the United Kingdom judgment of 21 February 1990, no. 9310/81, para. 41.
[123] 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 29 September 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.

Article 8 of the European Convention on Human Rights.[124] Besides, according to Article 52 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."[125]

As technology improved and the impacts of the digitisation became abundantly apparent, the EU acknowledged the need for data protection.[126] 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. 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.[127] 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.[128]

---

[124] 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 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-I). Those activities can include participation in a contract award procedure."

[125] CFR, Article 52(3).

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

[127] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136, Adopted on 20th June 2007, p. 1-26.

[128] 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."

Besides the right to respect for private and family life (Article 7)[129], the CFR recognises the right to the protection of personal data (Article 8)[130] 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 provides that individuals have the right to access and rectify their personal data.[131] 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,[132] shall be interpreted as a continuation of pre-existing EU data protection legislation.[133]

Initially, ECtHR case law issued data protection within Article 8 of the ECHR,[134] 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.[135]

With 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

---

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.

[129] CFR, Article 7.

[130] CFR, Article 8.

[131] CFR, Article 8(2).

[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.

[133] 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 29 September 2023).

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

[135] 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 29 September 2023).

force dates were not consistent.[136] Besides, the Member States' data protection approach was not uniformed. In terms of data protection, some Member States had very strict legislation while others had almost none at all.[137]

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 1990 to address the need for data protection rules to be harmonised across Member States in order to create a fully united market.[138] However, due to the poor language and numerous inconsistencies in this first draft, the EC published an amended proposal to replace it in 1992.[139] Afterwards, in October 1995, the European Union's Directive 95/46/EC was enacted[140] with the stated goal of harmonising data protection legislation at the national level within the European Union.[141]

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.[142] In this regard, the European Court

---

[136] 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 29 September 2023).

[137] "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.

[138] European Commission, Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, COM(90) 314 final – SYN 287, OJ C 277/3, 5.11.1990, pp. 3-12.

[139] 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), 309.

[140] "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).

[141] 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."

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

of Justice has concluded that directives do not have a direct effect on horizontal relations, even though the state can be held liable for failing to apply a rule that is clear precise, unconditional, and leaves no room for the Member State to exercise discretion.[143] 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's[144] 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.[145]

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 the EU".[146] 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.[147]

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

---

[143] "The Commission recalls the three tests which must be satisfied before a provision of a directive may have direct effect: (i) a clear and precise obligation, (ii) not accompanied by conditions, (iii) with no margin of discretion left to the Member State." Case 148/78, Pubblico Ministero v Ratti [1979] ECR 1629, EU:C:1979:110, p. 1636.
"[…] 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.
[144] TFEU, Article 16.
[145] TFEU, General Part, Context, para. 13-16.
[146] European Data Protection Supervisor (EDPS), 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 29 September 2023).
[147] Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, p. 47–390, Article 288.

and established in the EU, regardless of whether the processing occurs in the EU or not.[148] In addition, it applies if data subjects are in one of the Member States in the EU 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.[149] 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 portability is a new right introduced by the GDPR.[150] Besides, the right to be forgotten, initially articulated by the CJEU,[151] is incorporated into the GDPR as a separate data subject right.[152] 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".[153]

On one hand, the core concept of consent is quite similar to that of Directive 95/46/EC,[154] and it remains one of the lawful bases for processing personal data.[155] 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).[156] 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.[157]

---

[148] GDPR, Article 3(1).
[149] GDPR, Article 3(2).
[150] GDPR, Article 20.
[151] 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.
[152] GDPR, Article 17 and Recital 66.
[153] GDPR, Article 4(11).
[154] 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".
[155] GDPR, Article 6(1)(a) and Directive 95/46/EC, Article 7(a).
[156] GDPR, Article 7 and Recitals 32, 33, 42, 43.
[157] Article 29 Working Party, Guidelines on consent under Regulation 2016/679 17/EN WP 259 rev.01, Adopted on 28 November 2017, Last Revised and Adopted on 10 April 2018, 1-31, 4-5.

Furthermore, fines for the GDPR violations increased to a maximum of €20 million, or 4% of the company's global turnover of the preceding financial year.[158] 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.[159] 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 breach of the GDPR.[160]

There were no particular requirements for the protection of children's personal data in the 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.[161] 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.[162] 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.[163] 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 or 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.[164]

---

[158] GDPR, Article 83(6).
[159] GDPR, Article 82(1).
[160] Manu J. Sebastian: The European Union's General Date Protection Regulation: How Will It Affect Non-EU Enterprises, Syracuse Journal of Science and Technology Law 31 (2014-2015), 222-223.
[161] GDPR, Article 8.
[162] 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.
[163] "[...] 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 29 September 2023).
[164] 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."

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:[165]

> "(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 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."[166]

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.[167] It is unclear, however, how much work would be considered reasonable and how this should be proven and confirmed.[168]

---

[165] 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.
[166] 16 CFR COPPA 312.5(b)(2).
[167] GDPR, Article 8(2).
[168] 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.

The above-mentioned COPPA procedures do not have to be directly transplanted to the GDPR as they are because they may become ineffective over time as technology advances. However, it may be possible to create a rule as a general norm that is technology neutral (as in Article 32 of the GDPR[169]). However, it may still include certain instances, such as the measures stated in Article 32 in relation to data security requirements.[170]

We may draft a sample rule like this:

> Taking into consideration the state of the art, the controller and the processor should adopt adequate technologies to guarantee the consent is given or authorised by the holder of parental responsibility over the child, including inter alia as appropriate:
>
> (a) conducting a video conference with the parents to verify their official IDs
>
> (b) confirming the electronic identification (eID) of the parents compared with the eID of the children
>
> (c) Where the processing is unlikely to pose a high risk (e.g., subscribing to a newsletter), consent can also be given through email.[171]

The European Commission's eID solution for children will be examined in Chapter 3.4, which deals with online age verification methods. However, we should emphasise briefly that it can also be a solution for parental consent verification. Given the eID solution is a collection of services (for example, accessing electronic medical data) provided by the European Commission to enable mutual recognition across borders[172], it may also be feasible to utilise this solution to verify parental responsibility in a secure manner.

The European Commission aims that by 2030, the eID solution will be available across the EU, including all key public services and medical records, and that all citizens will have access to their secure eIDs, giving them control over their shared personal data and identity

---

[169] GDPR, Article 32.

[170] GDPR, Article 32: "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."

[171] The author developed this sample rule in light of the suggestions of her PhD thesis reviewer, Dr. Dániel Eszteri and Dr. Julien Rossi, as well as resembling the requirements of GDPR Articles 8 and 32.

[172] European Commission, eID, What is eID?, https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eID (last visited 29 September 2023).

transactions. It is also intended that 80% of citizens will utilise the solution provided.[173] It would be ideal if the children's eIDs included parental information (such as their names and surnames) so that data controllers could compare and verify accordingly.

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.[174] 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.

2.2 The recent history of transatlantic data transfers

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.[175] 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. The GDPR explicitly states that the transfer of personal data between non-EU countries and EU Member States is crucial for promoting international commerce and cooperation.[176] 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 have consistently taken place.

The EU and the US regard the personal data and data flows differently because of their differing approaches to privacy and data protection.[177] On one hand, personal data is

[173] European Commission, Shaping Europe's digital future, Electronic Identification, https://digital-strategy.ec.europa.eu/en/policies/electronic-identification (last visited 29 September 2023).
[174] 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.
[175] 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 29 September 2023).
[176] GDPR, Recital 101.
[177] 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.

regarded as a commercial commodity in the US[178] and there is a sectoral approach, enacting limited legislation that only applies to specific targets.[179] 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)[180] of Illinois or more general laws such as the California Consumer Privacy Act (CCPA)[181] 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,[182] as required by the GDPR.[183]

The EU, on the other hand, considers privacy and data protection to be fundamental rights and places a high value on them.[184] 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.[185] 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."[186] However, data transfers from the EU 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.[187]

---

[178] 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.
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.
[179] 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.
[180] Biometric Information Privacy Act (BIPA) of 2018, 740 ILL. COMP.STAT. 14/1-99.
[181] California Consumer Privacy Act (CCPA) of 2018, CAL. CIV.CODE §§ 1798.100-1798.199.100.
[182] 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.
[183] GDPR, Article 45(1).
[184] Charter of Fundamental Rights of the European Union, OJ C 326, 26.12.2012, p. 391-407, Article 7-8.
[185] GDPR, Article 1(1) and (2).
[186] GDPR, Recital (101).
[187] GDPR, Article 45.

It should be noted that this chapter will refrain from discussing particular advancements pertaining to children, given the historical advances connected to data transfer cover children's data as well. (During the examination of data controllers' duties under Chapter 5, we will specifically address the topic of children's control on transfer of their data. This includes considerations such as the ability of children to make decisions regarding the termination of data transfers, provided they possess the necessary maturity.)

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,[188] but it lasted until the European Court of Justice (CJEU) invalidated it in 2015 with the Schrems I. case.[189] Following that the Privacy Shield, the Safe Harbour's heir, entered into force in 2016.[190] Likewise, it was invalidated by the CJEU in 2020 with the Schrems II. case[191].

Furthermore, on March 25, 2022, the European Commission and the US announced a new agreement in principle on a joint statement on the Trans-Atlantic Data Privacy Framework.[192] Accordingly, the European Commission decided to adopt its adequacy decision for the EU-US Data Privacy Framework on July 10, 2023.[193] The ruling on adequacy determines that the US provides an adequate level of protection for personal data transferred from the EU to the US companies participating in the EU-US 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 the Schrems cases.

This chapter will examine briefly all previous agreements allowing free data flow from the EU to the self-certified US companies, as well as the present EU-US Data Privacy

---

[188] 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.
[189] Case C-362/14 Maximillian Schrems v Data Protection Commissioner EU:C:2015:650.
[190] 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.
[191] Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems EU:C:2020:559.
[192] 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 29 September 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 29 September 2023).
[193] European Commission, Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, OJ C (2023) 4745, 10.07.2023, 1-64.

Framework[194]. But first, the GDPR's requirements for data transfers to third countries or international organizations will be examined.

Nonetheless, our primary focus will be on transfers based on adequacy decisions, as they appear to be the most reliable option thus far. Indeed, they enable the unrestricted and secured movement of data, provided their implementation is sufficient.

Although data transfers to countries outside the EU and to international organizations were perceived as necessary for the growth of international relations and the economy by the GDPR, they have prompted concerns about the data protection of EU data subjects.[195] Therefore, all provisions in the GDPR's chapter on data transfers should be followed in order to ensure that the degree of protection of natural persons granted by this Regulation is not jeopardized by controllers and processors.[196]

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.[197]

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.[198]

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

[194] European Commission, Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, OJ C (2023) 4745, 10.07.2023, 1-64.
[195] GDPR, Recital (101).
[196] GDPR, Article 44.
[197] GDPR, Article 45(1).
[198] GDPR, Article 45(2)(a).

as assisting data subjects in exercising their data protection rights. The supervisory authority should also cooperate with supervisory authorities in the EU Member States.[199]

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.[200] For example, the European Commission issued the United Kingdom (UK) an adequacy decision after it becomes a third country following Brexit on June 28, 2021[201] especially because the UK has earned their trust owing to its continued adherence to

> "[...] the jurisdiction of the European Court of Human Rights and […] European Convention of Human Rights[202] as well as to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[203], which is the only binding international treaty in the area of data protection".[204]

Given the aforementioned strict requirements, only a few countries have been determined as possessing an adequate level of data protection 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, the US (US companies involved in the EU-US Data Privacy Framework) and Uruguay are among these countries. In the case of Canada and the US, since these adequacy decisions solely apply to commercial organizations and does not extend to the entire Canadian and US jurisdiction, they should be regarded as partial adequacy decisions.[205]

---

[199] GDPR, Article 45(2)(b).
[200] GDPR, Article 45(2)(3).
[201] 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.
[202] 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 29 September 2023).
[203] 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 29 September 2023).
[204] 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 29 September 2023).
[205] 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 29 September 2023).

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),[206] applies higher standards to EU data subjects' personal data than to its own citizens and residents.

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 effective legal remedies are in place.[207] 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.[208]

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. In Chapter 5, we will address these alternative methods of transferring data to third countries whose level of data protection is not essentially equivalent to the EU's level of data protection, as well as the data controllers' related obligations.

2.2.1 Safe Harbour, Privacy Shield and the EU-US Data Privacy Framework

This subchapter will begin by examining the Safe Harbour agreement, which facilitated the free transfer of personal data from the EU to the US for companies that self-certified their compliance. Subsequently, we will explore the invalidation of the Safe Harbour agreement by the CJEU. Afterwards, we will analyse the Privacy Shield agreement, which was introduced as a replacement for Safe Harbour, and its invalidation by the CJEU. Finally, we will examine the newly implemented EU-US Data Privacy Framework. We will discuss if this agreement would establish an adequate level of data protection for self-certified companies or whether it is susceptible to invalidation for comparable grounds as previous agreements.

---

[206] 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 29 September 2023).
[207] GDPR, Article 46(1).
[208] GDPR, Article 46(2)(a-f).

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.[209] 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.[210]

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.[211] 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.[212] Besides, all companies that self-certified their compliance

[209] 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).

[210] 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.

[211] 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."

[212] Safe Harbour, FAQ 6-Self Certification, 15.

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

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

with the Safe Harbour principles, should have made that fact clear in their published privacy policies.[213]

Although the self-certified companies asserted that they complied with the Safe Harbour principles, according to a study conducted by *Chris Connolly*[214] 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.[215] According to the enforcement principle of the Safe Harbour, effective privacy protection must include mechanisms for ensuring compliance with the principles. If a 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.[216]

However, it was discovered that the United States National Security Agency (NSA) gathered 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 such facts regarding the NSA's monitoring programme in 2013.[217] In reaction to the revelations that were provided by Edward Snowden, the privacy advocate *Max Schrems*[218] has lodged a complaint at the Irish Data Protection Commission, that Facebook's Irish subsidiary transfers part or all of the information that Mr. Schrems provided

---

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."

[213] Safe Harbour, FAQ 7-Verification, 16.

[214] Chris Connolly is a Director of Galexia, an independent consultancy specialising in privacy and electronic commerce. For more information about Galexia see: Galexia, http://www.galexia.com.au (last visited 13 September 2023).
Chris Connolly: The US Safe Harbor - Fact or Fiction?, Galexia (2008), 7-8, https://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf (last visited 13 September 2023).

[215] 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 29 September 2023).

[216] Safe Harbour, Annex I Safe Harbour Privacy Principles, Enforcement, 12.

[217] BBC News, Edward Snowden: Leaks that exposed US spy programme, 17 January 2014, https://www.bbc.com/news/world-us-canada-23123964 (last visited 29 September 2023).

[218] Privacy Lawyer, Honorary Chair of noyb, Author and Speaker.
Max Schrems, https://schre.ms/ (last visited 13 September 2023).

to Facebook to servers located in the US, where it is processed. The issue of Mr. Schrems was that the US does not provide an adequate level of protection against the public surveillance of the data that is transferred to that country. However, the Irish Data Protection Commissioner rejected, stating that the Safe Harbour covered the transfers.[219]

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.[220]

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 the Member States from querying whether the framework is compatible with the protection of privacy, fundamental rights, and individual freedoms.[221] Since the abovementioned conditions did not meet the expectations of the former Directive 5/46/EC's adequacy level of data protection, the CJEU declared that the Safe Harbour framework was invalid.[222]

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.[223] 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

[219] 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 Maximillian Schrems v Data Protection Commissioner, 6 October 2015, 1.
[220] Case C-362/14 Judgment of the Court (Grand Chamber) of 6 October 2015 Maximillian Schrems v Data Protection Commissioner ECLI:EU:C:2015:650, para 82 et seq.
[221] 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 Maximillian Schrems v Data Protection Commissioner, 6 October 2015, 2.
[222] Case C-362/14 Judgment of the Court (Grand Chamber) of 6 October 2015 Maximillian Schrems v Data Protection Commissioner ECLI:EU:C:2015:650, para 107/2.
[223] 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.

framework did: notice, data integrity and purpose limitation, choice, security, access, recourse, enforcement and liability, and accountability for onward transfer.[224]

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.[225] 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.[226]

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

[224] Privacy Shield, para 19 et seq.:
"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."
[225] Privacy Shield, Annex II.III.1-16.
[226] GDPR, Article 45(1).

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.[227]

After the judgment 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 US, and he sought to prohibit his data transfer to the US, 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).[228]

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 2010/87[229] and Decision 2016/1250[230] (Privacy Shield).[231]

The Court of Justice ruled on July 16, 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.[232]

---

[227] European Parliamentary Research Service (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 (last visited 29 September 2023).

[228] 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 29 September 2023).

[229] 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.

[230] 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.

[231] 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 29 September 2023).

[232] 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.

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 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.[233]

However, concerns raised regarding the inadequacy of necessity and proportionality of the 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 CJEU ruled in the Schrems II case 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.[234]

In the absence of an adequacy decision or for the companies that have not been participated in the new EU-US data privacy framework, the SCCs and BCRs were the only existing procedures for transferring personal data from the EU to the US for repeated and continuing personal data transfers. The derogations under Article 49 of the GDPR are limited to particular and exceptional transfers.[235]

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 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.[236] As a result, it often takes around two years to obtain approval,

---

https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf (last visited 29 September 2023).

[233] 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, 2-3. https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf (last visited 29 September 2023).

[234] 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, 3. https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf (last visited 29 September 2023).

[235] GDPR, Article 46-49.

[236] 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 29 September 2023).

which makes this process challenging and impractical compared to SCCs, but it remains a viable alternative for large companies with several entities in the EU and other third countries.[237] The official website of the EDPB provides access to the list of BCRs approved by DPAs under the GDPR as well as pre-GDPR prior to May 25, 2018.[238]

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 employed BCRs, adequacy decisions, and derogations altogether.[239] Whereas, according to the same survey, 85% percent of all respondents used SCCs for data transfers.[240]

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.[241] Moreover, EU data controllers should be 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.[242]

Following the Schrems II judgment, 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. In the event that this situation arises, data exporters have the option to use

---

[237] Nigel Cory, Ellysse Dick, and Daniel Castro: The Role and Value of Standard Contractual Clauses in EU-US Digital Trade, Information Technology and Innovation Foundation (2020), 13.
[238] European Data Protection Board, Approved Binding Corporate Rules, https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en?page=1 (last visited 29 September 2023).
[239] Nigel Cory, Ellysse 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 29 September 2023).
[240] Nigel Cory, Ellysse Dick, and Daniel Castro: The Role and Value of Standard Contractual Clauses in EU-US Digital Trade, Information Technology and Innovation Foundation (2020), 4.
[241] 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 29 September 2023).
[242] Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems EU:C:2020:559, para 133.

supplementary measures in order to elevate the level of data protection in the third country to align with the criteria set by the EU. 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.[243]

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)."[244]

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 govern the transferred data and the importer receiving it.[245] 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

[243] 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 29 September 2023).

[244] 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.

[245] 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.

not exhaustive, new supplemental measures would be implemented to keep up with the requirements of future technical and legal developments.[246]

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).[247] 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.[248]

In summary, adequacy decisions present a more reliable, consistent, and easily accessible option in comparison to the use of SCCs. Adequacy decisions, which are particularly advantageous for small and medium-sized enterprises, as they offer a considerably more secure solution compared to the SCCs, given the costly and case-by-case nature of SCCs.[249]

Following a period of uncertainty characterised by the absence of an adequacy decision pertaining to US companies, On October 7, 2022, US President *Joe Biden*[250] signed an Executive Order to implement the Transatlantic Data Privacy Framework, which was announced into US legislation in March 2022.[251] On this basis, the European Commission

---

[246] 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.
[247] 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.
[248] 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.
[249] 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.
[250] "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 29 September 2023).
[251] 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-

declared that they will prepare an adequacy decision and initiate its adoption procedure.[252] 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.[253]

The EU-US Data Privacy Framework (DPF) was ultimately implemented on July 10, 2023. The website that facilitates self-certification for companies in the US, also providing access to the DPF List for participants' verification, is currently available.[254] Self-certification requires companies to demonstrate compliance with the EU-US Data Protection Framework (DPF). The International Trade Administration (ITA) revises the list frequently by evaluating annual re-certification applications and may remove companies that do not meet compliance criteria.[255]

The newly introduced framework promised improvements. Surveillance by the US government's intelligence services shall be proportionate and conducted only when necessary for national security and for criminal law enforcement purposes; the Data Protection Review Court shall be established and will review EU complaints in a "two-layer" system for redress; self-certification of companies shall continue with strict obligations; and to ensure the limited surveillance activities, there must be objective and independent oversight mechanisms for intelligence agencies.[256]

At this point, we question the content of the proportionate access. Indeed, Mr. Schrems challenged whether the proportionality is based on the European idea of proportional or the US understanding.[257] Moreover, he asserted that this approach allows the EU and the US to

releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/ (last visited 29 September 2023).

[252] 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 29 September 2023).

[253] 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 29 September 2023).

[254] The International Trade Administration (ITA), U.S. Department of Commerce, Data Privacy Framework Program, https://www.dataprivacyframework.gov/s/ (last visited 1 September 2023).

[255] The International Trade Administration (ITA), U.S. Department of Commerce, Data Privacy Framework Program, Data Privacy Framework (DPF) Program Overview, https://www.dataprivacyframework.gov/s/program-overview (last visited 1 September 2023).

[256] European Commission, Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, OJ C (2023) 4745, 10.07.2023, 1-64.

[257] 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

assert their alignment in the use of the term "proportionate," although lacking consensus on its interpretation. If the US method of ensuring proportional access were implemented, it is unlikely that it would effectively prohibit mass surveillance.[258] It may also be observed within the context of Executive Order 14086, where the applicability of FISA (Foreign Intelligence Surveillance Act) provisions persists despite the fact that the mass surveillance regarding non-US persons authorised under FISA 702 has been deemed disproportionate by the CJEU on two different cases.[259]

---

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 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.

[258] For the full interview: Euractive: Schrems: round three (4 November 2022) https://www.euractiv.com/section/digital/podcast/schrems-round-three/ (last visited 29 September 2023).
NOYB, European Commission Gives EU-US Data Transfers Third Round At CJEU, 10 July 2023, https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu (last visited 29 September 2023).

[259] Executive Order No. 14086, vol. 87 no. 198 Federal Register, 14.10.2022, pp. 62283-62297, Section 2, (d)(iii)(e): "(e) Savings clause. Provided the signals intelligence collection is conducted consistent with and in the manner prescribed by this section of this order, this order does not limit any signals intelligence

On February 28, 2023, the EDPB published an opinion on the adequate protection of personal data under the Transatlantic Data Privacy Framework.[260] 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.[261] In this opinion, the EDPB asserted 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 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.[262]

Besides, Executive Order 14086 states 12 purposes for which collection is allowed as well as 4 objectives for which signals intelligence collection operations are prohibited.[263] In addition, 6 objectives for the use of data obtained in bulk are also outlined.[264] Yet, we are concerned that the President might, if required, add new objectives to these lists for new national security reasons.[265] 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.[266] We suggest that the President's power should have been limited under the adequacy decision at least with regard to the bulk collection of personal data.

---

collection technique authorized under the National Security Act of 1947, as amended (50 U.S.C. 3001 et seq.), the Foreign Intelligence Surveillance Act of 1978, as amended (50 U.S.C. 1801 et seq.) (FISA), Executive Order 12333, or other applicable law or Presidential directive."

[260] 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 29 September 2023).

[261] 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.

[262] 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.

[263] 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, 1-4.

[264] Executive Order No. 14086, vol. 87 no. 198 Federal Register, 14.10.2022, pp. 62283-62297, Section 2, (c)(ii).

[265] Executive Order No. 14086, vol. 87 no. 198 Federal Register, 14.10.2022, pp. 62283-62297, Section 2, (b)(i)(B).

[266] Executive Order No. 14086, vol. 87 no. 198 Federal Register, 14.10.2022, pp. 62283-62297, Section 2, (c)(ii)(C).

According to Executive Order 14086, personal data of non-US citizens are subject to the same retention periods and dissemination procedures as personal data of US citizens.[267] The EDPB notes that the retention period under Executive Order 14086 is not specified, and there are no stringent safeguards for onward transfers.[268] Indeed, no retention periods are specified for signal intelligence collection activities. However, the DPF requires intelligence agencies to define specific retention periods based on the various situations/factors (e.g., (e.g., whether the information is evidence of a crime; whether the information is foreign intelligence information) outlined in various legal instruments.[269] In the upcoming months, it will be determined if this implementation will be successful in practice.

In addition, according to the Executive Order 14086, data shall be disseminated within the US government if a trained individual has a reasonable belief that personal information will be adequately protected and the recipient has a need to know the data.[270] According to the DPF, however, onward transfers may be possible only for limited and specified purposes, on the basis of a contract between the EU-US DPF organisation and the third party. Besides, the contract should require the third party to provide the same level of protection as is guaranteed by the DPF Principles.[271]

Furthermore, the 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.[272]

What assurances does the "two-layer" redress mechanism offer? Under the first layer, the Civil Liberties Protection Officer (CLPO) in the Office of the Director of National Intelligence (ODNI) 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

[267] Executive Order No. 14086, vol. 87 no. 198 Federal Register, 14.10.2022, pp. 62283-62297, Section 2, (c)(iii)(A), 1(a) and 2(a).
[268] 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.
[269] European Commission, Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, OJ C (2023) 4745, 10.07.2023, 1-64, para 157.
[270] Executive Order No. 14086, vol. 87 no. 198 Federal Register, 14.10.2022, pp. 62283-62297, Section 2, (c)(iii)(A), 1(c).
[271] European Commission, Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, OJ C (2023) 4745, 10.07.2023, 1-64, para 38.
[272] Executive Order No. 14086, vol. 87 no. 198 Federal Register, 14.10.2022, pp. 62283-62297, Section 3, (d).

determine the appropriate remedy for those violations and ensure the compliance of US intelligence agencies with the privacy rights.[273]

Based on the second layer, EU citizens have the right to appeal the decisions of the CLPO before the newly established Data Protection Review Court (DPRC). The DPRC is comprised of qualified individuals selected from outside the US Government.[274] This court can issue binding decisions:

"When concluding its review, the DPRC may (1) decide that there is no evidence indicating that signals intelligence activities occurred involving personal data of the complainant, (2) decide that the ODNI CLPO's determinations were legally correct and supported by substantial evidence, or (3) if the DPRC disagrees with the determinations of the ODNI CLPO (whether a violation of applicable U.S. law occurred or the appropriate remediation), issue its own determinations."[275]

If the review concludes that a violation has occurred, the decision will specify the necessary measures for remedying the issue. These measures may encompass, for example, the removal of unlawfully acquired data or the recall of intelligence reports that contain data unlawfully transferred.[276]

The Executive Order also required that the DPRC select a special advocate for each case to represent the complainants' concerns and interests before the court, so ensuring the fair trial concept.[277] The Attorney General established regulations to accompany the DPRC's establishment.[278] The previous Ombudsman procedure lacked independence since the

[273] Executive Order No. 14086, vol. 87 no. 198 Federal Register, 14.10.2022, pp. 62283-62297, Section 3, (c)(i).
European Commission, Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, OJ C (2023) 4745, 10.07.2023, 1-64, para 181.
[274] European Commission, Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, OJ C (2023) 4745, 10.07.2023, 1-64, para 186.
[275] European Commission, Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, OJ C (2023) 4745, 10.07.2023, 1-64, para 190.
[276] European Commission, Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, OJ C (2023) 4745, 10.07.2023, 1-64, para 191.
[277] Executive Order No. 14086, vol. 87 no. 198 Federal Register, 14.10.2022, pp. 62283-62297, Section 3, (c)(i)(E)(3).
[278] 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.

Ombudsman was part of the US Department of State and lacked the similar investigative or decision-making authority. Therefore, we may conclude that the new oversight mechanism is more promising.[279]

According to Mr. Schrems, the Privacy Shield's "Ombudsperson" system was divided into two mechanisms: the review conducted by the Civil Liberties Protection Officer and the determination made by the Data Protection Review Court. In his perspective, he argues that this cannot be considered as a court, as individuals from the EU would not have the opportunity to present their cases personally. Instead, they would need to submit their applications through the EU data protection authorities. Moreover, he asserts that the outcome of the decision is predetermined even prior to the official ruling as[280]:

"After a review is completed in response to a complainant's application for review, the Data Protection Review Court, through procedures prescribed by the Attorney General's regulations, shall inform the complainant, through the appropriate public authority in a qualifying state and without confirming or denying that the complainant was subject to United States signals intelligence activities, that "the review either did not identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation."[281]

Nevertheless, DPF asserts that, in addition to the specific redress procedure implemented under Executive Order 14086, persons of any nationality or place of residence have access to other means for seeking redress within the regular US judicial system.[282]

---

[279] 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 29 September 2023).

[280] NOYB, European Commission Gives EU-US Data Transfers Third Round At CJEU, 10 July 2023, https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu (last visited 29 September 2023).

[281] Executive Order No. 14086, vol. 87 no. 198 Federal Register, 14.10.2022, pp. 62283-62297, Section 3, (d)(i)(H).

[282] "Access to these avenues is subject to the showing of 'standing'. This standard, which applies to any individual regardless of nationality, stems from the 'case or controversy' requirement of the U.S. Const., Article III. According to the Supreme Court, this requires that (1) the individual has suffered an 'injury in fact' (i.e. an injury of a legally protected interested that is concrete and particularised and actual or imminent), (2) there is a causal connection between the injury and the conduct challenged before the court, and (3) it is likely, rather than speculative, that a favourable decision by the court will address the injury (see Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992))".
European Commission, Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, OJ C (2023) 4745, 10.07.2023, 1-64, para 195.

Specifically, the FISA and an associated statute offer individuals the opportunity to initiate a civil lawsuit seeking monetary compensation from the US government in cases where their information has been unlawfully and intentionally utilised or disclosed. Moreover, people have the right to question the legality of surveillance if the US government plans to utilise or disclose any data acquired or generated through electronic monitoring as evidence in legal or administrative processes within the US.[283]

Before coming to a conclusion like Mr. Schrems', we suggest that it is necessary to examine the processes that DPRC as well as ordinary US courts will use in cases involving individuals who are non-US persons. Afterwards, it will be possible to evaluate how well they follow the principles of fairness, impartiality, and expediency.

Overall, the bulk surveillance issue of the US intelligence services continues to be the greatest concern, and as we have previously stated, the applicability of FISA (Foreign Intelligence Surveillance Act) provisions persists in Executive Order 14086 despite the fact that the CJEU has ruled twice that the mass surveillance authorised under FISA 702 is disproportionate.[284] Although unreasonable surveillance also violates the Fourth Amendment, non-US persons have no constitutional rights in the US. Therefore, EU data subjects' right to privacy is not protected by the Fourth Amendment.[285]

---

[283] European Commission, Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, OJ C (2023) 4745, 10.07.2023, 1-64, para 196.

[284] Executive Order No. 14086, vol. 87 no. 198 Federal Register, 14.10.2022, pp. 62283-62297, Section 2, (d)(iii)(e): "(e) Savings clause. Provided the signals intelligence collection is conducted consistent with and in the manner prescribed by this section of this order, this order does not limit any signals intelligence collection technique authorized under the National Security Act of 1947, as amended (50 U.S.C. 3001 et seq.), the Foreign Intelligence Surveillance Act of 1978, as amended (50 U.S.C. 1801 et seq.) (FISA), Executive Order 12333, or other applicable law or Presidential directive."

[285] "The Court has addressed the Fourth Amendment's scope with respect to whom the Fourth Amendment protects; that is, who constitutes the people, reasoning that it refers to a class of persons who are part of a national community or who have otherwise developed sufficient connection with [the United States] to be considered part of that community. The Fourth Amendment therefore does not apply to the search and seizure by United States agents of property that is owned by a nonresident alien and located in a foreign country. The community of protected people includes U.S. citizens who go abroad, and aliens who have voluntarily entered U.S. territory and developed substantial connections with this country. There is no resulting broad principle, however, that the Fourth Amendment constrains federal officials wherever and against whomever they act."
Congress.Gov, Constitution Annotated Analysis and Interpretation of the US Constitution, Fourth Amendment Searches and Seizures, Amdt4.3.1 Overview of Unreasonable Searches and Seizures, https://constitution.congress.gov/browse/essay/amdt4-3-1/ALDE_00013715/ (last visited 2 September 2023).

Mr. Schrems has already announced that NOYB has prepared a number of procedural options to bring the new framework before the CJEU.[286] In our viewpoint, it is likely that the CJEU will also invalidate the third transatlantic data transfer solution due to the unresolved surveillance issue. In order for the US to be deemed as providing an adequate level of data protection in comparison to the EU, it is essential that reforms be made to FISA 702 regarding surveillance practices involving non-US persons.

2.3 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 due to 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.

We have explained the background of the GDPR and the COPPA and we concluded the Subchapter 2.1 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.

Another reason to compare the relevant legislation of the EU and the US in this thesis is their strong economic cooperation. Since facilitating data sharing between these two jurisdictions is crucial to their economic collaboration, Subchapter 2.2 examined transatlantic data transfer history. We focused on the EU-US personal data free flow agreements. Since there are no specific requirements for children's data transfers, we didn't separate them in this Subchapter. However, we shall briefly explore in Chapter 5 whether children should have control over the transfers of their personal data to third countries before the age of digital consent.

This chapter contributes to the literature by providing a deductive comparison of the historical roots of the COPPA and Article 8 of the GDPR, along with an examination of the

[286] NOYB, European Commission Gives EU-US Data Transfers Third Round At CJEU, 10 July 2023, https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu (last visited 29 September 2023).

historical context surrounding transatlantic data transfers. In addition, we analysed the weaknesses and strengths of both pieces of legislation, as well as different privacy and data protection approaches on both sides of the Atlantic.

3. Concept of parental consent in the GDPR and the 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.[287] In accordance with the CFR, consent is one of the six legal grounds for processing personal data under the GDPR[288] 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".[289]

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. Otherwise, the processing of the collected personal information would be unlawful.[290]

Article 6 of the GDPR lists the lawful bases for processing personal data. These include the data subject's consent to the processing of his or her personal data for one or more specific purposes, the performance of a contract, compliance with a legal obligation, protection of the data subject's or other natural persons' vital interests, processing by public authorities, and the data controller's or a third party's legitimate interest.[291] Since our thesis focuses on Article 8 of the GDPR, which relates to conditions applicable to children's and parents' consent in regard to information society services, we shall concentrate on consent as the legal basis where data is processed in relation to information society services.[292]

Where data processing is not related to information society services[293], we should consult national civil legislation to see whether parental consent is necessary. Medical

[287] CFR, Article 8.
[288] GDPR, Article 6(1).
[289] GDPR, Article 4 (11).
[290] Article 29 Working Party, Guidelines on consent under Regulation 2016/679 17/EN WP 259 rev.01, 10 April 2018, 1-31, 3.
[291] GDPR, Article 6(1) (b-f).
[292] GDPR, Article 8(1).
[293] Indicative list of services not regarded as Information Society Services shall be found under the Annex I of Directive (EU) 2015/1535:
"1. Services not provided 'at a distance' Services provided in the physical presence of the provider and the recipient, even if they involve the use of electronic devices: (a) medical examinations or treatment at a

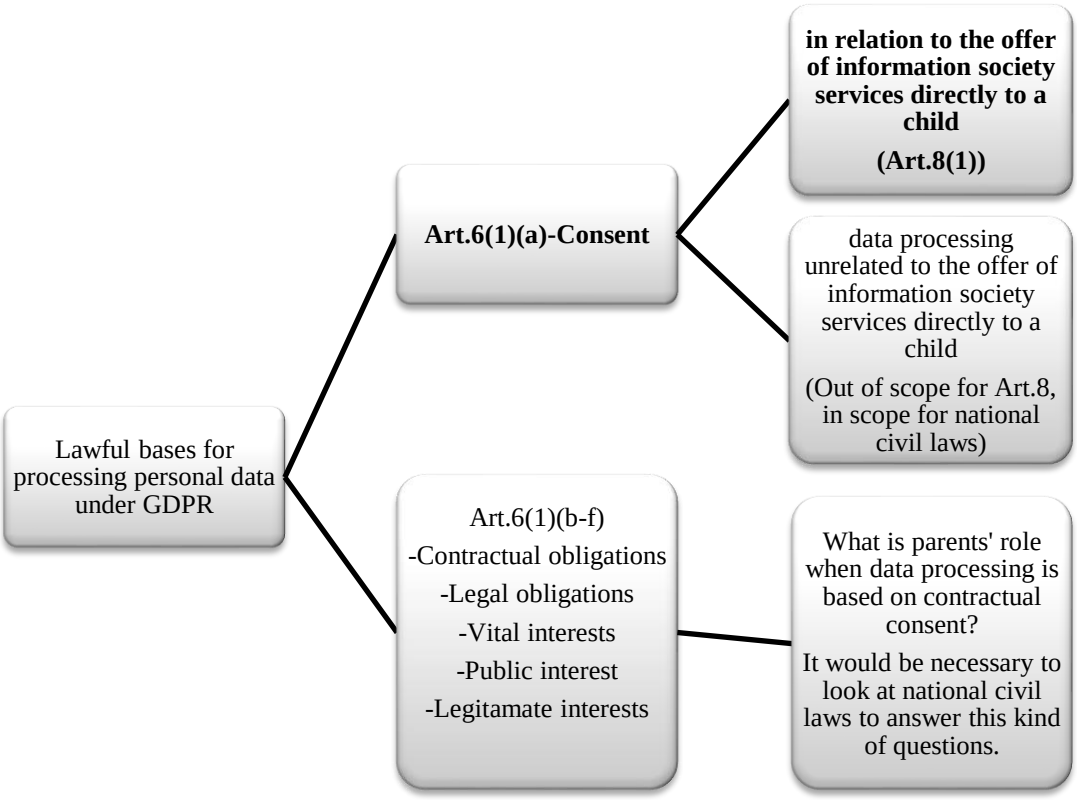
examinations or treatment at a doctor's office using electronic equipment, for example, would not be considered information society services[294], and we should consult national laws to determine the age at which a child can consent to his or her medical treatment without parental consent. It would be the age of majority (18) in countries such as Hungary and Italy, and 16 in countries such as Portugal and Spain, but in countries such as Germany and Sweden, it would be based on maturity rather than a fixed age.[295]

Other issues, such as the role of parents in data processing based on a contractual relationship, are outside the scope of this thesis and would necessitate a review of national civil laws. Nevertheless, this thesis will provide instances from civil law to clarify relevant issues, as case law concerning data protection, especially with children's personal data, remains limited. The focus points of this thesis from the standpoint of the lawful basis of data processing are highlighted in bold font in the schema below.

doctor's surgery using electronic equipment where the patient is physically present; (b) consultation of an electronic catalogue in a shop with the customer on site; (c) plane ticket reservation at a travel agency in the physical presence of the customer by means of a network of computers; (d) electronic games made available in a video arcade where the customer is physically present. 2. Services not provided 'by electronic means' — services having material content even though provided via electronic devices: (a) automatic cash or ticket dispensing machines (banknotes, rail tickets); (b) access to road networks, car parks, etc., charging for use, even if there are electronic devices at the entrance/exit controlling access and/or ensuring correct payment is made, — offline services: distribution of CD-ROMs or software on diskettes, — services which are not provided via electronic processing/inventory systems: (a) voice telephony services; (b) telefax/telex services; (c) services provided via voice telephony or fax; (d) telephone/telefax consultation of a doctor; (e) telephone/telefax consultation of a lawyer; (f) telephone/telefax direct marketing. 3. Services not supplied 'at the individual request of a recipient of services' Services provided by transmitting data without individual demand for simultaneous reception by an unlimited number of individual receivers (point to multipoint transmission): (a) television broadcasting services (including near-video on-demand services), covered by point (e) of Article 1(1) of Directive 2010/13/EU; (b) radio broadcasting services; (c) (televised) teletext." 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, Annex I.

[294] 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, Annex I(1)(a).

[295] FRA (European Union Agency for Fundamental Rights), 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 29 September 2023).



Schema 1: Lawful bases of data processing under the GDPR[296]

Furthermore, the GDPR and COPPA's concepts of children's and parents' consent and the definition of information society services will be examined in depth in the next subchapter (3.2). In this chapter, we will rather examine the GDPR's concept of consent by examining its definition.

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.[297]

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

[296] The author created this schema based on the Articles 6 and 8 of the GDPR.
[297] Article 29 Working Party, Guidelines on consent under Regulation 2016/679 17/EN WP 259 rev.01, 10 April 2018, 1-31, 5-6.

purposes"[298]. For instance, in the scenario where the data subject has provided consent to YouTube for the collection of personal data with the purpose of receiving recommendations for similar content videos, if YouTube were to thereafter let third parties provide adverts related to the content being seen, it would be necessary to get a new consent for this additional purpose.[299]

In light of the GDPR's transparency principle, consent should be informed.[300] 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.[301] 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.[302]

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 via several means, such as 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". 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.[303]

Moreover, before collecting personal data, the data controller should determine the legal basis that would be relied on at the time of collection. In the case of issues arising about consent, such as the data subject's choice to withdraw consent, the data controller is not permitted to replace the aforementioned legal bases with the data subject's consent.[304]

---

[298] GDPR, Article 5(1)(b).
[299] Article 29 Working Party, Guidelines on consent under Regulation 2016/679 17/EN WP 259 rev.01, 10 April 2018, 1-31, 11-12.
[300] GDPR, Article 5(1)(a).
[301] GDPR, Article 15.
[302] Article 29 Working Party, Guidelines on consent under Regulation 2016/679 17/EN WP 259 rev.01, 10 April 2018, 1-31, 13-15.
[303] Article 29 Working Party, Guidelines on consent under Regulation 2016/679 17/EN WP 259 rev.01, 10 April 2018, 1-31, 15-18.
[304] Article 29 Working Party, Guidelines on consent under Regulation 2016/679 17/EN WP 259 rev.01, 10 April 2018, 1-31, 23.

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 Recital 75 highlights that:

"The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: […] where personal data of vulnerable natural persons, in particular of children, are processed".[305]

Data Protection Authorities may also publish some processes for which mandatory data protection impact assessments (DPIAs) are required.[306] For example, the Hungarian Data Protection Authority (NAIH) requires DPIA where personal data processing involves biometrics for the purpose of uniquely identifying natural persons, particularly vulnerable persons such as children.[307] Additionally, a DPIA is required where large amounts of personal data related to vulnerable persons, including children, are processed for purposes other than the original purpose of the processing.[308] Furthermore, if children's personal data are processed for the purpose of profiling and automated decision making, a DPIA is also necessary.[309]

Likewise, the UK DPA requires a mandatory DPIA when using the personal data of children or other vulnerable persons in the context of marketing, profiling, other automated decision-making activities, or when offering online services directly to children.[310]

[305] GDPR, Recital 75.
[306] GDPR, Article 35(4).
[307] Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), GDPR 35 (4) Mandatory DPIA List, List of Processing Operations Subject to DPIA GDPR 35 (4), point (2), https://www.naih.hu/data-protection/gdpr-35-4-mandatory-dpia-list (last visited 29 September 2023).
[308] Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), GDPR 35 (4) Mandatory DPIA List, List of Processing Operations Subject to DPIA GDPR 35 (4), point (19), https://www.naih.hu/data-protection/gdpr-35-4-mandatory-dpia-list (last visited 29 September 2023).
[309] Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), GDPR 35 (4) Mandatory DPIA List, List of Processing Operations Subject to DPIA GDPR 35 (4), point (20), https://www.naih.hu/data-protection/gdpr-35-4-mandatory-dpia-list (last visited 29 September 2023).
[310] Information Commissioner's Office (ICO), When do we need to do a DPIA?, What does the ICO consider likely to result in high risk?, point (9), https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/ (last visited 29 September 2023).

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."[311]

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 […]".[312]

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"[313]; and second, the processing should be based on consent.[314] Contracts 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.[315] Furthermore, the phrase "offered directly to a

[311] GDPR, Article 8(1).
[312] GDPR, Recital 38.
[313] GDPR, Article 8(1).
[314] 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. [...]"
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).
[315] Article 29 Working Party, Guidelines on consent under Regulation 2016/679 17/EN WP 259 rev.01, 10 April 2018, 1-31, 24.
"The ECJ held that information society services cover contracts and other services that are concluded or transmitted on-line. Where a service has two economically independent components, one being the online component, such as the offer and the acceptance of an offer in the context of the conclusion of a contract or

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).[316]

Whereas the 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.[317]

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 Article 8 of the GDPR does. Furthermore, the COPPA requires operators to make reasonable efforts to obtain parental consent, taking into account the available technology. Unlike Article 8 of the GDPR, the COPPA provides some examples of methods for verifying parental consent. These include providing parental consent through e-mail or electronic scan;

---

the information relating to products or services, including marketing activities, this component is defined as an information society service, the other component being the physical delivery or distribution of goods is not covered by the notion of an information society service. The online delivery of a service would fall within the scope of the term information society service in Article 8 GDPR." EDPB, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1, Adopted on 4 May 2020, Updated on 13 May 2020, 1-33 para. 129.

[316] 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.

[317] 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.

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.[318]

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.[319] 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.[320]

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 updated 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.[321]

As stated above, unlike the COPPA, the 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 verifying parental consent would be good for both parents and data controllers as guidance. Nonetheless, there is still the possibility to adjust and adopt methods of the COPPA in

[318] 16 CFR COPPA 312.5(b)(2).
[319] FTC, Complying with COPPA: Frequently Asked Questions, QI.4., Complying with COPPA: Frequently Asked Questions | Federal Trade Commission (ftc.gov) (last visited 29 September 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 29 September 2023).
[320] 16 CFR COPPA 312.5(b)(2)(vi).
[321] 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 29 September 2023)

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.[322]

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.[323] 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 legislations 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.[324] 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.[325]

Furthermore, the exemptions granted by the COPPA, which allow operators to collect children's personal information without parental consent under some circumstances, do not qualify as an exception under the GDPR. To avoid any confusion, it is important to note that Article 8 of the GDPR does not use the term collection as the COPPA does.[326] The COPPA defines the collection as:

---

[322] For more information about the exceptions see: 16 CFR 312.5(c).
[323] GDPR, Recital (38).
[324] GDPR, Article 6(1)(f).
[325] GDPR, Article 6(1)(d) and (e).
[326] 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

"[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.[327] 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 the COPPA does not cover deletion if the operator takes reasonable measures to delete them prior to their public availability.[328]

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.[329] Consequently, parental sharing might result in (cyber)bullying among the teens' classmates.

---

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."

[327] 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."

[328] 16 CFR COPPA 312.2(2).

[329] 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, 104407.

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 online assistance from school counsellors/teachers.[330]

In this subchapter, 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 subchapter, we will analyse the threshold age at which parental consent must be obtained in accordance with the GDPR and the 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

Children under the age of 13 are more vulnerable to the hazards and consequences of their online behaviours and interactions, according to the FTC.[331] Hence, the COPPA defines the term "child" as an individual under the age of 13.[332] Can one argue that a child of 12 years old is vulnerable, but a child of 13 years old is not? In everyday life, children aged 12 and 13 frequently have similar abilities.[333]

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 subject matter in his initial draft. He classified a child as anyone under the age of 16, but they changed it to 13 for some economic reasons. Some e-commerce companies did not want to lose this attractive adolescent market. He now admits that the age threshold of 13 years was too low, but he

[330] The observed discrepancy could possibly be attributed to the differing extents of applicability of various legislations. The scope of COPPA is limited to the Internet, but the GDPR is not restricted by technology and applies to the processing of personal data regardless of the method employed, whether it be online or offline. It is conceivable that at the time of the enactment of the COPPA in 1998, the legislators may not have foreseen the emergence of online counselling services.

[331] 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 29 September 2023)

[332] 16 CFR COPPA 312.2 "Child: means an individual under the age of 13."

[333] 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.

claims that it was the best he could do, because not only e-commerce companies, but also civil liberties groups, were opposed to the age threshold of 16 years old.[334]

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.[335] 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.

[334] 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 29 September 2023).

[335] 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 29 September 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.

	Digital platforms[336]	Part-time work[337]	Medical treatments[338]	Sexual activity[339]
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

[336] 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 29 September 2023).

[337] 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://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Ffra.europa.eu%2Fsites%2Fdefault%2Ffiles%2Ffra_uploads%2Ffra-2018-social-rights-lgbti-specific-data_en.xlsx&wdOrigin=BROWSELINK (last visited 29 September 2023).

[338] 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 29 September 2023).

[339] FRA, Minimum age requirements related to rights of the child in the EU, Marriage and sexual consent; Citizenship; Political Participation; Religion; Health, https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Ffra.europa.eu%2Fsites%2Fdefault%2Ffiles%2Ffra_uploads%2Ffra-2017-status-religion-health-specific-data_en.xlsx&wdOrigin=BROWSELINK (last visited 29 September 2023).

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 States[340]

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

Given that health data is classified as a special category of personal data according to Article 9 of the GDPR[341], it is justifiable to set higher age thresholds for obtaining digital consent for the use of health data. In the GDPR's Preamble, it is stated that processing personal data which are sensitive by their nature poses a significant risk to the fundamental rights and freedoms of individuals.[342] 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 met[343]: 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).

[340] This table created by the author using the abovementioned sources.
[341] GDPR, Article 9(1).
[342] GDPR, Recital 51.
[343] GDPR, Article 9(2) (a-j).

Nevertheless, internet service providers profit from the processing of individuals' personal data; even if the personal data falls under the special categories,[344] 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."[345] 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.[346] 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 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.[347] 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.[348]

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

[344] 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.
[345] MyFitnessPal Privacy Policy, https://www.myfitnesspal.com/privacy-policy (last visited 29 September 2023).
[346] MyFitnessPal Privacy Policy, https://www.myfitnesspal.com/privacy-policy (last visited 29 September 2023).
[347] Happify, Legal, Happify™ Privacy Policy: Last Updated in July 2020, https://www.happify.com/public/legal/#legal (last visited 29 September 2023).
[348] 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 29 September 2023).

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 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.[349] It is also straightforward for a child to get a Gmail account. A child may simply provide an age that is appropriate in their country to open a Gmail account.[350] This method makes it very easy for a child to lie. This issue will be covered in-depth in the next chapter.

[349] MyFitnessPal, Sign Up, https://www.myfitnesspal.com/account/create (last visited 29 September 2023).
[350] Google, Sign Up, https://accounts.google.com/signup/v2/webcreateaccount?flowName=GlifWebSignIn&flowEntry=SignUp (last visited 29 September 2023).

Children may also get social media accounts by registering with the proper age requirement in their jurisdiction. Considering children under the age of 13 (or in some jurisdictions up to 16) cannot legally register for certain social media networks (e.g., Facebook[351], Instagram[352]), they appear to be lying about their ages in order to register for those platforms, as seen below in the Pew Research Center's 2020 surveys conducted in the US.[353] 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).

[351] 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 29 September 2023).
[352] Instagram Help Center, How to Report Things, Report a child under 13 on Instagram, https://help.instagram.com/2922067214679225/?helpref=hc_fnav (last visited 29 September 2023).
[353] In "Complying with COPPA: Frequently Asked Questions" FTC answers the question regarding the responsibility of operators for children's lie in general audience sites as: "The Rule does not require operators of general audience sites to investigate the ages of visitors to their sites or services. See 1999 Statement of Basis and Purpose, 64 Fed. Reg. 59888, 59892. However, operators will be held to have acquired actual knowledge of having collected personal information from a child where, for example, they later learn of a child's age or grade from a concerned parent who has learned that his child is participating on the site or service."
Federal Trade Commission, Complying with COPPA: Frequently Asked Questions, H. General Audience and Teen Sites or Services, 1, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#I.%20Verifiable%20Parental%20Consent (last visited 9 September 2023).
It should be also noted that 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. As mentioned before, 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. Moreover, there exist study findings and statistical data that confirm the presence of underage children within social media networks.

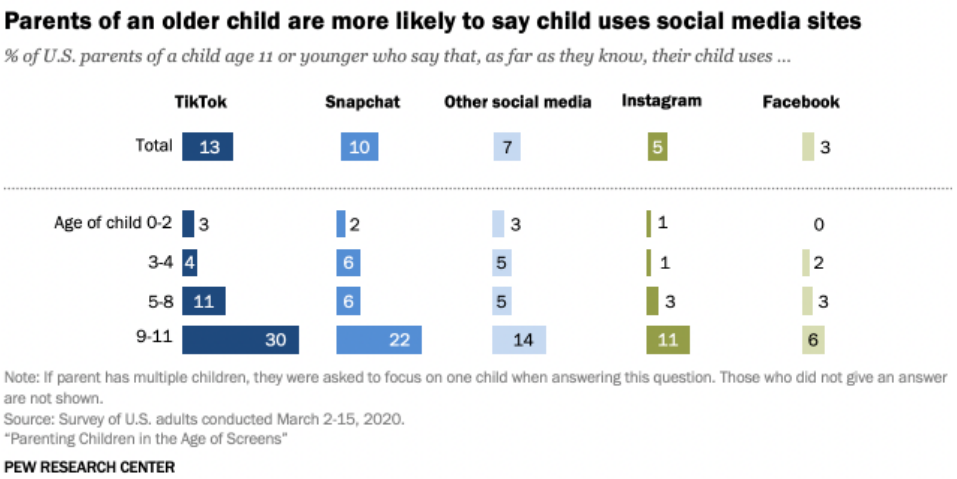


Chart 1: Children using social media sites by ages[354]

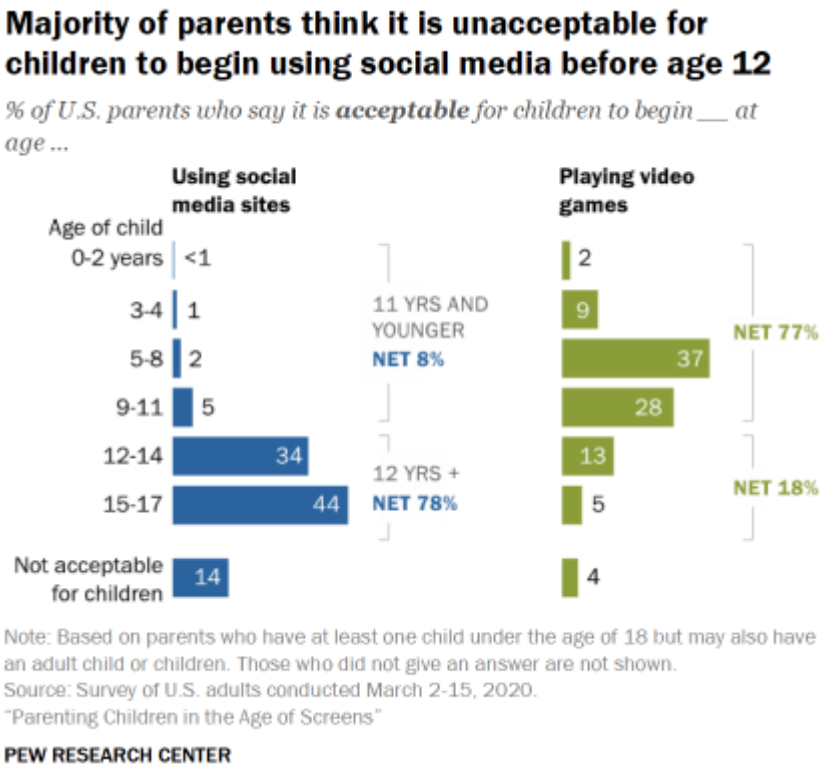


Chart 2: Appropriate ages for children to begin using social media sites and playing video games according to the parents[355]

[354] 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 29 September 2023).

[355] 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 29 September 2023).

As observed in the below 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 underage.

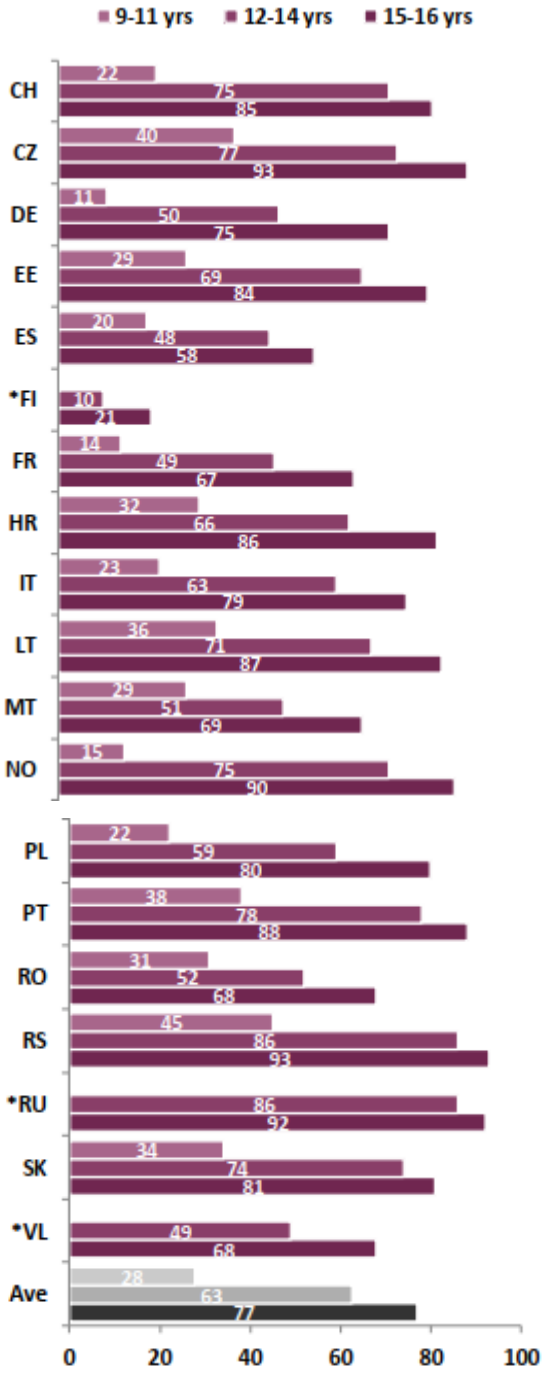


Chart 3: Percentages of children who visits social media networks daily[356]

[356] 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.

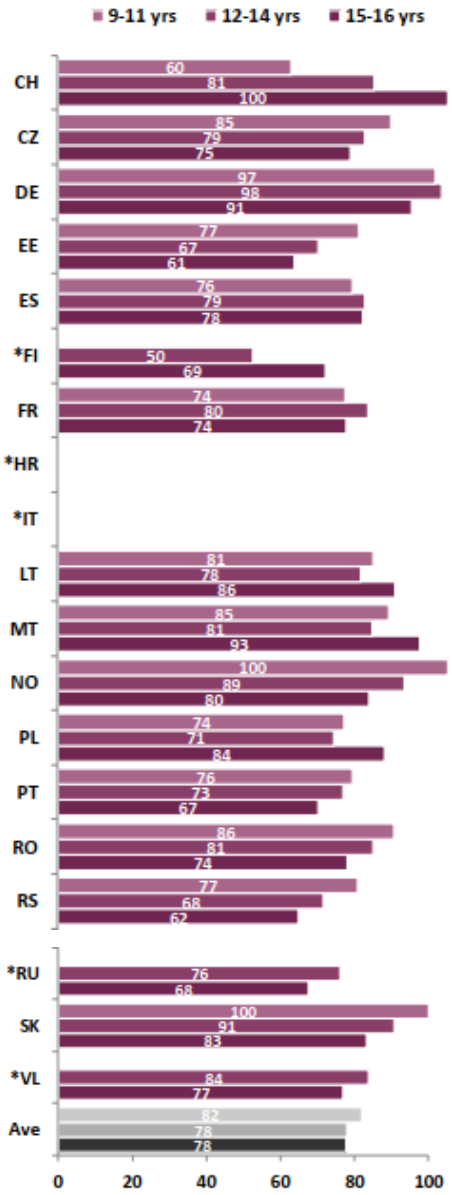


Chart 4: Percentages of children who suffered harm from online victimisation (at least a bit upset)[357]

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 networks. According to a research (2019) conducted by Better Internet for Kids (BIK)[358] about children's age of consent for data processing across the Europe, the selected countries'

[357] 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.

[358] 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.

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.[359] 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.[360]

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 chances 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.[361] 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.

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

[359] 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.

[360] 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 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), 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 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), 3.

[361] 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.

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 from the BIK report and EU Kids Online survey (2020) 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.[362]

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.[363] 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, unlike the draft law, the final law does not mention children and the age was set at 16 years.[364]

---

[362] 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.

[363] "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.

[364] "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

Another interesting example stated by the Czech Republic in their explanatory note on the draft law *(Dôvodová 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.[365] 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. Chapter 6 of this thesis will include further suggestions on the standardised age at which children may provide digital consent. Establishing a uniform age is also crucial for transferring data not only to third countries but also inside the Union. This topic will be discussed in Chapter 5.

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 digital platforms. Furthermore, there are certain advantages to participating in online

---

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.

[365] "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.

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 information[366] and freedom of expression.[367]

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.[368] We suggest that policymakers should review whether imposing age limits is useful or whether there would be other solutions.[369]

An alternative and optimal method would be to achieve a good balance with the aid of digital education and literacy. Another alternative would be the combination of parental supervision with the use of a software solution that limits inappropriate content and websites.[370] Furthermore, ethical design principles could be adopted by data controllers and online service providers (e.g., third-party suppliers who do not determine the processing purposes but offer online platforms). These principles would entail the inclusion of child-friendly content that considers the specific online needs of children.

However, currently, we should implement legal age restrictions on the Internet as mandated by 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.

[366] 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.
[367] 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.
[368] GDPR, Article 8 and 16 CFR COPPA 312.5.
[369] 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.
[370] 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 the 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.[371]

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.[372] 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 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.[373]

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)[374] or clicking a yes or no box (e.g., mralkohol.hu)[375] as proof that they are of legal age. That is affordable and extremely simple

[371] Asli Alkis, Investigating the usefulness of online age verification methods, Studia Iurisprudentiae Doctorandorum Miskolciensium, (2021) vol.1, 8.
[372] Carl Van der Maelen: The Coming-of-Age of Technology: Using Emerging Tech for Online Age Verifications, Delphi 2 (2019), 115.
[373] 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.
(*) "The Progress & Freedom Foundation is a market-oriented think tank that studies the digital revolution and its implications for public policy. Founded in 1993, its mission is to educate policymakers, opinion leaders and the public about issues associated with technological change, based on a philosophy of limited government, free markets and individual sovereignty. PFF's senior fellows and other scholars are leading experts in their fields, with distinguished careers in government, business, academia and public policy. Its underlying philosophy combines an appreciation for the positive impacts of technology with a classically conservative view of the proper role of government." It terminated its activities in 2010.
U.S. Department of State, Archive, Progress & Freedom Foundation https://2001-2009.state.gov/p/io/unesco/members/48807.htm (last visied 14 October 2023).
[374] Facebook, Sign Up: https://www.facebook.com/signup (last visited 29 September 2023).
[375] Mr.Alkohol (Coctails&Drinks), https://mralkohol.hu/ (last visited 29 September 2023).

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.[376]

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 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.[377]

Third, there is the use of a credit card, debit card, or other online payment systems as an age verification method.[378] 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.[379] 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.[380] 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.[381] Furthermore, while not all adults or children use credit or debit cards, requiring them and assuming that everyone has or should have one

---

[376] 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.

[377] 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.

[378] 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.

[379] 16 CFR COPPA 312.5(b)(2)(ii).

[380] 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 29 September 2023).

[381] 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 29 September 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.

might be discriminatory to those who do not prefer to use credit cards or cannot afford them at all.[382] 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 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., Ügyfélkapu[383] in Hungary).[384]

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. (However, this rule may not be applicable to adults with intellectual disabilities, since they may have the cognitive functioning of underage children.)[385] 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.[386]

Sixth, fingerprints, bone density, characteristic markings on the surface of the eye, or other biologically unique identifiers may be used to determine the age of users. There are not just physical biometrics, but also behavioural biometrics that may be used to determine

[382] 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.
[383] Ügyfélkapu, https://ugyfelkapu.gov.hu/ (last visited 29 September 2023).
[384] 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.
[385] Dilip R. Patel, Maria Demma Cabral, Arlene Ho, and Joav Merrick: A clinical primer on intellectual disability, Translational pediatrics 9, no. Suppl 1 (2020), S23-S35.
[386] 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.

a user's age, such as typing style.[387] 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..."[388] 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"[389]). 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.

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. Furthermore, fake fingerprints may imitate real ones in today's technology.[390] 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.[391] 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

[387] 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.
[388] GDPR, Article 9(1).
[389] GDPR, Article 6(1)(d).
[390] 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 29 September 2023).
[391] 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 29 September 2023).

a specific technological measures.[392] There are voice recognition artificial intelligence (AI) solutions that might be used for verifying the age of individuals, such as Apple's Siri,[393] which detects the users' voice and assists them with vocal instructions, or voice signatures,[394] 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 is used for unlocking the screen and accessing certain applications (e.g., Internet banking apps, e-wallet) on users' phones.[395]

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.[396] Therefore, we suggest that verifying the age via voice recognition tools is not an appropriate solution, and it can also cause the same security problems with fingerprints as we mentioned above. There is always the risk of having those unique features stolen by malicious attackers. Matching Face IDs and voice signatures with individuals' personal IDs might pose a significant risk since it may provide access to sensitive personal information, such as bank accounts[397] and phone access.

None of the aforementioned methods are flawless. On the one hand, there are 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

---

[392] 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.
[393] Apple, Siri, https://www.apple.com/siri/ (last visited 29 September 2023).
[394] For instance: HSBC Voice ID, https://www.hsbc.com.hk/ways-to-bank/phone/voice-id/ (last visited 29 September 2023).
[395] 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 29 September 2023).
[396] Asli Alkis: Investigating the usefulness of online age verification methods, Studia Iurisprudentiae Doctorandorum Miskolciensium, (2021) vol.1, 16-17.
[397] 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 29 September 2023).

that does not violate privacy but is ineffective in identifying exact age. Moreover, as previously mentioned, this method seems to be unhelpful for adults with intellectual disabilities. There is no middle ground solution that protects children's personal information while also protecting them from harmful content.[398]

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.

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 providers[399] 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.[400]

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 requirements of the GDPR, and what children and parents expect in terms of the safety and security of their personal data.[401]

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

[398] Asli Alkis: Investigating the usefulness of online age verification methods, Studia Iurisprudentiae Doctorandorum Miskolciensium, (2021) vol.1, 21.
[399] 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 29 September 2023).
[400] euCONSENT, FAQ: What is euCONSENT?, https://euconsent.eu/faq/ (last visited 29 September 2023).
[401] euCONSENT, euCONSENT's first large scale pilot (18 March 2022) https://euconsent.eu/euconsents-first-large-scale-pilot/ (last visited 29 September 2023).

seller website, and in order to do so, the children should verify their age using one of the methods provided. Subsequently, the website should redirect the users to the secure website, where they will be notified that they are underage to visit the aforementioned adult material website. The second objective was to access the dummy social networking platform. However, due to being recognised as underage in the previous task, they needed parental consent to proceed. The final task was gaining entry to a dummy chat website, which likewise required obtaining parental consent in order to successfully complete the mission. Other scenarios included a dummy knife seller website and a dummy dating site.[402]

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 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.[403]

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

[402] 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 29 September 2023).
[403] 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 29 September 2023).

means of age verification with only 3% of participants in the euCONSENT project, but the reason behind this is not mentioned.[404]

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

Taking all into account, the spirit of the GDPR and the 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. Although parents have authority over their children's internet activity, it is important to recognise that children are separate individuals and 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.[406]

The European Commission also acknowledges that age verification methods and parental consent tools, notwithstanding the implementation of the GDPR, are ineffective. This is due to the fact that most users are only required to submit their birth date or just tick a

[404] 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 29 September 2023).
[405] 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 29 September 2023).
[406] Asli Alkis: Investigating the usefulness of online age verification methods, Studia Iurisprudentiae Doctorandorum Miskolciensium, (2021) vol.1, 18-19.

box during the registration process.[407] As a result, in accordance with its eID proposal,[408] the Commission encourages the Member States to implement effective age-verification methods.[409] According to the Commission, children can use their eIDs to prove their age without revealing any other personal information (e.g., name or address).[410] On one hand, it would be a trustworthy solution, because it would be based on reliable government databases.[411] On the other hand, it may result in discrimination against those who do not wish to participate in this system; thus, this system would be preferable if it remained a voluntary choice.[412]

As mentioned before in Subchapter 2.1, the eID solution may also be employed to securely verify parental responsibility. Article 8 would encompass a paragraph, which would further elaborate on the subject matter:

> "Taking into consideration the state of the art, the controller and the processor should adopt adequate technologies to guarantee the consent is given or authorised by the holder of parental responsibility over the child, including inter alia as appropriate:
>
> (a) conducting a video conference with the parents to verify their official IDs
>
> (b) confirming the electronic identification (eID) of the parents compared with the eID of the children
>
> (c) Where the processing is unlikely to pose a high risk (e.g., subscribing to a newsletter), consent can also be given through email."[413]

---

[407] 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.

[408] 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).

[409] 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.

[410] 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.

[411] 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.

[412] 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 29 September 2023).

[413] The author developed this sample rule in light of the suggestions of her PhD thesis reviewers, Dr. Dániel Eszteri and Dr. Julien Rossi, as well as resembling the requirements of GDPR Articles 8 and 32.

Due to the mass storage of official documents and biometric data of users, this system might pose certain security and privacy risks. Therefore, it is essential that the system adheres to the privacy requirements outlined in the GDPR and is adequately safeguarded from malevolent cyber-attacks and hacking attempts. For instance, security measures such as the use of robust encryption techniques for both data storage and transmission, as specified in the GDPR.[414] It is also crucial to safeguard the encryption keys effectively to prevent any breach. Implementing a multi-factor authentication mechanism for users accessing eID services may enhance security.[415]

Undoubtedly, doing regular security audits and penetration testing is necessary for maintaining system security by identifying vulnerabilities. If a vulnerability is noticed, it should be promptly addressed and appropriately remedied. External professional third parties may offer security measures if needed.[416] Maintaining the latest security patches and upgrades for all software and systems is of utmost importance.[417] Another crucial measure is to provide users with comprehensive information on security protocols, including the need to generate robust passwords[418], refrain from exchanging login credentials with anybody, including close acquaintances[419], and promptly identify and report phishing attacks.[420]

[414] GDPR, Article 32(1)(a).

[415] "Multifactor authentication (MFA) is a secure process of authentication which requires more than one authentication technique chosen from independent categories of credentials. Like single factor, multifactor is increasingly used to verify the users' identities in accessing the cyber system and information. MFA combines two or more types of authentication to provide better and secure way of authenticating users. […] the most common four types of authentication factors are:
-What the user knows—usually the cognitive information of the users (example: passwords)
-What the user has—usually the items that a user possesses (example: smart cards)
-What the user is—a user's physiological and biometric traits (example: face, fngerprint, and voice)
-Where the user is—a user's location information (example: GPS, IP address)."
Dipankar Dasgupta, Arunava Roy and Abhijit Nag: Multi-Factor Authentication: More secure approach towards authenticating individuals, Advances in User Authentication, Springer International Publishing AG (2017), 186.

[416] GDPR, Article 32(1)(d) and for more information see: Sugandh Shah and Babu M. Mehtre: An overview of vulnerability assessment and penetration testing techniques, Journal of Computer Virology and Hacking Techniques 11 (2015), 27-49.

[417] Sugandh Shah and Babu M. Mehtre: An overview of vulnerability assessment and penetration testing techniques, Journal of Computer Virology and Hacking Techniques 11 (2015), 38.

[418] Kevin F McCrohan, Kathryn Engel, and James W. Harvey: Influence of awareness and training on cyber security, Journal of internet Commerce 9, no. 1 (2010), 24-27.

[419] Kevin F McCrohan, Kathryn Engel, and James W. Harvey: Influence of awareness and training on cyber security, Journal of internet Commerce 9, no. 1 (2010), 26.

[420] Matthew L Jensen, Michael Dinger, Ryan T. Wright, and Jason Bennett Thatcher: Training to mitigate phishing attacks using mindfulness techniques, Journal of Management Information Systems 34, no. 2 (2017), 599.

Finally, in the event that an incident occurs despite all the diligent efforts and rigorous security measures, it is important to have a well-defined incident response plan that clearly delineates the necessary actions to be taken in the case of a security breach.[421]

Moreover, governments or service providers should not abuse the system by monitoring individuals' use of eIDs.[422] Nonetheless, we welcome that unlike traditional personal ID verification solutions, the eID concept is based on the data minimisation principle[423] and is designed to provide selective disclosure of features (for example, allowing age verification without revealing the legal name, address, or other irrelevant data).[424] If the abovementioned security and privacy issues are mitigated and the security controls applied, 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.[425]

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. The 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.

---

[421] Eric C. Thompson: The incident response strategy, Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents (2018), 65-70.

[422] 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 29 September 2023).

[423] 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).

[424] 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 29 September 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 29 September 2023).

[425] 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 29 September 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 online activity habits and behaviours. Thus, we questioned the necessity of these threshold ages in the GDPR and the COPPA. However, given the current state of laws, we promoted awareness that the 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 the Internet age restrictions under the Subchapter 3.4. We examined age verification methods for implementing these restrictions. We observed that if security and privacy risks (e.g., cyber-attacks, hacker activities) are mitigated, the proposed eID solution by the European Commission would provide a privacy-friendly and EU-wide age verification method.

The GDPR's children-related provisions and the COPPA are predicated on parental supervision and responsibility. Indeed, parental actions are crucial for ensuring children's online safety. We emphasised, however, that parents should not use this responsibility to invade their children's privacy or restrict their access to the Internet's benefits. Therefore, it is optimal to design online platforms with child-friendly content that prioritises children's online needs. Also, online age verifications (such as the eID solution, which we regarded the safest to date) would help provide a solution that protects children's privacy, even from their parents, while protecting them from harmful content. This can be achieved not only by parental intervention, but also by data controllers and service providers providing the essential services.

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

This chapter will begin with evaluating the requirements concerning the data protection rights of children in accordance with the GDPR, followed by an examination of the rights afforded to parents under the COPPA. Ultimately, we will draw a conclusion by offering our recommendations for the ideal approach via a comparative analysis of the two legislations.

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.[426]

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.[427] Article 12 of the GDPR requires data controllers to use plain and clear language, particularly when any information relates to a child.[428]

Second, data subjects have the right to request access to any personal information about them obtained by data controllers.[429] 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.[430] For example, if a child wishes to access his/her data that is being processed by an educational children's website (e.g., Funbrain.com[431]), the privacy policies usually mention this right for EU data subjects.[432] 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

[426] GDPR, Article 12-23.
[427] GDPR, Article 12-14.
[428] GDPR, Article 12.
[429] GDPR, Article 15.
[430] GDPR, Recital 63.
[431] Fun Brain: https://www.funbrain.com/ (last visited 29 September 2023).
[432] Fun Brain, Privacy Policy: https://www.funbrain.com/privacy-policy (last visited 29 September 2023).

delay.[433] 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.[434] Most importantly, the data subjects exercise this right if they give consent 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.[435]

Furthermore, Article 17(2) of the GDPR refers to the right to be forgotten.[436] The "right to be forgotten" is a broader concept that originated in a European Court of Justice decision.[437] 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.[438] 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.[439] 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?

In the hypothetical scenario of this case occurring in the present day, it is worth considering that while the physical newspaper articles cannot be retroactively altered, Sidis might have potentially pursued the option of requesting the anonymisation of his personal

[433] GDPR, Article 16.
[434] GDPR, Article 17.
[435] GDPR, Recital 65.
[436] GDPR, Article 17(2).
[437] 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.
[438] 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.
[439] Case 113 F.2d 806, Sidis v. F-R Pub. Corporation (No. 400), Judgment 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.

information on the newspaper's website.[440] Consequently, this would afford him the opportunity to finally fade into obscurity in the public's perception. 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.[441] 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 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.[442] 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.[443] 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.[444] In addition, data controllers shall perform a data protection impact assessment (DPIA), if the processing of children's personal data 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.[445] For example, as mentioned above if the children's data is being processed with

[440] Hurbain v. Belgium judgment on 21 June 2021, referral to the Grand Chamber 11 October 2021, no.57292/16 para. 132 et seq. and Hurbain v. Belgium judgment (Grand Chamber) on 4 July 2023, no.57292/16 para. 255 et seq.
[441] GDPR, Recital 67.
[442] GDPR, Article 20 and Recital 68.
[443] GDPR, Article 21(1).
[444] GDPR, Article 6(1)(f).
[445] GDPR, Article 35(1) and Recital 75.

other aggravating factors (large number of data subjects, purpose of profiling, together with biometrics etc.), it may be required by the DPA in charge.[446]

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.[447] Besides, the GDPR's preamble offers additional protections for children when it comes to the use of their data for direct marketing purposes.[448] 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 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."[449]

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.[450] 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.[451]

---

[446] See the mandatory DPIA list of Hungarian DPA: Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), GDPR 35 (4) Mandatory DPIA List, List of Processing Operations Subject to DPIA GDPR 35 (4), points (2), (19), and (20), https://www.naih.hu/data-protection/gdpr-35-4-mandatory-dpia-list (last visited 29 September 2023).

[447] GDPR, Article 21(2) and Article 21(3).

[448] GDPR, Recital 38.

[449] GDPR, Article 22(1) and (2).

[450] GDPR, Recital 38 and 71.

[451] GDPR, Article 22(2).
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.

The child data privacy policy implemented by Vodafone serves as a noteworthy example in this context. If personal data processing occurs at the initial phase of a product or project, it is necessary to conduct a Privacy Impact Assessment (PIA), which is equivalent to the data protection impact assessment (DPIA) as stipulated by 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.[452] In other words, Vodafone's approach to child privacy goes beyond the GDPR's obligations in terms of profiling and direct marketing.

The GDPR does not specify how or when children can exercise these rights although the rights outlined above apply to children. 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.[453] 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.[454]

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. For example, accessing or erasing sensitive data (e.g., medical data) on the Internet requires a different handling than accessing or erasing personal data shared on social media networks

[452] 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 4 September 2023).
[453] 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.
[454] 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 29 September 2023).

(e.g., Facebook).[455] 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 preferrable 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.[456] Additionally, it would be optimal if there were forthcoming official guidance for children and their parents to effectively exercise the aforementioned data protection rights.

We recognise that there may be some rights that are too complex for children to exercise, hence parents should have the ability to do so if necessary. However, children who are sufficiently competent to comprehend the repercussions of their online acts may find it simpler to exercise their rights to access, ratification, and deletion without parental involvement. Besides, the exercise of these rights will not give rise to perilous circumstances for children under normal conditions.

Furthermore, the COPPA does not address the privacy rights of children, but rather focuses on outlining the "parental rights" related to the personal information of children. 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.[457] Second, parents have the right to review any personal information provided online by their children. The operator should provide the parents 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."[458]

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,

[455] 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.
[456] 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.
[457] 16 CFR COPPA 312.4(a).
[458] 16 CFR COPPA 312.6(a)(2).

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.

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 took her own life 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.[459]

Moreover, 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) could 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)[460], 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,[461] 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,[462] and the right to engage in play and recreational activities appropriate to their age and maturity.[463] 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.

---

[459] YouTube, Thesomebodytoknow channel: My story: Struggling, bullying, suicide, self-harm, available at: https://www.youtube.com/watch?v=vOHXGNx-E7E (29 September 2023) cited in 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 29 September 2023).

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

[461] UNCRC, Article 12.

[462] UNCRC, Article 13.

[463] UNCRC, Article 31.

However, the GDPR's, and particularly the COPPA's overprotective parental 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 the COPPA should not disregard this, and children should be given as much 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 only 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, the 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 would 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. Children shall be provided with the means to acquire knowledge regarding their rights and then engage in their exercise independently or give such responsibility to their parents.

Ergo, it has been determined that legislation alone is insufficient in establishing a safe online environment for children. Instead, a collaborative effort involving data controllers, service providers, and parents is necessary to accomplish this goal.

5. Main obligations imposed on data controllers under the GDPR and the COPPA

This chapter will commence by assessing the requirements imposed by the GDPR on data controllers, with particular emphasis on the data protection and privacy rights of children. Subsequently, we will proceed to examine the aforementioned matter within the context of the COPPA. Finally, we will do an analysis that compares the data controller requirements regarding children (and their parents) within both legislations.

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"[464] 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."[465]

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.[466]

Second, the following measures should be implemented by the data controller: appropriate technical measures including pseudonymisation and encryption of relevant personal data,[467] and organizational measures including risk assessment which means mitigating solutions to reduce risks[468] as well as having effective and compliant data

[464] GDPR, Article 4(7).
[465] GDPR, Article 24(1).
[466] GDPR, Article 5(1)(a)(b)(c)(d)(e)(f).
[467] GDPR, Article 32(1)(a).
[468] GDPR, Article 35 (Data Protection Impact Assessment).

protection policies in place.[469] Third, the data controller shall make it possible and easy for data subjects to exercise their rights.[470]

Fourth and most significantly for our thesis, data controllers 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.[471]

Approved codes of conduct, as defined in Article 40 of the GDPR,[472] or approved certification mechanisms, as defined in Article 42 of the GDPR,[473] might be used to demonstrate that the data controller is appropriately implementing the obligations.[474]

Fifth obligation of the data controller is to guarantee that the concept of data protection by design and by default is followed.[475] Data protection by design involves the incorporation of data protection principles from the first stages of a project, product, or asset's development, and throughout its entire life cycle. To attain this objective, the GDPR requires data controllers to implement suitable technological or organisational measures, including the use of pseudonymisation and encryption mechanisms.[476]

---

[469] GDPR, Article 24(2).
[470] GDPR, Article 12(2).
[471] GDPR, Article 8(2).
[472] 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."
[473] 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."
[474] GDPR, Article 24(3).
[475] GDPR, Article 25.
[476] GDPR, Article 25(1).
European Commission, What does data protection 'by design' and 'by default' mean?, https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en (last visited 13 September 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 13 September 2023).

The principle of data protection by default entails that data controllers exclusively handle data that is essential for the fulfilment of their processing purposes. The concept is linked to the fundamental principles of data minimization and purpose limitation. In this scenario, should there be any alterations in the personal data processing conducted by the data controller, or if the data controller opts to process more data pertaining to the data subject, it is imperative for the data controllers to obtain updated consent from the data subjects accordingly. It is important to ensure that accessibility is limited as well. For instance, it is recommended to promote the implementation of user profile settings on social media platforms that prioritise privacy, ensuring that they are not by default accessible to an unlimited number of individuals.[477]

Sixth, 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.[478]

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 GDPR[479] and 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.[480] The processor's responsibility also includes returning or deleting the processed data at the end of processing, if demanded by the data controller.[481]

Seventh, each data controller and processor shall also document their processing actions and make them available to the supervisory authority if required, so that this documentation

---

[477] GDPR, Article 25(2).
European Commission, What does data protection 'by design' and 'by default' mean?, https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en (last visited 13 September 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 13 September 2023).
[478] GDPR, Article 28(1) and Recital 81.
[479] 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 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 29 September 2023).
[480] GDPR, Article 28(3) and Recital (81).
[481] GDPR, Article 28(3)(g).

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.[482]

Eighth, data controllers and processors should collaborate with the supervisory authority to perform its tasks where required.[483] Furthermore, as a ninth obligation, as soon as the data controller gets aware of a personal data breach, they must notify the supervisory authority within seventy-two hours of being aware of it.[484] Failure to address the data breach might

[482] GDPR, Article 30 and Recital (82).

[483] 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 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."

[484] GDPR, Article 33(1).

> "[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".[485]

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.[486] 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.[487]

The tenth obligation states that if the data breach is likely to result in a high risk to a data subject's rights and freedoms, data controllers 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 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.[488]

Data subjects may not need to be warned 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,

[485] GDPR, Recital (85).
[486] 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 29 September 2023).
[487] 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).
[488] GDPR, Article 34(1) and (2).

the communication shall not be required when disproportionate effort is involved. Instead, in such cases, public communication may occur to inform data subjects.[489]

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.[490] 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 health[491] 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).[492]

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.[493]

---

[489] GDPR, Article 34 (3)(a)(b) and (c).

[490] 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.

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

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

[493] 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

As per the eleventh obligation under the GDPR, in cases where new technologies are employed and a particular method of data processing is expected to pose a high risk to the rights and freedoms of individuals, data controllers shall conduct a data protection impact assessment (DPIA) before the processing occurs.[494] 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".[495] The reason of this exception can be due to the obligation of confidentiality of these professions.

Moreover, the DPAs provide comprehensive information on DPIA methodologies, which may help data controllers in determining how to conduct DPIAs.[496] DPAs may also publish guidelines outlining the specific processes that necessitate mandatory DPIAs.[497] Besides, it should be noted that when conducting the data protection impact assessment, the data controller should

---

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.

[494] GDPR, Article 35(1).

[495] GDPR, Recital (91).

[496] CNIL (French DPA), Privacy Impact Assessment (PIA) Methodology, (February 2018), https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-pia-1-en-methodology.pdf (last visited 29 September 2023).
AEPD (Spanish DPA), Risk Management and Impact Assessment in the Processing of Personal Data, (June 2021), https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf (last visited 29 September 2023).

[497] See various mandatory DPIA listings of different DPAs:
Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), GDPR 35 (4) Mandatory DPIA List, List of Processing Operations Subject to DPIA GDPR 35 (4), https://www.naih.hu/data-protection/gdpr-35-4-mandatory-dpia-list (last visited 13 September 2023).
AEPD (Spanish DPA), List of The Types of Data Processing That Require a Data Protection Impact Assessment under Art 35.4, p. 1-3, https://www.aepd.es/sites/default/files/2019-09/listas-dpia-en-35-4.pdf (last visited 13 September 2023).
Data Protection Commission Ireland, List of Types of Data Processing Operations which require a Data Protection Impact Assessment, p. 1-6, https://www.dataprotection.ie/sites/default/files/uploads/2018-11/Data-Protection-Impact-Assessment.pdf (last visited 13 September 2023).
CNIL (French DPA), Analyse d'impact relative à la protection des données : publication d'une liste des traitements pour lesquels une analyse est requise (6 November 2018), https://www.cnil.fr/fr/analyse-dimpact-relative-la-protection-des-donnees-publication-dune-liste-des-traitements-pour (last visited 13 September 2023).

the data protection officer, if one has been appointed.[498] The data controller or processor shall assist and provide enough resources to data protection officers in order for them to carry out their functions and obligations as outlined in Article 39[499] of the GDPR.[500]

Therefore, 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.[501] There are new platforms (e.g., OneTrust, The open source DPIA software by the French DPA[502]) 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.[503]

According to the twelfth obligation, before processing personal data, the data controller shall consult the supervisory authority if the data protection impact assessments shows that data controller cannot mitigate unacceptably high residual risks. 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

---

[498] GDPR, Article 35(2).

[499] 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."

[500] GDPR, Article 38(2).

[501] 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 29 September 2023).

[502] CNIL, The open source PIA software helps to carry out data protection impact assessment, (30 June 2021), https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment (Portable and online versions are available. CNIL provided English translations for the tool, and a few EU DPAs offered translations as well, such as Hungarian DPA and Italian DPA. In addition, other translations are given by the community, such as Spanish and Croatian.) (last visited 29 September 2023).

[503] 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 29 September 2023).

extended by up to six more weeks considering the complexity of the planned data processing.[504]

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, 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.[505]

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.[506]

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.[507]

Ultimately, 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.[508]

---

[504] GDPR, Article 36 (1) and (2).

[505] 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 29 September 2023).

[506] GDPR, Recital (75).

[507] 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.

[508] GDPR, Article 44-50.

As previously indicated, the exchange of personal data between countries outside the European Union is essential for fostering the growth of international trade and cooperation.[509] In accordance with Article 45 of the GDPR, the transfer of data to a third country or international organisation is allowed only if the European Commission determines that said third country or international organisation offers an adequate level of data protection, as mandated by the Regulation. In the event that the European Commission ascertains that the third country or international organisation in question offers a sufficient level of protection, there is no need for any additional measures to be taken by the data controller in facilitating the transfer.[510]

In the absence of an adequacy decision, it remains feasible to transfer personal data from the EU to a third country in accordance with the GDPR. This can be achieved by implementing appropriate safeguards by the data controller or processor and ensuring that data subjects possess enforceable rights and effective legal remedies.[511] Therefore, it is important to thoroughly assess every single case for both data importers and exporters. In the absence of adequacy decisions, data controllers bear a substantial burden.

According to Article 46 of the GDPR, suitable measures for ensuring data protection may involve various safeguards such as binding corporate rules (BCRs), standard contractual clauses (SCCs), certification mechanisms, and codes of conduct.[512] The BCRs and SCCs were established specifically targeting controllers and processors (data exporters) who transfer personal data from the EU to third countries. On the other hand, the certification system and codes of conduct were developed for controllers and processors located in third countries that fall outside the scope of the GDPR. Certification and codes of conduct mechanisms can be sought and obtained by the data importer established in a third country.[513]

---

[509] GDPR, Article 101.

[510] GDPR, Article 45(1).
For the list showing the countries who have been determined as possessing an adequate level of data protection by the European Commission see: 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 29 September 2023).
For more detailed information about EU-US free data flow agreements and related adequacy decisions see: Subchapter 2.2.

[511] GDPR, Article 46(1).

[512] GDPR, Article 46(2)(a-f).

[513] For more information about the certification mechanism: EDPB, Guidelines 07/2022 on certification as a tool for transfers, version 2.0, 14 February 2023, 1-19, edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_en_0.pdf (europa.eu) (last visited 4 September 2023). For more information about the codes of conducts: EDPB, Guidelines 04/2021 on codes of conduct as tools for

Furthermore, in the absence of an adequacy decision or appropriate safeguards, the transfer of personal data to a third country or international organisation may be allowed if one of the exceptions enumerated in Article 49 of the GDPR is applicable.[514]

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.[515]

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.[516] 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. 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.[517]

The GDPR does not specifically include provisions regarding the transfer of data pertaining to children. Nevertheless, it is our contention that children need to possess a certain degree of agency in managing their data transfers, particularly in low-risk scenarios such as the cessation of those transfers. We suggest that if a child demonstrates sufficient maturity to request, for example, the termination of the transfer of their personal data to third countries, it should be incumbent upon data controllers to fulfil this request, even in the absence of parental consent.

---

transfers, 22 February 2022, 1-16, https://edpb.europa.eu/system/files/2022-03/edpb_guidelines_codes_conduct_transfers_after_public_consultation_en_1.pdf (last visited 4 September 2023).

[514] GDPR, Article 49.

[515] GDPR, Article 49(1) (a-g).

[516] GDRP, 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 4 September 2023).

[517] 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 4 September 2023).

Moreover, it is possible to observe instances from real-life scenarios. Due to the requirements set forth by the GDPR, children who are underage are not permitted to exercise control over the transfer of their personal data. Consequently, the services listed below do not offer the option for underage children to grant consent for a prohibition or termination of such data transfers without the involvement of their parents.

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.[518] 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).[519]

YouTube Kids is a new and relatively safer platform for children, and its privacy standards are identical to those of Google.[520] 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).[521]

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.[522] 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 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

[518] Google Family Link https://families.google/familylink/ (last visited 29 September 2023).
[519] 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 4 September 2023).
[520] YouTube Kids: An application specially designed for children https://www.youtube.com/kids/ (last visited 4 September 2023).
[521] YouTube Kids Privacy Notice: Information we share https://kids.youtube.com/t/privacynotice (last visited 4 September 2023).
[522] Johnson & Johnson, Privacy Policy: Use by Minors https://www.jnj.com/corporate/privacy-policy (last visited 4 September 2023).

group in order to perform a comparison for research purposes.[523] 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.[524] Johnson & Johnson is also based in the US; consequently, according to these latest updates, the data protection and privacy rights of Johnson & Johnson vaccine study participants, who are children, are at risk of being violated.[525]

The current privacy policies of Facebook and Instagram do not provide any specific information on the transfer of children's data from the EU to third countries.[526] The utilisation of social media platforms by children is evident based on news reports, research studies, and statistical data, as will be further explored in Chapter 6 of this thesis. However, the privacy policies of Facebook and Instagram neglect this aspect of the matter.

Chapter 5 of the GDPR does not apply to the transfers of personal data within the EU. It is important to note that there are no restrictions in place concerning the free movement of personal data within the Union.[527] Nevertheless, another issue arises when the transfer of personal data is conducted between different Member States. The age restrictions for processing personal data based on consent among children in EU Member States differ, as indicated in Subchapter 3.3 of this thesis.[528]

---

[523] 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 4 September 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 4 September 2023).

[524] 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 4 September 2023).

[525] "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 4 September 2023).

[526] Facebook, Privacy Policy: How do we transfer information?, https://www.facebook.com/privacy/policy?section_id=9-HowDoWeTransfer (last visited 4 September 2023).
Instagram, Privacy Policy, How do we transfer information?, https://privacycenter.instagram.com/policy/?section_id=9-HowDoWeTransfer (last visited 4 September 2023).

[527] "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." GDPR, Article1(3).

[528] 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),

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,[529] 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.[530]

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.[531]

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, by making the age requirement uniform throughout all EU Member States.

In Chapter 6 of this thesis, we will propose an age of digital consent that would be applicable to all Member States. This proposal will be predicated upon the influence of age disparities on the comprehension of online data protection and privacy among children and teenagers.

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).
See the Table 1 of this thesis under the Subchapter 3.3.

[529] 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.

[530] 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.

[531] 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.

The GDPR lacks a particular provision that addresses the specific obligations of data controllers in relation to the processing of personal data belonging to children. Yet, the COPPA specifically addresses the responsibilities of operators with respect to the processing of children's personal information. Further, we will examine how COPPA's approach differs from that of the GDPR. This will enable us to compare the two pieces of legislation and offer suggestions in accordance with our findings.

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."[532]

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.[533]

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.[534] 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.

[532] 16 CFR COPPA 312.2 "Operator".
[533] 16 CFR COPPA 312.2 "Operator" (1) and (2).
[534] 16 CFR COPPA 312.3(a).

Second, before collecting information from children, operators should provide direct notification to parents and get verifiable parental consent from them.[535] 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.[536] 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 request[537] or for the child's safety[538]. 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.[539]

Nonetheless, reasonable efforts are likewise a vague phrase in this context, as it is in Article 8 of the GDPR.[540] For instance, some website administrators could understand "reasonable efforts" as the act of looking for parents on social networking platforms and discontinuing the search if their account cannot be found.

Third, the operator shall provide parents the choice of giving consent for the collection of their children's data without giving consent for the disclosure of such data to third parties.[541] Fourth, the operator guarantees that parents have access to their children's personal data in order to review and/or delete it.[542]

Fifth, operators should provide parents with the option to restrict future use or collection of their children's personal information.[543] 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

[535] 16 CFR COPPA 312.4(a)(b).
[536] 16 CFR COPPA 312.5(c)(1).
[537] 16 CFR COPPA 312.5(c)(3).
[538] 16 CFR COPPA 312.5(c)(5).
[539] 16 CFR COPPA 312.5(c)(5).
[540] 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."
[541] 16 CFR COPPA 312.5(a)(2).
[542] 16 CFR COPPA 312.6(a).
[543] 16 CFR COPPA 312.3(c).

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.[544] 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.[545] 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.[546] Finally, the eighth obligation of operators under the COPPA is consistent with the GDPR's data minimisation principle.[547] It is prohibited for operators to condition children's participation in a game or other online activities on disclosing more information about the children than is required to engage in such activity.[548] 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.

[544] 16 CFR COPPA 312.8.
[545] GDPR Article 5(1)(b).
[546] 16 CFR COPPA 312.10.
[547] GDPR Article 5(1)(c).
[548] 16 CFR COPPA 312.7.

The following table presents the obligations and responsibilities of data controllers under the GDPR and operators under the COPPA, aiming to facilitate comprehension prior to comparing the approaches of these two legislations.

Obligations of data controllers under the GDPR	**Obligations of operators under the COPPA**
Adhering to the personal data processing principles outlined in Article 5 (Lawfulness, fairness, and transparency, accuracy, purpose limitation, data minimisation, storage limitation, integrity, confidentiality, and accountability)	Posting a privacy policy on their websites outlining their practices with children's personal information collected online
Implying appropriate technical measures (e.g., pseudonymisation and encryption of personal data), and organizational measures (e.g., risk assessment which means mitigating solutions to reduce risks) as well as having effective and compliant data protection policies in place	Providing direct notification to parents and getting verifiable parental consent from them prior to collecting information from children
Enabling data subjects to exercise their rights efficiently and easily	Granting parents the option to provide consent for the collecting of their children's data while withholding consent for the disclosure of this data to third parties
Making reasonable efforts, considering current technology, to get consent for processing children's data from the holder of parental responsibility for the child if the child is underage	Ensuring that parents have access to their children's personal data in order to review and/or delete it
Ensuring adherence to the concept of data protection by design and by default is being followed	Offering parents the opportunity to restrict future use or collection of their children's personal information

Choosing processors who are knowledgeable, reliable, and having adequate resources to ensure the requirement of appropriate technical and organizational measures	Keeping the information they gather from children confidential, secure, and intact
Documenting their processing actions and making them available to the supervisory authority if required	Keeping the obtained information for as long as it is required for the purpose for which it was collected in the first place (in line with GDPR's purpose limitation principle)
Cooperating with the supervisory authority to perform its tasks	Avoiding from making children's involvement in a game or other online activities contingent upon the disclosure of excessive personal information beyond what is necessary for participation (in line with GDPR's data minimisation principle)
Notifying the supervisory authority within seventy-two hours of being aware of a personal data breach	
Notifying data subjects without undue delay if the data breach is likely to result in a high risk to a data subject's rights and freedoms	
Conducting a DPIA prior to processing in cases where new technologies are employed, and a particular method of data processing is expected to pose a high risk to the rights and freedoms of individuals	
Consulting the supervisory authority before processing personal data if the data protection impact assessments shows that data controller cannot mitigate unacceptably high residual risks	

Facilitating the transfer of personal data from the EU to third countries (via adequacy decisions/appropriate safeguards/derogations for specific situations)	

Table 2: The obligations of data controllers under the GDPR and operators under the COPPA[549]

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.

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 as discussed above. For riskier actions, such as sharing content on publicly available websites or transferring data, data controllers may still seek parental consent.[550]

[549] The table has been constructed by the author, drawing upon the aforementioned information.
[550] 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.

In light of the preceding discussions in Chapter 4 and 5, it is possible to suggest an article for the GDPR that focuses on the specific obligation of data controllers with regard to children. The article would be presented as follows:

> "1. Children may lack awareness regarding privacy policies and their rights pertaining to privacy and data protection. In accordance with best practises, data controllers shall employ simple video presentations or visually engaging images accompanied by easily comprehensible language to enhance children's understanding of their data protection rights, particularly with regard to the right to be informed and the right to access their personal data.
>
> 2. The use of the rights to ratification, erasure and prohibition or termination of data transfers shall be allowed in cases when children possess the necessary level of maturity to independently request such actions, hence eliminating the requirement for parental consent.
>
> 3. The practise of profiling may be subject to prohibition unless there exists a compelling or public interest that may outweigh the interests of the child in question. However, in the event that such a situation arises, it shall be still possible for a child to object to this profiling. In this scenario, it is imperative for the data controller to take prompt action, without delay, even in the absence of parental consent.
>
> 4. In the event of data breaches, data controllers are required to inform parents and children concurrently, even if the children are at an age where they can provide consent, as a precautionary measure. In addition, it is essential that they provide parents with information and assistance to assist them in mitigating the negative consequences of personal data breaches on their children. The exemptions specified in Article 34(3) shall not be applicable in cases where the individual whose data is being processed is a child.
>
> 5. The Regulation shall reserve all other responsibilities of data controllers and all other rights of children."

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, we assert that 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.[551]

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. Given the potential high risk involved in processing children's personal data, it would be advantageous for operators to work together with supervisory authorities and carry out data protection/privacy impact assessments with the help of specialised data protection/privacy officers. This would allow for the identification, evaluation, and mitigation of risks prior to processing the children's personal data, ultimately benefiting them.

In conclusion, it is essential for operators regulated by COPPA and data controllers regulated by GDPR to ensure that children have access to data protection and privacy rights, enabling them to have control over their data and make informed choices about their online activities with mitigated risks.

5.2 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.

The COPPA takes a different approach and particularly addresses the obligations of operators regarding processing children's personal data. Yet, COPPA requires operators to engage with parents to protect children's personal data, rather than directly communicating with the children in question. We proposed that operators provide children (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

[551] 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.

justified this suggestion by asserting that processing children's personal data would almost certainly pose a high risk owing to children’s vulnerability.

6. 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.[552]

As Facebook, YouTube, and Instagram are the most popular social networks in the world,[553] 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,[554] and the COPPA rule defines a child as an individual under the age of 13,[555] 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.[556]

---

[552] 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.

[553] Statista: Most popular social networks worldwide as of January 2023, 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 29 September 2023).

[554] "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 29 September 2023).

[555] 16 CFR COPPA 312.2 "Child": "means an individual under the age of 13."

[556] 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 29 September 2023) Instagram, Help Centre, Tips for Parents: Report a child under 13 on Instagram, https://help.instagram.com/517920941588885/?helpref=uf_share (last visited 29 September 2023). YouTube, Terms of Service, General Terms and Conditions: Who can use the service?, Age requirements https://kids.youtube.com/t/terms (last visited 29 September 2023).

However, parents who post their children's material, images, and/or videos online suffer no consequences under the COPPA and the GDPR. Furthermore, these parents are not bound by any legal restrictions imposed by the COPPA or the GDPR.[557] Even so, it is important to note that parents may encounter some repercussions under the civil laws of EU Member States and the US.[558] Given the scope of our thesis, which focuses on data protection and privacy legislations, we shall not delve into the provisions of civil laws in this context.

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.[559]

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).[560]

---

[557] 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 29 September 2023).

[558] For example, according to Hungarian civil law, parents might potentially face loss of parental custody if they engage in the act of disclosing their child's personal data on the internet, provided that this action causes serious harm or violation of the child's interests.

"Section 4:191 [Judicial termination of parental custody] (1) The court shall terminate parental custody if a) the parent is at fault in seriously harming or jeopardising the interests of the child, in particular the physical well-being, mental or moral development of the child […]"

"Section 4:193 [Eligibility for bringing an action for the termination and restoration of parental custody rights; defendants in the action] (1) An action for the termination of parental custody shall be brought by the other parent; and for its restoration by either parent. The child, the guardianship authority and the prosecutor shall also be eligible to bring an action in both cases. [...]"

Act V of 2013 on the Civil Code (2013. évi V. törvény a Polgári Törvénykönyvről) (1 July 2021), Section 4:191(1)(a) and Section 4:193(1) [Translated by Nemzeti Jogszabálytár], https://njt.hu/jogszabaly/en/2013-5-00-00 (last visited 15 September 2023).

Other such instances may exist within the civil legislation of various countries.

[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 29 September 2023).

[560] Haley Keltie: Sharenting and the (Potential) Right to Be Forgotten, Ind. LJ, 95 (2020), 1006.

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.[561]

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 also law enforcement officers were incompetent. The officers of the Royal Canadian Mounted Police (RCMP) suggested the deletion of Amanda Todd's Facebook account as a measure aimed at protecting her from the adverse outcomes associated with bullying and blackmail. Nevertheless, this proposition remains a cosmetic solution that neglects to address the underlying issue.[562] Indeed, the parents of Amanda strongly encouraged her to deactivate her Facebook account, a course of action she undertook for a duration of many months, but without yielding any favourable outcomes.[563] Amanda's response to the police officer's query about why she communicates with so many strangers online was heart-breaking: "I am lonely."[564]

Aydin Coban, a Dutch citizen, has been found guilty of engaging in child luring, child pornography, extortion, and harassment in relation to Amanda Todd. For a duration of three years, Coban engaged in persistent online harassment towards the girl, using a total of 22 different fake social media profiles. The individual employed coercion by issuing a threat to Amanda, wherein he asserted his intention to disseminate sexual visual content featuring her

[561] YouTube, Thesomebodytoknow channel: My story: Struggling, bullying, suicide, self-harm, available at: https://www.youtube.com/watch?v=vOHXGNx-E7E (29 September 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.
[562] 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 29 September 2023).
[563] 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 29 September 2023).
[564] 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 29 September 2023).

to her friends, family members, and school staff unless she consented to perform a so-called "show" for him in front of a webcam.[565]

During the period in question, Coban concealed his IP address and managed to evade arrest due to either insufficient technological capabilities or the negligence of law enforcement agencies.[566] A decade had elapsed following Amanda's tragic suicide, culminating in Coban being sentenced to a jail term of 13 years for his involvement in activities such as child luring, child pornography, extortion, and harassment. However, no formal charges were brought against him in connection with Amanda's death.[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] There may be potential ramifications within the fields of civil law or criminal law. However, as our thesis does not centre around these specific areas, we shall refrain from delving into the discussion of this matter within the framework of criminal and civil law.[569] Hence, ensuring the right to be forgotten remains crucial in enabling children to regain control over their personal data within the framework of our thesis.

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

---

[565] BBC News: Amanda Todd: Dutchman sentenced for fatal cyber-stalking (15 October 2022) https://www.bbc.com/news/world-us-canada-63218797 (last visited 15 September 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 29 September 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 15 September 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 29 September 2023).

[569] For example, the Hungarian Criminal Code has provisions for the imposition of penalties on those who possess pornographic recordings of individuals who are under the age of 18. The severity of the sentence would be heightened in cases when the child's age is below 12 years. Moreover, the imposition of sanctions is more severe than mere possession of the record, particularly if that individual distributes it to others, makes it accessible to a wider audience, or profits from its dissemination.
Act C of 2012 on the Criminal Code (Magyar Büntető Törvénykönyvről szóló 2012. évi C. törvény) (1 January 2023) Section 204(1)(a,b,c) and (2)(a) [Translated by Nemzeti Jogszabálytár], https://njt.hu/jogszabaly/en/2012-100-00-00 (last visited 15 September 2023).

online sharing activities and freedom of expression and children's right to a private life.[570] Accordingly, in this chapter, we will offer examples of child influencers and evaluate the 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.

6.1 How well do children understand the risks and consequences of losing control over personal data online?

Given the prevalence of computers and electronic devices in the lives of the current generation of children, commonly referred to as Generation Z, it is possible to suggest that they might possess a higher level of proficiency in utilising such technologies compared to their parents. They have been early adopters of several forms of technology, beginning use of computers, tablets, and smartphones. In recent years, it is possible that children have exceeded their parents' proficiency in operating these technological 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.[571]

[570] Stacey B. Steinberg: Sharenting: Children's Privacy in the Age of Social Media, Emory Law Journal 66, no. 4 (2017), 876-877.
[571] Sheila Donovan: 'Sharenting': The Forgotten Children of the GDPR, Peace Human Rights Governance 4(1), (2020), 43.

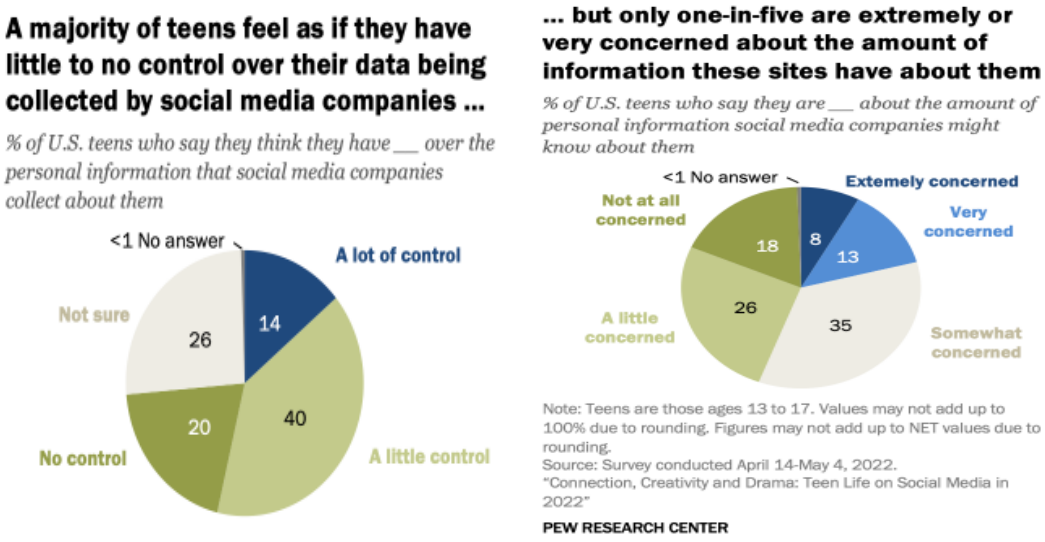


Chart 5 and 6: How much control teenagers have over their data and how much they worry about it[572]

According to a Pew Research Center study above, 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 claim that younger children are much more 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 study[573]:

[572] 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 29 September 2023).
[573] 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 29 September 2023).

"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 them[574]:

"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 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."[575] – 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

[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 29 September 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 29 September 2023).

and then it pops up as an ad for something else. It makes me a little uncomfortable almost."[576] – 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."[577] – 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."[578] – 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.[579]

Besides, empirical studies over past two decades has revealed a significant link between the usage of social media among teenagers and the development of negative body views. A study was conducted utilising a sample of 103 adolescent female students, ranging in age from 12 to 18 years (with a mean age of 15.4), who were selected from a public middle/high school located in the state of New York. This research investigated the association between

[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 29 September 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 29 September 2023).
[578] 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 29 September 2023).
[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 29 September 2023).

body image and the online activity of adolescent girls on the social media platform Facebook.[580]

The findings of the study reveal a positive correlation between the duration of time spent on Facebook participating in activities related to photos and increased levels of internalisation of the thin-ideal, self-objectification[581], dissatisfaction with weight, and aspiration for thinness.[582] Besides, another study conducted on female teenagers aged 10-19 in the US revealed a noteworthy association between self-objectification, disordered eating, and body shame.[583]

The eating disorders and phenomenon of body shaming might be linked to the culture of dieting and bodybuilding that is popular on various social media platforms. A study was undertaken to examine the influence of body shame on adolescents' use of social networking sites and their controlling of body image in the photographs they upload on these platforms. The study involved the participation of 693 Italian teenagers, with 45% of them being male. The average age of the participants was 16 years, with an age range spanning from 13 to 19 years. The findings of this research demonstrate a noteworthy correlation between feelings of body shame and the act of altering and manipulating photographs on social media platforms. Consequently, this relationship indirectly contributes to the development of problematic patterns of social media engagement among adolescent individuals, irrespective of their gender. In conclusion, while the correlation between body shame and problematic social media usage is more pronounced among female teenagers, the presence of similar

[580] Evelyn P. Meier and James Gray: Facebook photo activity associated with body image disturbance in adolescent girls, Cyberpsychology, behavior, and social networking 17, no. 4 (2014), 200.

[581] In accordance with the objectification theory, it is posited that individuals, particularly women, may progressively adopt an objectifying attitude towards themselves as a result of repeated instances of being viewed primarily as bodies. The process of internalising external standards of appearance and treating oneself as an object is commonly referred to as self-objectification.
Barbara L Fredrickson and Tomi-Ann Roberts: Objectification theory: Toward understanding women's lived experiences and mental health risks, Psychology of women quarterly 21, no. 2 (1997), 179-180.
"Self-objectification theory describes a two-step process where females are trained to objectify females in the media and then transfer this pattern inwards by taking an outsider's perspective on the physical self. The nature of FB photo sharing may expedite this process. Taking an outsider's perspective on the physical self is by definition the very purpose of publicly sharing photos on FB, and often the outsider's perspective is explicitly provided in the form of 'likes' or comments."
Evelyn P. Meier and James Gray: Facebook photo activity associated with body image disturbance in adolescent girls, Cyberpsychology, behavior, and social networking 17, no. 4 (2014), 202.

[582] Evelyn P. Meier and James Gray: Facebook photo activity associated with body image disturbance in adolescent girls, Cyberpsychology, behavior, and social networking 17, no. 4 (2014), 202.

[583] Kristen Harrison and Barbara L. Fredrickson: Women's sports media, self-objectification, and mental health in black and white adolescent females, Journal of Communication 53, no. 2 (2003), 228.

patterns among male adolescents implies a growing involvement in self-objectification experiences.[584]

Furthermore, one Instagram user reported seeing 33 Instagram stories from accounts she follows in addition to 14 advertisements, many of which focused on physical looks, within 2 minutes of watching Instagram stories.[585] Furthermore, in March of 2020, Instagram researchers posted on an internal message board that their survey data showed that 1/3 of the teenage girls who reported having body image issues felt worse after using Instagram.[586]

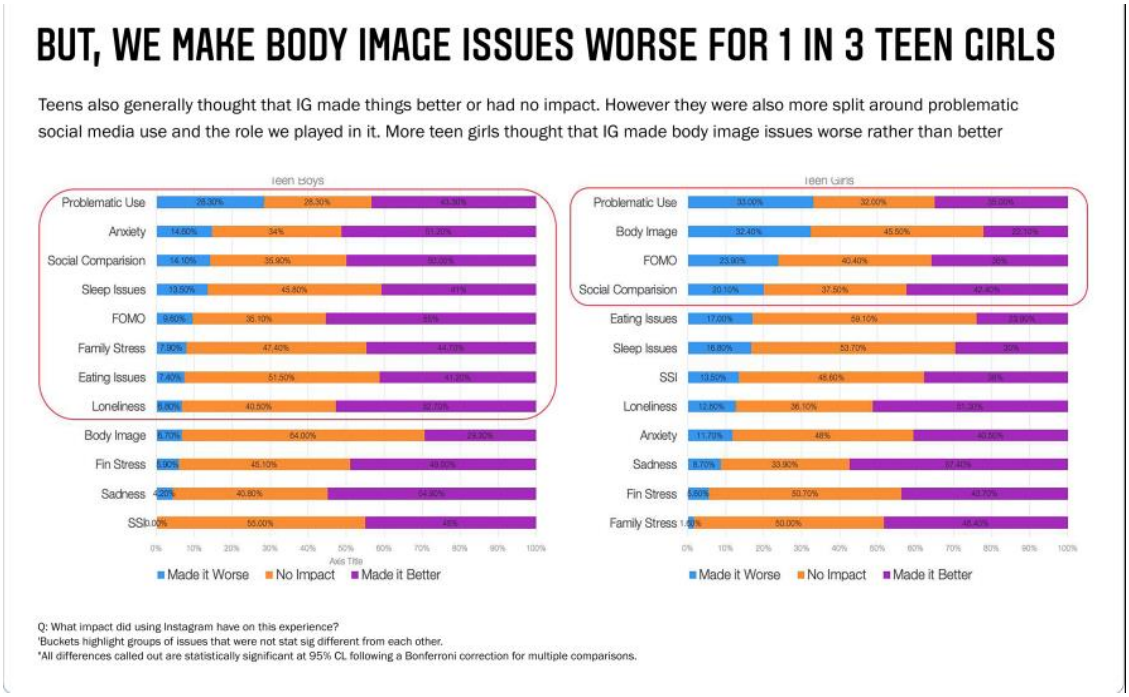


Chart 7: Slides from summary of Instagram's own research in 2019[587]

The aforementioned findings together suggest that children possess limited awareness of the consequences associated with relinquishing control over their personal data when utilising the Internet. They may also have a limited understanding of the level to which they can be used and manipulated by social media platforms, as well as by others who employ

[584] Francesca Gioia, Mark D. Griffiths and Valentina Boursier: Adolescents' body shame and social networking sites: The mediating effect of body image control in photos, Sex Roles 83 (2020), 773, 776 and 781.
[585] 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 29 September 2023).
[586] 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 29 September 2023).
[587] 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 29 September 2023).

harmful practices on these platforms, whether intentionally or unintentionally. Furthermore, many lack awareness of the various possible dangers that the Internet may provide, encompassing both mental and physical risks (Subsequent subchapters will go into a more comprehensive examination of these potential hazards). Consequently, it is imperative to provide children with adequate supervision and assistance in order to ensure their safe utilisation of the advantages offered by the online realm, while mitigating the risks associated with online manipulations.

6.2 To what extent are parents aware of the hazards to their children's privacy and data protection posed by the Internet?

It has been determined that children may exhibit a deficiency in comprehending the significance of their privacy and protecting of their personal data on the Internet. 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, the majority of parents do not perceive online marketing directed at their children as problematic and believe their children are not influenced. Despite the significant responsibilities imposed by the COPPA and the GDPR, many parents lack the necessary preparedness to protect their children's digital privacy. 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.[588]

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

[588] 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 29 September 2023).

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.[589]

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 freedom to receive and share information and ideas.[590] Regarding the US, the freedom of speech is guaranteed by the first amendment of the US Constitution.[591]

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.[592] 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.[593] The sharing of naked photographs and the most intimate moments of

[589] 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.

[590] 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."

[591] 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."

[592] 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."

[593] 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.

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 the 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 they had an interest in maintaining their private; yet they also accepted that the public had an interest in gaining knowledge about his life.[594]

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.[595]

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. A number of additional risks may be enumerated inside this subchapter.

First, 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

[594] Case 113 F.2d 806, Sidis v. F-R Pub. Corporation (No. 400), Judgment 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.

[595] 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.

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.[596] Moreover, it is possible that children may become victims of the organ black market, leading to the potential loss of crucial organs and posing a significant threat to their well-being. 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.[597]

Second risk may be 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.[598]

As a third risk, 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 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.[599] If we consider individuals over 30 years old, their

[596] 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.
[597] Stacey B. Steinberg: Sharenting: Children's Privacy in the Age of Social Media, Emory Law Journal 66, no. 4 (2017), 849.
[598] 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.
[599] 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.

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.[600] 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.[601]

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. Instances of humiliating incidents or disgraceful offenses, specifically, might serve as key elements in the act 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.[602]

Yet, the practises and the tables below 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.[603]

[600] Stacey B. Steinberg: Sharenting: Children's Privacy in the Age of Social Media, Emory Law Journal 66, no. 4 (2017), 849-850.
[601] 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 29 September 2023).
[602] Neil M. Richards: The dangers of surveillance, Harvard Law Review 126, no. 7 (2013), 1952-1958.
[603] 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 29 September 2023).

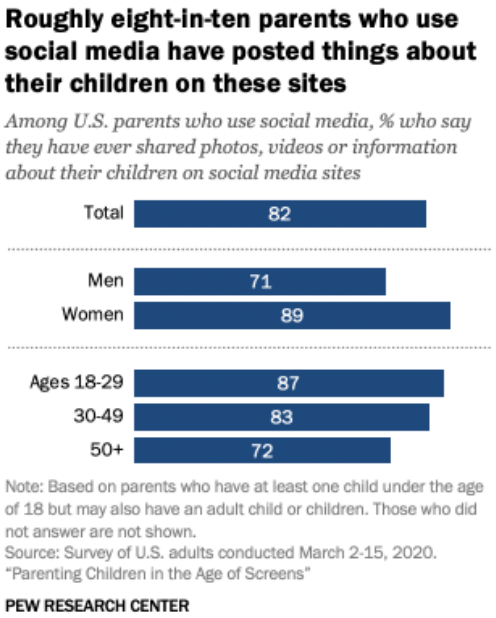


Chart 8: Parents who share information about their children[604]

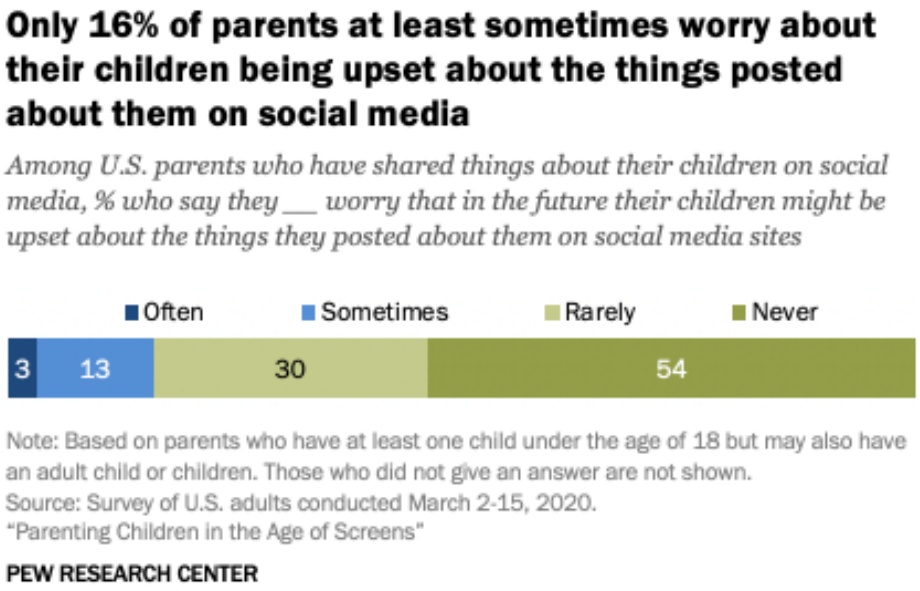


Chart 9: Parents worry about their children being upset about the information they posted about them on social media[605]

[604] 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 29 September 2023).

[605] 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 29 September 2023).

In Subchapter 6.1, we have 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. Therefore, parents should take responsibility for their children's digital privacy and data protection rights, as required by the GDPR, the 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, as shown in Chart 9 and 10? In this scenario, we suggest that the laws 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.[606]

Indeed, social networking platforms have made some progress in restricting some content pertaining to children, and they have already taken steps to remove some restricted content relating to children (we will examine those solutions in detail in the Subchapters 6.4 and 6.5). We assume that if the COPPA and the 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 should restrict even more.[607]

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

[606] 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).

[607] The Digital Services Act imposes restrictions on some types of information pertaining to children, including targeting materials associated with child sexual abuse and child pornography. However, in our perspective, these restrictions are not enough and should be more extensive. Social media platforms impose restrictions on various types of content beyond child sexual abuse, which we will discuss in Chapter 6 of this thesis. In our point of view, lawmakers should adopt a proactive approach rather than falling behind social media platforms. Lawmakers should take the initiative to assert a greater influence over these platforms by implementing stricter enforcement measures. Currently, the Digital Services Act (DSA) does not seem to have a significant impact on the stringency and effectiveness of regulations governing social media platforms. However, a more precise evaluation may be conducted after its implementation in the Member States starting in February 2024.
Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) OJ L 277, 27.10.2022, pp. 1–102, Recitals 12, 61, 64, 80 and 119.

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.[608]

6.3 Children's right to self-determination and the conflict between parental freedom of speech and the right of children to privacy and data protection

In Europe, the German Federal Constitutional Court was the first to enunciate the concept of informational self-determination.[609] Afterwards, it became one of the foundational pillars of Article 8 of the CFR's right to protection of personal data.[610] Finally, it is consistent with the spirit of the GDPR, which offers people more control over their data[611], for example by assuring the rights to access, rectify, delete, and object. In addition, the duties imposed by the GDPR on data controllers, such as notifying the subject and obtaining consent, would be also based on the right to informational self-determination.[612]

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 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.[613] Obviously, this right is not absolute; as children

---

[608] 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 29 September 2023).

[609] BVerfG, Order of the First Senate of 15 December 1983 - 1 BvR 209/83 -, paras. 1-214, BVerfGE 65, 1 - 71 Volkszählung.

[610] 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."
Charter of Fundamental Rights of the European Union, OJ C 326, 26.12.2012, p. 391-407, Article 8(2).

[611] GDPR, Recital 7: "[…] Natural persons should have control of their own personal data. […]".

[612] 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.

[613] For more information about the data protection and privacy rights of children and their parents see the Chapter 4 of this thesis.

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 from 13 to 16 under the GDPR.[614] 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.[615]

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.[616]

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."[617] Moreover, the Recital (65) stipulates as follows:

---

[614] GDPR, Article 8 and 16 CFR COPPA 312.2 “Child”.

[615] 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.

[616] 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, 104407.

[617] GDPR, Article 17(1).

> "[...]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. [...]"[618]

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,[619] 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.[620] 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.[621] After this decision, J.K. Rowling and her husband filed an appeal, which the Court of Appeal allowed it on the grounds that:

> "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

[618] GDPR, Recital 65.
[619] GDPR, Article 17(3)(a).
[620] Case EWCA Civ446, Murray v Express Newspapers plc and another, Judgment of the Court of Appeal, England and Wales, 7 May 2008, 481.
[621] Case EWCA Civ446, Murray v Express Newspapers plc and another, Judgment of the Court of Appeal, England and Wales, 7 May 2008, 512, para 62.

> 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."[622]

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.[623] 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.[624]

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. The non-absolute nature of this right is evident when considering that, if a user downloads child-related material, no one else has the authority to erase this information until the user chooses to remove 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.[625]

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 material they uploaded.[626] However, the COPPA does not provide children with the right to

---

[622] Case EWCA Civ446, Murray v Express Newspapers plc and another, Judgment of the Court of Appeal, England and Wales, 7 May 2008, 485.
[623] Case EWCA Civ446, Murray v Express Newspapers plc and another, Judgment of the Court of Appeal, England and Wales, 7 May 2008, 512, para 62.
[624] 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 29 September 2023).
[625] 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 29 September 2023).
[626] James Lee: SB 568: Does California's Online Eraser Button Protect the Privacy of Minors, 48(3) U.C. Davis Law Review (2015), 1203.

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.[627] 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.[628]

6.4 Manifestation of parental sharing restrictions on social media in practise

The COPPA and the GDPR 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. However, in order to ensure the privacy of children, social media platforms have implemented privacy policies that restrict adults from sharing specific content pertaining to children. We will start our discussion by examining the YouTube restriction policies pertaining to content that is targeted toward 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.[629]

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.[630] YouTube's enforcement team may

---

For further information see the Online Eraser Button Law: S.B. 568, 2013 LEG. 2013-14 SESS. (Cal. 2013), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568 (last visited 29 September 2023).

[627] 16 CFR COPPA Part 312.4(d)(3).

[628] 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.”

[629] 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 16 September 2023).

[630] 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%A

initially provide a warning; if the behaviour persists, they may issue a strike; if 3 strikes are issued, they may terminate the channel; and if they believe a child is in danger based on reported content, they will assist law enforcement in investigating the content.[631]

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 37th 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.[632] 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? In actual fact, the GDPR and the 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

1ros-tartalom%2Ckiskor%C3%BAakat-megc%C3%A9lz%C3%B3-tartalom%2Ccontent-featuring-minors (last visited 16 September 2023).

[631] 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 16 September 2023).

[632] YouTube, Newsnercom channel: Barber Pranks Kid By Pretending He's Cut His Ear Off, https://www.youtube.com/watch?v=0TSNKp4Xs0U (last visited 29 September 2023).

permission.[633] Law enforcement is effective if there is a significant public response, as in the 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.[634] 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.[635] 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

[633] 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 16 September 2023).
[634] 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 16 September 2023).
[635] 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 16 September 2023).

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 accessible on YouTube for more than five years without any restrictions and has received approximately fifteen million views.[636]

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."[637]

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."[638]

---

[636] YouTube, Storyhive Channel: Yoga for Kids! https://www.youtube.com/watch?v=X655B4ISakg (last visited 16 September 2023).

[637] 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 16 September 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.

[638] 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 16 September 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.

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.[639] Hence, they should be concerned 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.[640]

Furthermore, the Instagram Community Guidelines explicitly prohibit, for instance, the sharing of nudity.[641] 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.[642]

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.[643]

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

---

[639] 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 16 September 2023).

[640] 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.

[641] Instagram, Help Centre, Community Guidelines, https://help.instagram.com/477434105621119/?helpref=uf_share (last visited 16 September 2023).

[642] 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 16 September 2023) cited in Stacey B. Steinberg: Sharenting: Children's privacy in the age of social media, Emory LJ 66 (2016), 847.

[643] Instagram, Kids Diana Show (image posted on 21 August 2021) https://www.instagram.com/p/CSeZgdHjkVF/?hl=tr (last visited 16 September 2023).

children.[644] Besides, in accordance with current law[645], they report instances of child sexual exploitation to the National Center for Missing and Exploited Children (NCMEC).[646]

The suggestions provided by Facebook about prohibited content pertain to instances of child sexual exploitation and the solicitation of sexual material, encompassing both actual and fictitious children, including the sharing of nude photos. Moreover, the aforementioned suggestions may involve information pertaining to non-sexual abuse of children. In addition to instances of physical abuse, it is important to acknowledge that this may cover emotional and psychological forms of abuse. Engagement in inappropriate interactions with children is likewise prohibited. This form of online communication could consist of obtaining sexual material from children through private chat, as well as arranging in-person meetings for the purpose of forcing children into sexual acts. The act of sextortion and the dissemination of exploitative personal photos are also forbidden. This sort of online conduct includes the act of pressuring children into offering monetary resources, favours, or intimate material using threats to reveal intimate images or associated private data belonging to the children in question.[647]

While implementing a complete ban on parental sharing may not be a feasible approach, it is imperative to consider the implementation of some legislative restrictions, as previously indicated. In this manner, social media platforms would possess a basis and structure upon which to enhance their privacy policies. To emphasise again briefly, allowing only modest family images that do not reveal any personal information to others, posting photos of children fully from behind, concealing their facial features, or placing emojis on their faces may be acceptable.[648]

---

[644] Meta, Facebook Community Standards, https://transparency.fb.com/en-gb/policies/community-standards/?source=https%3A%2F%2Fwww.facebook.com%2Fcommunitystandards (last visited 16 September 2023).

[645] 18 U.S.C. 2258A (2011) (Reporting requirements of electronic communication service providers and remote computing service providers) (a).

[646] Meta, Facebook Community Standards, Child sexual exploitation, abuse and nudity, Policy rationale, https://transparency.fb.com/en-gb/policies/community-standards/child-sexual-exploitation-abuse-nudity/ (last visited 16 September 2023).

[647] Meta, Facebook Community Standards, Child sexual exploitation, abuse and nudity, Policy rationale, https://transparency.fb.com/en-gb/policies/community-standards/child-sexual-exploitation-abuse-nudity/ (last visited 16 September 2023).

[648] 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 16 September 2023).

6.5 Social media solutions against threats to children's privacy and protection of personal data in light of current technology

Children's internet safety should be handled differently than adults' since they are more vulnerable and lack discernment. They may experience threats that adults are unlikely to encounter. Even in such situations, adults have the ability to stand up for their rights. Children, on the other hand, lack the necessary tools to combat difficulties, particularly at younger ages. For example, if an adult encounters a predator and discovers that his/her naked images are being disseminated, they may contact the police and sue the individual immediately. They may also be cognitively more prepared to deal with the emotional consequences of such violations.

However, if children are being exploited online by predators, they may not even be aware of such violations or the repercussions of such malevolent behaviours, let alone claim their rights to privacy and data protection. Thus, it is critical that violations are avoided before they occur.

Given that there is no instructions or restrictions in the GDPR requesting data controllers to develop solutions specifically for children's online safety, social media platforms would do so on their own, considering the threats of present practise and using current technology. This subchapter will cover some of the current technological solutions used by social media providers.

For example, Instagram claims that they encourage users under 18 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.[649] The automated selection of a safer alternative for teenagers is advantageous due to the correlation between the level of accessibility of an account and the increased likelihood of encountering hate speech, bullying, condemnation, and severe criticism.

Moreover, marketers may only target users under 18 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.[650] It would be ideal, in our view, not to even allow the marketers to target their location, age, or

[649] 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 16 September 2023).
[650] 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 16 September 2023).

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. In accordance with our viewpoint, the Digital Services Act (DSA), which will be implemented in the EU from February 2024, prohibits online service providers from displaying targeted advertising on their platform using profiling techniques if they have reasonable assurance that the recipient is a minor.[651]

Research on children's comprehension of advertising indicates that children between the ages of 3 and 7 possess the ability to differentiate between advertisements and content. As an illustration, a child may assert that the advertisements are shorter compared to the relevant content. However, they lack the understanding that the primary purpose of these commercials is to encourage the acquisition of a product or service. Children between the ages of 7 and 11, with the assistance of their families and educational institutions, begin to develop an awareness of bias and deception within advertisements, while also gaining an understanding of the persuasive nature inherent in advertising. Nevertheless, there is a deficiency in their understanding of the fundamental principles behind advertising, including its nature and operational mechanisms, as well as the many approaches and strategies employed in advertising campaigns. Teenagers aged 12 and above shown the ability to recognise advertisements, discern the underlying intentions of advertisers to influence behaviour, and recognise particular advertising methods and appeals. Nevertheless, even while teenagers aged 12 and older may acknowledge the presence of persuasive intentions, it does not imply that they are impervious to marketing tactics, particularly when very enticing items are involved.[652]

The findings of this study pertain specifically to conventional advertising methods, such as television advertisements, and do not encompass emerging marketing strategies like influencer marketing and sponsored content on social media platforms. For instance, the utilisation of widely popular unpacking and toy-play videos[653], along with influencers

[651] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) OJ L 277, 27.10.2022, pp. 1–102.
Article 93 of the DSA: "This Regulation shall apply from 17 February 2024."
The DSA currently lacks a precise determination of the age threshold that designates an individual as a minor.
[652] Deborah Roedder John: Consumer socialization of children: A retrospective look at twenty-five years of research, Journal of consumer research 26, no. 3 (1999), 183-213.
[653] Some examples are presented below:

providing reviews or demonstrations of sponsored items, might be more efficacious in comparison to traditional television commercials.[654] This phenomenon may be attributed to the facilitation of direct contact through social media platforms, wherein influencers have the ability to immediately respond to comments from their followers. Consequently, this interaction fosters the development of a "parasocial relationship"[655] with the influencers. This phenomenon leads individuals to perceive influencers as peers or friends rather than just promoters of things. In this manner, individuals, including both children and parents, have the chance to cultivate trust and establish the reliability of influencers, operating under the assumption that influencers would only promote a product if they genuinely had a favourable opinion of it.[656]

According to Instagram's policies, once individuals begin following influencer accounts and engaging with related information, the algorithms employed by social media platforms ensure that such content continues to appear in their newsfeeds. For instance, Instagram provides suggestions to its users in order to facilitate their exploration of new communities and content. Instagram has the capability to suggest content and profiles that users do not already follow. The process of personalising content for Instagram users involves the generation of individualised recommendations for each person, utilising artificial intelligence (AI) and machine learning (ML) techniques. For instance, when toddlers engage with toy-play videos on Instagram, the platform may then suggest material related to toy reviews, unboxing videos, and similar genres.[657]

YouTube, Ryan's World Channel: Christmas Morning 2016 Opening Presents with Ryan ToysReview, https://www.youtube.com/watch?v=WyOkjW5FqBU (last visited 24 September 2023).
YouTube, Vlad and Niki's Channel: Vlad and Nikita play with Toy Cars - Collection video for kids, https://www.youtube.com/watch?v=NtzftGb0EcM (last visited 24 September 2023).

[654] Jenny Radesky, Yolanda Linda Reid Chassiakos, Nusheen Ameenuddin, and Dipesh Navsaria: Digital advertising to children, Pediatrics 146, no. 1 (2020), 2.

[655] "The viewer may develop a one-sided or parasocial relationship (PSR) with the influencer, a term that describes an emotional connection felt by the viewer for the influencer, in which the influencer is perceived as more of a peer or friend. Youth who follow social media personae and have received responses from the influencer have even stronger perceived relationships with the influencer."
Yolanda N. Evans: One-sided social media relationships and the impact of advertising on children, Pediatrics 146, no. 5 (2020), 1.

[656] Yolanda N. Evans: One-sided social media relationships and the impact of advertising on children, Pediatrics 146, no. 5 (2020), 1-2.

[657] Instagram Help Centre, Recommendations on Instagram, https://help.instagram.com/313829416281232/?helpref=uf_share (last visited 24 September 2023).
Meta AI, Powered by AI: Instagram's Explore recommender system (25 November 2019), https://ai.meta.com/blog/powered-by-ai-instagrams-explore-recommender-system/ (last visited 24 September 2023).

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 18.[658] This change is intended to provide a more inclusive approach in the absence of a standardised age of digital consent among Member States. 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.

As mentioned earlier, the regulatory frameworks governing Facebook and Instagram demonstrate similarities as they are both under the umbrella of Meta. As stated by the Meta Safety Centre, the platform places clear emphasis on proactively avoiding damage from occurring in the first place. This is achieved by the implementation of zero-tolerance rules and the state-of-the-art preventive measures. The company makes a commitment to promptly remove any nude images of children, regardless of the initial intent for their sharing. This proactive approach is motivated by the recognition that such images possess the potential to be exploited or misused by others.[659]

In one of our recent papers, we recommended that AI and 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."[660]

---

[658] 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 16 September 2023).

[659] Meta, Safety Centre, Online Child Protection, https://about.meta.com/actions/safety/onlinechildprotection (last visited 16 September 2023).

[660] 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 29 September 2023).

Indeed, Facebook and Instagram has begun employing these technologies to detect and remove shared harmful data in a manner similar to our earlier recommendation.[661] However, it would have been ideal if they 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. Therefore, it would be ideal to employ AI and ML to identify inappropriate data and prohibit its sharing before it reaches other users.

From 2018 through 2023, the Chart 8 below displays the total amount of relevant content deleted by Facebook due to their association with child nudity and sexual exploitation. During the second quarter of 2021, Facebook saw a significant increase in the volume of material pertaining to child exploitation that was removed, which may be attributed to the implementation of a modified detection system, as seen in the chart.[662]

Besides, it is visible that there was a decline in the removal of Facebook material related to child sexual exploitation, child nudity, and physical abuse during the first quarter of 2023. The downward trend persisted throughout the second quarter of 2023. Currently, the average number of removals seems to have returned to pre-system change levels seen before to the implementation of the system modification in the second quarter of 2021.

[661] Meta, Online Child Protection: Tools and Technology https://about.meta.com/actions/safety/onlinechildprotection (last visited 25 September 2023).
[662] Meta, Community Standards Enforcement Report, Second Quarter 2021 (18 August 2021), https://about.fb.com/news/2021/08/community-standards-enforcement-report-q2-2021/ (last visited 4 October 2023).

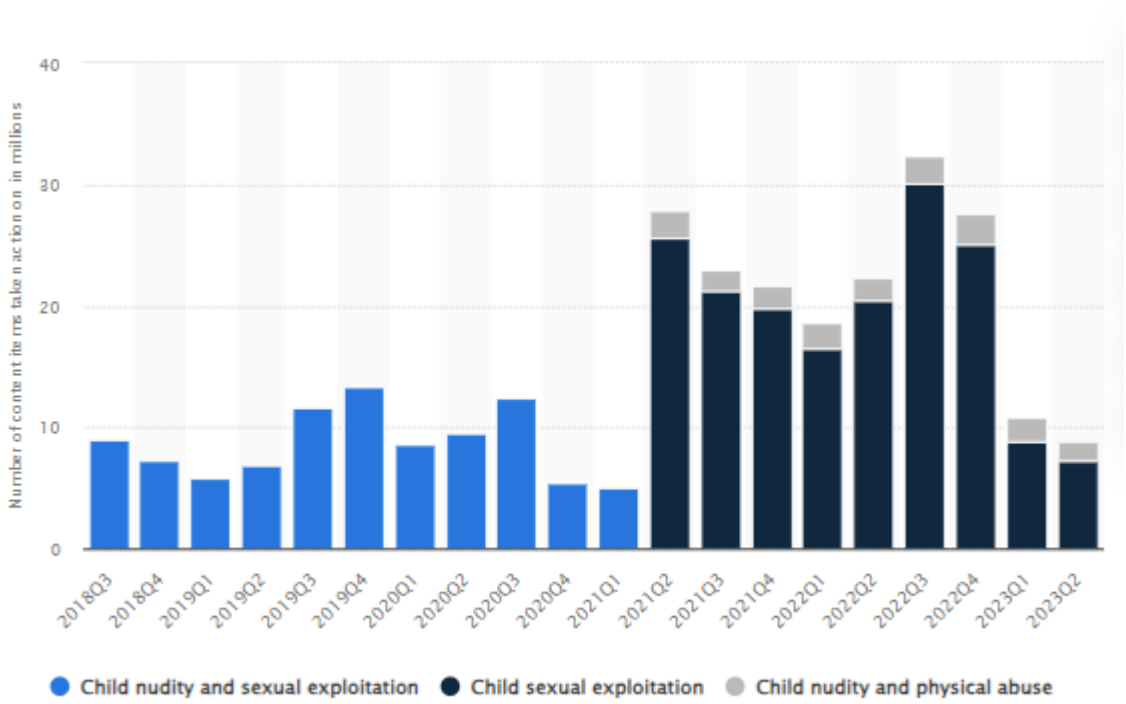


Chart 10: Global number of child nudity and sexual exploitation-related content items removed by Facebook from 2018 to 2023 (in millions)[663]

There might be underlying factors contributing to the notable increase seen after the change of tracking the relevant consent in the second quarter of 2021, as well as the following decrease observed from the first quarter of 2023. It is reasonable to assume that the improved ability of Facebook to identify and eliminate such data, together with the notable rise in the quantity of erased data, stems from the progressions achieved in its own technology and tools. Facebook's proactive strategy, which involves taking action without relying only on user reports to address improper content, represents a notable advancement.

However, the use of AI solutions by Facebook may lead to mistakes and excessive identification of innocent material, including situations when parents share private content of their children for their best interests. Later in this subchapter, we will discuss relevant and specific real-life examples to illustrate this point. The primary cause of this issue may be due to the limitations of existing AI technologies. The significant decline seen in 2023 might be attributed to the heightened vigilance of reviewer teams of Facebook after becoming aware

[663] Statista, Global number of child nudity and sexual exploitation-related content items removed by Facebook from 3rd quarter 2018 to 2nd quarter 2023 (in millions), https://www.statista.com/statistics/1013776/facebook-child-exploitation-removal-quarter/ (last visited 29 September 2023).

of instances when AI systems produced excessive false alarms due to the limitations of current detection methods.

Google also combats child sexual abuse via the use of technical solutions. (The YouTube platform is subject to the same requirements since it is a product of Google.[664]) Google utilises two primary solutions: hash matching and AI. Hash matching involves the process of assigning distinct digital signatures, referred to as "hashes," to photos and videos. These hashes are then compared to a pre-existing database of recognised signatures. When the two items are identical or exhibit significant resemblance, the content is said to be equivalent or nearly analogous. The hashes are acquired from reputable entities such as the Internet Watch Foundation (IWF) and the National Centre for Missing and Exploited Children (NCMEC). Hash matching is a technique used to identify pre-existing instances of child sexual abuse material. In conjunction with this, artificial intelligence is utilised to detect novel content exhibiting striking resemblances to established patterns of proven child sexual abuse material. A group of skilled individuals is assigned to examine and assess every newly identified picture, ensuring its classification as child sexual abuse material before it is reported. As mandated by US legislation, following this review, the team notifies NCMEC of any images designated as containing sexually abusive material involving children.[665] The National Centre for Missing and Exploited Children (NCMEC) thereafter assesses the submitted report and may choose to direct the matter to an appropriate law enforcement entity.[666]

However, as this technology is new and not flawless, controls should be in place. In some circumstances, mistaken assumptions may cause major issues when attempting to safeguard children. For example, a father recently took images of his child's groin since the child had a medical concern and wanted to submit these photos to the doctor on the advice of their healthcare provider. The doctor detected the problem using the images and recommended antibiotics, which rapidly resolved the medical condition. However, Mark, the father who would like to be called only by his first name, encountered serious troubles

[664] See the list of products owned by Google:
Google, Products, https://about.google/products/ (last visited 25 September 2023).
[665] 18 U.S.C. 2258A (2011) (Reporting requirements of electronic communication service providers and remote computing service providers) (a).
[666] Google, Safety and Security, How we detect, remove and report child sexual abuse material, Susan Jasper (28 October 2022), https://blog.google/technology/safety-security/how-we-detect-remove-and-report-child-sexual-abuse-material/ (last visited 25 September 2023).

following the detection of hazardous content concerning child sexual abuse and exploitation by an AI tool of Google.[667]

Mark realised it was due to his son's infection, but it was too late because all his Google accounts involving Google cloud, Gmail, Google Calendar, and Google Fi had already been disabled. The San Francisco Police Department already begun an investigation after Google's review team detected a video he shot with his son and unclothed wife in their bed. Mark received a letter from the San Francisco Police Department in December 2021. It included a letter notifying him that he was being investigated, as well as copies of the search warrants executed on Google and his internet service provider.[668]

In the report, the investigator, Nicholas Hillard, stated, "I determined that the incident did not meet the elements of a crime and that no crime occurred."[669] Despite the fact that law enforcement acquitted Mark, he was still unable to access his account or material on Google accounts since a Google spokesperson stated that they stick to their decision due to the zero-tolerance policy against this content.[670]

On the one hand, we believe that Google's cooperation with law enforcement may be critical and beneficial to children's online safety. One the other hand, if the review teams of technology companies or investigators are not cautious, it may cause some major challenges, and in the worst circumstances, some parents may lose custody. In the present conditions, it is inevitable that human involvement is necessary. Nevertheless, it is crucial that companies shall be highly finicky in their decisions when they are assigning experts to

[667] The New York Times, A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal, Published 21 August 2022, Updated 21 June 2023, https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html (last visited 29 September 2023).
[668] The New York Times, A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal, Published 21 August 2022, Updated 21 June 2023, https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html (last visited 29 September 2023).
[669] The New York Times, A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal, Published 21 August 2022, Updated 21 June 2023, https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html (last visited 29 September 2023).
[670] The New York Times, A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal, Published 21 August 2022, Updated 21 June 2023, https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html (last visited 29 September 2023).

such reviewing teams. Hence, in such delicate issues, service providers should make the process simple for data subjects to challenge even the final decisions of review teams.[671]

Carissa Byrne Hessick, a law professor at the University of North Carolina who is specialised in child pornography crimes, has remarked that it is critical that technology firms provide information to law authorities in order to combat child sexual abuse. She does, however, say that there should be an opportunity for corrections.[672]

After all, Mark's is not the only example. Similar incidents exist, such as the one that occurred in Texas. Cassio, who also likes to be named only by his first name, photographed his son's infected intimates at his paediatrician's request. He then sent them to his wife using Google's chat service. Google photos was also used to preserve the images. His Gmail account was similarly disabled, and he was in the midst of purchasing a home at the time. His mortgage broker was sceptical when Cassio suddenly wanted to alter his mailing address until the real estate agency vouched for him.[673]

There might be countless additional cases like this all throughout the world. Obviously, not all naked children's images are child pornography. However, parents should exercise extreme caution since once it is collected and stored in the cloud, it may be accessed on the Internet by malevolent individuals. Sharing those images for health reasons, in our view, is also not very prudent, although in exceptional circumstances, such as pandemic periods, it may be acceptable.

As AI and ML improve, there may be certain modifications and a reduced need for humans to participate in assessing shared information. Nonetheless, given the current circumstances, it is evident that the AI may make mistakes, and well selected review teams and investigators may be of great assistance, particularly in situations involving law enforcement. Furthermore, as the GDPR currently grants data subjects the right not to be subject to a decision based only on automated processing, compliance with the Regulation's

---

[671] ICO, Rights related to automated decision making including profiling, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/rights-related-to-automated-decision-making-including-profiling/ (last visited 29 September 2023).

[672] The New York Times, A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal, Published 21 August 2022, Updated 21 June 2023, https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html (last visited 29 September 2023).

[673] The New York Times, A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal, Published 21 August 2022, Updated 21 June 2023, https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html (last visited 29 September 2023).

requirements in its current version would necessitate human intervention and simple mechanisms to object their final decisions.[674]

6.6 Long-term solution for protecting children's privacy and data protection in practice

In addition to the legal and technological 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.[675]

When addressing data and privacy literacy, it is important to consider three distinct aspects of privacy: interpersonal privacy, which involves an individual's digital footprint; institutional privacy, which concerns the collection of information by governments or public authorities; and commercial privacy, which relates to how businesses utilise personal information for marketing purposes.[676]

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.[677]

The study conducted by *Livingstone et al.* (2020) 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, 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

[674] GDPR, Article 22(1).
[675] 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.
[676] 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.
[677] 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.

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.[678]

An overview of the research is provided in the table below:

Ages of children	Interpersonal privacy	Institutional and commercial privacy
5-7	• 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	• 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

[678]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), 416.

8-11	• Starting to understand the risks of sharing, but generally trusting • 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	• Still little research available • 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
12-17	• Online as "personal space" for expression, socializing, learning • 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	• Privacy tactics focus on online identity management, not data flows (see data as static and fragmented). • 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 3: Children's data and privacy literacy[679]

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.[680] Dual-meaning online interactions are not only perplexing for children, but also for the parents who should be guiding their children.[681]

[679] 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.
[680] "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 29 September 2023).
[681] 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	• 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	• 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	• 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	• 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)

	• Why reporting stuff is so hard • Why they make mistakes about who you are	
13-14	• 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	• 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	• 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	• 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 4: Children's views of how their data and privacy online should be addressed (entries paraphrased and summarized by the authors)[682]

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. This understanding stems from their prior experiences of doing searches and then receiving targeted adverts. 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.[683]

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.

Additionally, based on the findings of Table 3 above, the children aged 15 to 16 made very impressive statements about what they believe companies should do differently, such as improving age restrictions, disclosing the information they have about the data subjects, safely storing data with sensitive nature, and upholding the data minimisation principle. Furthermore, teenagers aged 12-17 are aware of "data traces" (e.g., advertisements) and

[682] 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.
[683] 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.

device monitoring (e.g., location), but are less personally worried or aware of potential ramifications according to the findings in Table 2 above. Nonetheless, given that their understanding is greater than that of younger children, children who are in their adolescent years should benefit most from education on media literacy.

Accordingly, we consider the age of 16 adopted by the GDPR as the uniform age for digital consent across the EU is appropriate, since studies show that children at this age are capable of comprehending the consequences of their online behaviour. If these children are sufficiently taught media literacy at the age of 16, they will gain even more knowledge to the point where they may be considered fully competent. Furthermore, the age of 16 would be consistent with the consent ages indicated in Subchapter 3.3 for other legal disciplines and situations, such as medical treatment or sexual activity.

However, in order to avoid the existing lack of consistency across EU Member States regarding the age of digital consent, we believe that the clause in Article 8 of the GDPR stating that Member States may provide through legislation for a lower age not less than 13 years should be removed. Even further, considering the aforementioned findings, it would be ideal for the COPPA to increase the age requirement from 13 to 16. The mentioned change would provide an enhanced level of protection for teenagers and promote the harmonisation between the EU and the US.

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."[684] 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."[685]

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."[686]

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

[684] 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.
[685] 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.
[686] 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.

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.[687]According to considerations mentioned above, it is not unexpected that people, especially parents and teachers, believe they are falling behind in adoption and utilisation of emerging technologies.[688]

The overall findings of this thesis indicate that both parents and children often lack a comprehensive understanding of the significance of privacy and data protection, as well as the potential hazards associated with relinquishing control over children's data. Moreover, individuals lack a comprehensive understanding of how to effectively exercise their rights pertaining to privacy and data protection. Additionally, there is a lack of sufficient guidance on the relevant legislation. Furthermore, the GDPR does not adequately include the responsibilities of data controllers when it comes to the processing of personal data belonging to children. The COPPA, on the other hand, entails distinct responsibilities that primarily focus on parental involvement in data management, rather than granting children autonomy over their own information wherever feasible.

Hence, we propose that legislators should include privacy and data protection rights within the authority of children, with the provision that children may use these rights with the assistance of their parents if needed. Additionally, duties should be imposed on data controllers to facilitate direct contact with children once they have reached a level of maturity deemed appropriate. Moreover, legislative measures should be implemented to impose more stringent regulations on shared material pertaining to children, serving as a prompt resolution instead of overreliance on parental authority. Furthermore, these restrictions would necessitate social media sites to enhance their privacy practices in relation to potentially harmful or sensitive information pertaining to children.

Governments and other stakeholders must also take responsibility and make more investments to help parents and teachers improve their digital skills. This would enable them to effectively facilitate children's educational development and progress within the context

[687] 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.
[688]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.

of the digital age.[689] 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 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. Due to their prominent positions in data protection and privacy, these jurisdictions are likely to set a precedent for legal systems worldwide, with their exemplary legislative standards and instructional methods.[690]

6.7 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 the 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

[689] 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, Berkman Center research Publication (2015), 26-29.
[690] 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 29 September 2023).

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 subject to judicial consideration. In situations where there is a clash between the parents' freedom of expression and the children's right to privacy, the courts should prioritise the protection of the children's rights 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.

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 the GDPR and the COPPA should be reformed to 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 also emphasised that certain photographs shot from behind, blurred images, or the insertion of emojis to the children's faces may 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.

7. 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.

The backdrop of the GDPR and the COPPA has been explained in Subchapter 2.1, accompanied by an examination of the provisions that necessitate enhancement. 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 clauses [691]) and entirely applicable in all Member States upon its entry into force.

[691] "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

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.

In Subchapter 2.2, the significance of the free movement of personal data across the Atlantic between the EU and the US was analysed, as it is a fundamental element of the transatlantic digital economy and cooperation. 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. It was highlighted that both the EU and the US are unable to impede the transfer of personal data across the Atlantic, irrespective of their distinct privacy and data protection approaches. Due to the US being the EU's primary commercial partner and being the most globally integrated economy, this relationship has significant importance. Consequently, over an extended period, they have engaged in negotiations to establish accords that facilitate the unrestricted movement of data.

In Subchapter 2.2.1, we have conducted a comprehensive analysis of the Safe Harbour, Privacy Shield, and the new EU-US Data Privacy Framework, with a particular focus on their historical context. The examination of the Schrems I and II cases aimed to gain insights into the termination of the Safe Harbour and Privacy Shield by the CJEU. Furthermore, an analysis has been conducted on the outstanding matters pertaining to the recently implemented EU-US Data Privacy Framework.

The disparity in proportionality methods between the EU and the US over the intelligence services' access to personal information and bulk collection continues to be the foremost challenges within this framework. Max Schrems has already said that they have made preparations for the third round of proceedings before the CJEU. It is also our expectation that the CJEU is likely to declare the third transatlantic data transfer solution invalid, primarily owing to the unsolved matter of surveillance. In order to establish the US as a jurisdiction that offers a satisfactory degree of data protection compared to the EU, it is imperative to undertake necessary reforms pertaining to the FISA Section 702. These reforms should specifically address surveillance practises concerning individuals who are not citizens of the US.

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.

This chapter contributes to the literature by tracing the origins of the COPPA and Article 8 of the GDPR and investigating the historical context of transatlantic data transfers. We also compared the different approaches to privacy and data protection on both sides of the Atlantic. Besides, we have provided an overview of the strengths and drawbacks inherent in both legislations.

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 legislations, 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.

> Accordingly, we discussed the findings of the study completed by *Livingstone et al. (2020)* pertaining to the online data and privacy of children in the digital era in Chapter 6. This analysis is also evaluated with the information shown in Table 1 under

Subchapter 3.3, which outlines the varying ages of consent across different areas within the Member States. It has been determined that individuals between the ages of 15 and 16 exhibit the highest level of awareness regarding the potential ramifications of their online actions. Furthermore, they possess a greater aptitude for digital media literacy and demonstrate an inclination to inquire about the data processing practices employed by online service providers. These inquiries often relate to the adherence of mentioned providers to legal principles such as data minimization and purpose limitation (while the teenagers may not use precise legal terms, the intended message remains unchanged.) Moreover, the age of 16, as set by the GDPR, aligns with the ages of consent established in other fields, such as consent for medical treatment, working part-time, and sexual intercourse. Hence, it is deduced that the age threshold of 16, as established by the GDPR, may be considered suitable. However, it is recommended that the phrase in Article 8 of the GDPR, which allows Member States to reduce the age threshold to 13, be eliminated due to the resulting lack of uniformity among the Member States. Current studies also indicate that children aged 13 exhibit distinct differences, which are disadvantageous, in their level of awareness and comprehension compared to children aged 16.

In addition, according to our perspective, it would be ideal if the COPPA were to raise the age criterion from 13 to 16. This proposed amendment would offer a higher level of protection for teenagers and foster the alignment between the EU and the US.

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.

We argued that the mechanisms used to validate parental consent under COPPA do not need to be directly applied to the GDPR, since they may lose their effectiveness as technology progresses. Nevertheless, it is conceivable to establish a rule that serves as a general standard and is not biased towards any specific technology. However, it may still include certain instances, as the provisions outlined in Article 32 pertaining to data security criteria.

We drafted a prototype rule in the following manner:

"Taking into consideration the state of the art, the controller and the processor should adopt adequate technologies to guarantee the consent is given or authorised by the holder of parental responsibility over the child, including inter alia as appropriate:

(a) conducting a video conference with the parents to verify their official IDs

(b) confirming the electronic identification (eID) of the parents compared with the eID of the children

(c) Where the processing is unlikely to pose a high risk (e.g., subscribing to a newsletter), consent can also be given through email."

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, however, 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 potential 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. We also claimed that while being underage to provide consent, children could nonetheless exercise certain rights that entail little risk, such as the right to access, terminate (e.g., a data transfer), and delete. Children who possess a sufficient level of maturity to understand the repercussions of their online behaviour might find it less challenging to use these rights without requiring consent from their parents. 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 the 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 the COPPA in detail. The 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. We stated that when children are under the age of consent, data controllers must inform their parents about any 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 technology, and the purposes of processing 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.

We also mentioned that Chapter 5 of the GDPR requires data controllers to meet certain criteria before transferring personal data to third countries. Article 45 of the GDPR allows data transfer to a third country or international organisation if the European Commission determines that said third country or international organisation provides an adequate level of data protection. In this case, the data controllers do not need to take any extra measures to facilitate the transfer.

It is still possible to transfer EU data to third countries in the absence of adequacy decisions where appropriate safeguards are implemented by the data controller or processor. However, in this case, data transfers need case-by-case analysis and this procedure places significant burdens on data importers and exporters. According to Article 46 of the GDPR, the appropriate safeguards may be provided by binding corporate rules (BCRs), standard contractual clauses (SCCs), certification mechanisms, and codes of conduct to protect data.

If one of the exceptions in Article 49 of the GDPR applies, personal data may be transferred to a third country or international organisation without an adequacy decision or

appropriate safeguards. However, Article 49 derogations cannot be used to repeatedly transfer data. These exceptional data transfers will only be accepted occasionally, when necessary for a specific purpose.

The GDPR does not specifically address the transfer of child data. We suggested, however, that children should have some control over their data transfers in low-risk situations such as not allowing their data to be transferred to third countries. If a child is mature enough to request, for example, the cessation of the transfer of personal data to third countries, data administrators should comply even without parental consent.

In addition, real-life instances were provided. It was observed that Instagram and Facebook fail to particularly address the transfer of child data. Google and YouTube have rather advanced privacy policies that require parental consent before sharing any information concerning a child.

Transfers of personal data within the EU are not subject to the provisions outlined in Chapter 5 of the GDPR. Accordingly, there are no restrictions on the free flow of personal data within the Union. Yet, when personal data is transferred between Member States, another issue arises.

As shown in Subchapter 3.3 of this thesis, EU Member States have varying age restrictions for the processing of personal data based on parental consent. According to the first Commission report on the assessment and review of the GDPR, the various consent ages of Member States for information society services generate ambiguity and challenges for cross-border commerce.

Hence, we emphasised once more that Member States should agree on a uniform consent age online to stabilise the sharing of children's personal information. Besides, national variations in legislation implementation and interpretation by data protection authorities increase the costs of EU legal compliance. Thus, consistent age thresholds across Member States would also aid data controllers in minimising the costs associated with the transfer of children's data.

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. The article would be presented as follows:

> "1. Children may lack awareness regarding privacy policies and their rights pertaining to privacy and data protection. In accordance with best practises, data controllers shall employ simple video presentations or visually engaging images accompanied by easily comprehensible language to enhance children's understanding of their data protection rights, particularly with regard to the right to be informed and the right to access their personal data.
>
> 2. The use of the rights to ratification, erasure and prohibition or termination of data transfers shall be allowed in cases when children possess the necessary level of maturity to independently request such actions, hence eliminating the requirement for parental consent.
>
> 3. The practise of profiling may be subject to prohibition unless there exists a compelling or public interest that may outweigh the interests of the child in question. However, in the event that such a situation arises, it shall be still possible for a child to object to this profiling. In this scenario, it is imperative for the data controller to take prompt action, without delay, even in the absence of parental consent.
>
> 4. In the event of data breaches, data controllers are required to inform parents and children concurrently, even if the children are at an age where they can provide consent, as a precautionary measure. In addition, it is essential that they provide parents with

information and assistance to assist them in mitigating the negative consequences of personal data breaches on their children. The exemptions specified in Article 34(3) shall not be applicable in cases where the individual whose data is being processed is a child. 5. The Regulation shall reserve all other responsibilities of data controllers and all other rights of children."

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 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).

In Chapter 6 of this thesis, we addressed the seventh research question pertaining to the impact of the GDPR and the COPPA on the operational procedures of social media platforms and the sharing behaviours of parents with regards to their children. This chapter also addresses the last and overarching question of this thesis, which examines whether an excessive reliance on parental consent and responsibility may efficiently protect the personal data and privacy of children. Regarding the answer of the seventh research question, this thesis argues the following:

Given that the GDPR and the 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 the COPPA impose no penalties on parents who disclose personal information about their children on the Internet. Nonetheless, 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 Chapter 6. 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.

However, we acknowledged the implementation of AI and ML technology by Meta (including Facebook and Instagram) and Google (including YouTube) for the purpose of identifying and removing harmful content, such as nudity, violence, and sexual exploitation of children. This approach aligns with a suggestion we previously proposed in one of our publications. Nevertheless, it would have been more advantageous to enhance this system in order to identify potentially detrimental information prior to its dissemination by parents or other adults, hence preventing its accessibility to malicious individuals inside the online realm.

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 of 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 the GDPR and the 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. (2020) 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 experience exploitative commercial operations, due to their lack of commercial 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.

Based on the comprehensive analysis presented in the thesis, it is highly recommended that the following be considered as a response to the overarching research question:

> Both parents and children might not possess an adequate awareness of the significance associated with privacy and data protection. Furthermore, their understanding of the potential ramifications and risks associated with relinquishing control over children's data on the Internet could be limited. Both children and parents may possess a lack of knowledge of the privacy and data protection rights of children, as well as the mechanisms via which these rights might be exercised. They could lack

information regarding the responsibilities of data controllers in relation to the exercise of their rights. Hence, it is imperative for lawmakers to adopt a more precise, specific, and instructive approach when establishing the rights of children and the corresponding responsibilities of data controllers.

As previously stated, it is important that children have the opportunity to exercise their rights autonomously, without requiring parental approval whenever possible, and that they have the ability to directly communicate with data controllers when appropriate. Besides, lawmakers need to consider implementing more stringent regulations on shared material pertaining to children. This approach would prioritise the establishment of immediate measures, rather than excessively relying on parental consent and delegating the responsibility of determining the sharing of child-related information only to parental authority. Furthermore, these limitations would require social media sites to enhance their privacy practices in relation to potentially harmful or sensitive information pertaining to children.

As a prospective long-term strategy, the government may provide financial resources to facilitate the implementation of educational seminars and lectures on digital literacy inside schools, targeting both children and their parents. Additionally, it is essential to ensure that the legislations are executed in a way that is conducive to the needs and understanding of children. Moreover, it is crucial for the courts in both the EU and the US to interpret these legislations in a manner that safeguards the privacy and data protection rights of children. Accordingly, they could have the ability to serve as models for other legal systems and jurisdictions.

In summary, it can be inferred that fostering cooperation among governments, parents, schools, and data controllers is the optimal approach for protecting children's privacy and ensuring data protection in the realm of the internet, rather than only burdening parents with this responsibility.

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: 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 29 September 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), 11 available at https://arsboni.hu/wp-content/uploads/2022/09/Arsboni-foly%C3%B3irat_2022_1_2.pdf (last visited 29 September 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 L Fredrickson and Tomi-Ann Roberts: Objectification theory: Toward understanding women's lived experiences and mental health risks, Psychology of women quarterly 21, no. 2 (1997), 179-180.

- 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 29 September 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 4 September 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 4 September 2023).
- Chris Connolly: The US Safe Harbor - Fact or Fiction?, Galexia (2008), 7-8, https://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf (last visited 13 September 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.
- Cunningham McKay: Complying with International Data Protection Law, University of Cincinnati Law Review 84, no. 2 (2016), 446-447.

- 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.
- Deborah Roedder John: Consumer socialization of children: A retrospective look at twenty-five years of research, Journal of consumer research 26, no. 3 (1999), 183-213.
- Dilip R. Patel, Maria Demma Cabral, Arlene Ho, and Joav Merrick: A clinical primer on intellectual disability, Translational pediatrics 9, no. Suppl 1 (2020), S23-S35.
- Dipankar Dasgupta, Arunava Roy and Abhijit Nag: Multi-Factor Authentication: More secure approach towards authenticating individuals, Advances in User Authentication, Springer International Publishing AG (2017), 186.
- 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.
- Eric C. Thompson: The incident response strategy, Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents (2018), 65-70.
- 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.
- Evelyn P. Meier and James Gray: Facebook photo activity associated with body image disturbance in adolescent girls, Cyberpsychology, behavior, and social networking 17, no. 4 (2014), 200 and 202.
- 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.
- Francesca Gioia, Mark D. Griffiths and Valentina Boursier: Adolescents' body shame and social networking sites: The mediating effect of body image control in photos, Sex Roles 83 (2020), 773, 776 and 781.
- 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.
- Graham Pearce and Nicholas Platten: Achieving personal data protection in the European Union, JCMS: Journal of Common Market Studies 36, no. 4 (1998), 531.
- 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.
- 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.
- 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.

- Jenny Radesky, Yolanda Linda Reid Chassiakos, Nusheen Ameenuddin, and Dipesh Navsaria: Digital advertising to children, Pediatrics 146, no. 1 (2020), 2.
- 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
- Joshua Warmund: Can COPPA Work - An Analysis of the Parental Consent Measures in the Children's Online Privacy Protection Act," Fordham Intellectual Property, Media &Entertainment Law Journal 11, no. 1 (2000), 192-193.
- 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.
- 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, 104407.
- Kevin F McCrohan, Kathryn Engel, and James W. Harvey: Influence of awareness and training on cyber security, Journal of internet Commerce 9, no. 1 (2010), 24-27.
- Kristen Harrison and Barbara L. Fredrickson: Women's sports media, self-objectification, and mental health in black and white adolescent females, Journal of Communication 53, no. 2 (2003), 228.
- Manu J. Sebastian: The European Union's General Date 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), 46.
- Máté Dániel Szabó: Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival, Információs Társadalom: társadalomtudományi folyóirat 5, no. 2 (2005), 44.
- Matthew L Jensen, Michael Dinger, Ryan T. Wright, and Jason Bennett Thatcher: Training to mitigate phishing attacks using mindfulness techniques, Journal of Management Information Systems 34, no. 2 (2017), 599.
- 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, Ellysse 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 Ceruzzi: From scientific instrument to everyday appliance: The emergence of personal computers, 1970–77, History and Technology: An International Journal 13, no. 1 (1996), 1-31.
- 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, Berkman Center research Publication (2015), 26-29.
- 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.
- Sugandh Shah and Babu M. Mehtre: An overview of vulnerability assessment and penetration testing techniques, Journal of Computer Virology and Hacking Techniques 11 (2015), 27-49.
- 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.
- 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), 145.
- Yolanda N. Evans: One-sided social media relationships and the impact of advertising on children, Pediatrics 146, no. 5 (2020), 1-2.

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.
- Bart Custers, Alan M. Sears, Francien Dechesne, Ilina Georgieva, Tommaso Tani, and Simone Van der Hof: EU personal data protection in policy and practice, Hague: TMC Asser Press, Springer (2019), 1.
- 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.
- Tobias Naef: The Global Reach of the Right to Data Protection. In: Data Protection without Data Protectionism. European Yearbook of International Economic Law, vol 28. Springer (2023), 21.
- W. Page Keeton (et al.): Prosser and Keeton on the Law of Torts, West Publishing Co. St. Paul Minn. 5th ed. (1984), 850-851.
- William Blackstone and William Carey Jones (eds): Commentaries on the Laws of England, San Francisco, Bancroft-Whitney Co. (1916), 2430-2431.

Legal Texts

- 15 U.S.C. § 45(a)(1) (1994): "Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."
- 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.
- 18 U.S.C. 2258A (2011) (Reporting requirements of electronic communication service providers and remote computing service providers) (a).
- 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.
- 5 U.S.C.§ 552a(b)-(f).
- 50 U.S.C. 1801 et seq.
- Act C of 2012 on the Criminal Code (Magyar Büntető Törvénykönyvről szóló 2012. évi C. törvény) (1 January 2023) Section 204(1)(a,b,c) and (2)(a) [Translated by Nemzeti Jogszabálytár], https://njt.hu/jogszabaly/en/2012-100-00-00 (last visited 15 September 2023).
- Act V of 2013 on the Civil Code (2013. évi V. törvény a Polgári Törvénykönyvről) (1 July 2021), Section 4:191(1)(a) and Section 4:193(1) [Translated by Nemzeti Jogszabálytár], https://njt.hu/jogszabaly/en/2013-5-00-00 (last visited 15 September 2023).
- Article 29 Data Protection Working Party, Adequacy Referential, 18/EN WP 254 rev01, Adopted on 28 November 2017, Last Revised and Adopted on 6 February 2018, p. 1-9.

- 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, Adopted on 25 March 2014, p. 5-6.
- Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136, Adopted on 20th June 2007, p. 1-26.
- Article 29 Working Party, Guidelines on consent under Regulation 2016/679 17/EN WP 259 rev.01, Adopted on 28 November 2017, Last Revised and Adopted on 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 7-8.
- Charter of Fundamental Rights of The European Union, OJ C 364, 18.12.2000, pp. 1-22, Article 11. It became legally binding as EU primary law with the Lisbon Treaty(*) in 1 January 2009.
- 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 29 September 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 29 September 2023).
- Congress.Gov, Constitution Annotated Analysis and Interpretation of the US Constitution, Fourth Amendment Searches and Seizures, Amdt4.3.1 Overview of Unreasonable Searches and Seizures, https://constitution.congress.gov/browse/essay/amdt4-3-1/ALDE_00013715/ (last visited 2 September 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 29 September 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 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 29 September 2023).
- 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 29 September 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 Maximillian 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, 23.11.1995, p. 31–50.
- EDPB, Guidelines 04/2021 on codes of conduct as tools for transfers, 22 February 2022, 1-16, https://edpb.europa.eu/system/files/2022-

03/edpb_guidelines_codes_conduct_transfers_after_public_consultation_en_1.pdf (last visited 4 September 2023).

- EDPB, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1, Adopted on 4 May 2020, Updated on 13 May 2020, 1-33 para. 129.
- 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 29 September 2023).
- EDPB, Guidelines 07/2022 on certification as a tool for transfers, version 2.0, 14 February 2023, 1-19, edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_en_0.pdf (europa.eu) (last visited 4 September 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 29 September 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 (last visited 29 September 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 (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_sto_edpb_recommendations.pdf (last visited 10 March 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 29 September 2023).
- 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 Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, OJ C (2023) 4745, 10.07.2023, 1-64.
- 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, 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 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 29 September 2023).
- European Commission, eID, What is eID?, https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eID (last visited 29 September 2023).
- European Commission, Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, COM(90) 314 final – SYN 287, OJ C 277/3, 5.11.1990, pp. 3-12.
- 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, Shaping Europe's digital future, Electronic Identification, https://digital-strategy.ec.europa.eu/en/policies/electronic-identification (last visited 29 September 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 29 September 2023).
- European Data Protection Board, Approved Binding Corporate Rules, https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en?page=1 (last visited 29 September 2023).

- European Data Protection Supervisor (EDPS), Data Protection, https://edps.europa.eu/data-protection/data-protection_en (last visited 13 January 2023).
- 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 29 September 2023).
- 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".
- 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 4 September 2023).
- Health Insurance Portability and Accountability Act. Pub. L. No. 104-191, 110 Stat.1936 (1996).
- Hessisches Datenschutzgesetz of 7 October 1970, Gesetz- und Verordnungsblatt für das Land Hessen Teil I, No. 41, 625 of 12 October 1970.
- N.Y. Sess. Laws 1903, ch. 132, §§ 1-2, amended by N.Y. Civ. Rights Law, §§ 50-51 (McKinney 1909).
- Online Eraser Button Law: S.B. 568, 2013 LEG. 2013-14 SESS. (Cal. 2013), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568 (last visited 29 September 2023).
- 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 29 September 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.
- Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) OJ L 277, 27.10.2022, pp. 1–102.
- 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 29 September 2023).
- 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.
- 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 29 September 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), Judgment of the Court of Appeals for the Second Circuit, New York, 22 July 1940.
- Case 148/78, Pubblico Ministero v Ratti [1979] ECR 1629, EU:C:1979:110, p. 1636.
- 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-404/92 P X v Commission [1994] ECR I-4737, paragraph 17.
- 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-62/90 Commission v Germany [1992] ECR I-2575, paragraph 23.

- 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, Judgment 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) 484-86. https://tile.loc.gov/storage-services/service/ll/usrep/usrep381/usrep381479/usrep381479.pdf (last visited 29 September 2023).
- Hurbain v. Belgium judgment (Grand Chamber) on 4 July 2023, no.57292/16 para. 255 et seq.
- Hurbain v. Belgium judgment on 21 June 2021, referral to the Grand Chamber 11 October 2021, no.57292/16 para. 132 et seq.
- 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.
- Peck v The United Kingdom No 44647/98.
- Powell and Rayner v. the United Kingdom judgment of 21 February 1990, no. 9310/81, para. 41.
- Société Colas Est and Others v France, no. 37971/97.
- 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 16 September 2023).
- AEPD (Spanish DPA), Risk Management and Impact Assessment in the Processing of Personal Data, (June 2021), https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf (last visited 29 September 2023).
- Apple, Siri: https://www.apple.com/siri/ (last visited 29 September 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 29 September 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 29 September 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 15 September 2023).
- 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 29 September 2023).
- Britannica, Joe Biden, https://www.britannica.com/biography/Joe-Biden (last visited 29 September 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 29 September 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 29 September 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 29 September 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 29 September 2023).
- CNIL (French DPA), Analyse d'impact relative à la protection des données : publication d'une liste des traitements pour lesquels une analyse est requise (6 November 2018), https://www.cnil.fr/fr/analyse-dimpact-relative-la-protection-des-donnees-publication-dune-liste-des-traitements-pour (last visited 13 September 2023).

- CNIL (French DPA), Privacy Impact Assessment (PIA) Methodology, (February 2018), https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-pia-1-en-methodology.pdf (last visited 29 September 2023).
- CNIL, The open source PIA software helps to carry out data protection impact assessment, (30 June 2021), https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment (Portable and online versions are available. CNIL provided English translations for the tool, and a few EU DPAs offered translations as well, such as Hungarian DPA and Italian DPA. In addition, other translations are given by the community, such as Spanish and Croatian.) (last visited 29 September 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&treatynum=108 (last visited 29 September 2023).
- Data Protection Commission Ireland, List of Types of Data Processing Operations which require a Data Protection Impact Assessment, p. 1-6, https://www.dataprotection.ie/sites/default/files/uploads/2018-11/Data-Protection-Impact-Assessment.pdf (last visited 13 September 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 29 September 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 29 September 2023).
- euCONSENT, euCONSENT's first large scale pilot (18 March 2022) https://euconsent.eu/euconsents-first-large-scale-pilot/ (last visited 29 September 2023).
- 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 29 September 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 29 September 2023).
- euCONSENT, FAQ: What is euCONSENT?, https://euconsent.eu/faq/ (last visited 29 September 2023).
- Euractive: Schrems: round three (4 November 2022) https://www.euractiv.com/section/digital/podcast/schrems-round-three/ (last visited 29 September 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 29 September 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 29 September 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 29 September 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 29 September 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 29 September 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 29 September 2023).

- European Commission, Trans-Atlantic Data Privacy Framework (25 March 2022), https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100 (last visited 29 September 2023).
- European Commission, Types of EU law, Types of EU legal acts: Directives, Types of EU law (europa.eu) (last visited 29 September 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 29 September 2023).
- European Commission, What does data protection 'by design' and 'by default' mean?, https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en (last visited 13 September 2023)
- European Data Protection Supervisor (EDPS), Data Protection: Privacy- a fundamental right, https://edps.europa.eu/data-protection/data-protection_en (last visited 29 September 2023).
- European Data Protection Supervisor (EDPS), Data Protection: What is data protection?, https://edps.europa.eu/data-protection/data-protection_en (last visited 29 September 2023).
- European Data Protection Supervisor (EDPS), Data Protection: What is privacy?, https://edps.europa.eu/data-protection/data-protection_en (last visited 29 September 2023).
- European Data Protection Supervisor (EDPS), 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 29 September 2023).
- European Parliamentary Research Service (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 (last visited 29 September 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 29 September 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 29 September 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 29 September 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 29 September 2023).
- Facebook, Privacy Policy: How do we transfer information?, https://www.facebook.com/privacy/policy?section_id=9-HowDoWeTransfer (last visited 4 September 2023).
- Facebook, Safety Centre, Online Child Protection: Our Policies https://www.facebook.com/safety/onlinechildprotection (last visited 2 October 2023).
- Facebook, Sign Up: https://www.facebook.com/signup (last visited 29 September 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 29 September 2023).
- Federal Trade Commission, Complying with COPPA: Frequently Asked Questions, H. General Audience and Teen Sites or Services, 1, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#I.%20Verifiable%20Parental%20Consent (last visited 9 September 2023).
- Federal Trade Commission, FTC Staff Sets Forth Principles For Online Information Collection From Children, July 1997, https://www.ftc.gov/news-events/news/press-releases/1997/07/ftc-staff-sets-forth-principles-online-information-collection-children (last visited 29 September 2023).

- Federal Trade Commission, Privacy Online: A report to Congress, June 1998, https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf (last visited 29 September 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 29 September 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 29 September 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 29 September 2023).
- FRA (European Union Agency for Fundamental Rights), 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 29 September 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 29 September 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 2 October 2023).

- Fun Brain, Privacy Policy: https://www.funbrain.com/privacy-policy (last visited 29 September 2023).
- Fun Brain: https://www.funbrain.com/ (last visited 29 September 2023).
- Galexia, http://www.galexia.com.au (last visited 13 September 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 29 September 2023).
- Google Family Link https://families.google/familylink/ (last visited 29 September 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 4 September 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 2 October 2023).
- Google, Privacy & Terms, When Google shares your information https://policies.google.com/privacy?hl=en-US#infosharing (last visited 2 October 2023).
- Google, Products, https://about.google/products/ (last visited 25 September 2023).
- Google, Safety and Security, How we detect, remove and report child sexual abuse material, Susan Jasper (28 October 2022), https://blog.google/technology/safety-security/how-we-detect-remove-and-report-child-sexual-abuse-material/ (last visited 25 September 2023).
- Google, Sign Up: https://accounts.google.com/signup/v2/webcreateaccount?flowName=GlifWebSignIn&flowEntry=SignUp (last visited 29 September 2023).
- Happify, Legal, Happify™ Privacy Policy: Last Updated July, 2020, https://www.happify.com/public/legal/#legal (last visited 29 September 2023).
- HSBC Voice ID, https://www.hsbc.com.hk/ways-to-bank/phone/voice-id/ (last visited 29 September 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 29 September 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/#:~:text=A%20DPIA%20is%20a%20tool,by%20design%20and%20by%20default. (last visited 29 September 2023).
- ICO, Rights related to automated decision making including profiling, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/rights-related-to-automated-decision-making-including-profiling/ (last visited 29 September 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 29 September 2023).
- 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 29 September 2023).
- 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 29 September 2023).
- Information Commissioner's Office (ICO), When do we need to do a DPIA?, What does the ICO consider likely to result in high risk?, point (9), https://ico.org.uk/for-

organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/ (last visited 29 September 2023).

- Instagram Help Center, How to Report Things, Report a child under 13 on Instagram, https://help.instagram.com/2922067214679225/?helpref=hc_fnav (last visited 29 September 2023).
- Instagram Help Centre, Recommendations on Instagram, https://help.instagram.com/313829416281232/?helpref=uf_share (last visited 24 September 2023).
- Instagram Help Centre, Sharing to other social networks, https://help.instagram.com/169948159813228 (last visited 29 September 2023).
- Instagram, Help Centre, Community Guidelines, https://help.instagram.com/477434105621119/?helpref=uf_share (last visited 16 September 2023).
- Instagram, Kids Diana Show (image posted on 21 August 2021) https://www.instagram.com/p/CSeZgdHjkVF/?hl=tr (last visited 16 September 2023).
- Instagram, Privacy Policy, How do we transfer information?, https://privacycenter.instagram.com/policy/?section_id=9-HowDoWeTransfer (last visited 4 September 2023).
- Johnson & Johnson, Privacy Policy: Contacting us https://www.jnj.com/corporate/privacy-policy (last visited 4 September 2023).
- Johnson & Johnson, Privacy Policy: Use by Minors https://www.jnj.com/corporate/privacy-policy (last visited 4 September 2023).
- Max Schrems, https://schre.ms/ (last visited 13 September 2023).
- Meta AI, Powered by AI: Instagram's Explore recommender system (25 November 2019), https://ai.meta.com/blog/powered-by-ai-instagrams-explore-recommender-system/ (last visited 24 September 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 29 September 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 2 October 2023).

- Meta, Community Standards Enforcement Report, Second Quarter 2021 (18 August 2021), https://about.fb.com/news/2021/08/community-standards-enforcement-report-q2-2021/ (last visited 4 October 2023).
- Meta, Facebook Community Standards, Child sexual exploitation, abuse and nudity, Policy rationale, https://transparency.fb.com/en-gb/policies/community-standards/child-sexual-exploitation-abuse-nudity/ (last visited 16 September 2023).
- Meta, Facebook Community Standards, https://transparency.fb.com/en-gb/policies/community-standards/?source=https%3A%2F%2Fwww.facebook.com%2Fcommunitystandards (last visited 16 September 2023).
- Meta, Online Child Protection: Tools and Technology https://about.meta.com/actions/safety/onlinechildprotection (last visited 25 September 2023).
- Meta, Safety Centre, Online Child Protection, https://about.meta.com/actions/safety/onlinechildprotection (last visited 16 September 2023).
- Mr. Alkohol (Coctails&Drinks), https://mralkohol.hu/ (last visited 29 September 2023).
- MyFitnessPal Privacy Policy, https://www.myfitnesspal.com/privacy-policy (last visited 29 September 2023).
- MyFitnessPal, Sign Up: https://www.myfitnesspal.com/account/create (last visited 29 September 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 29 September 2023).
- Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), GDPR 35 (4) Mandatory DPIA List, List of Processing Operations Subject to DPIA GDPR 35 (4), points (2), (19), and (20), https://www.naih.hu/data-protection/gdpr-35-4-mandatory-dpia-list (last visited 29 September 2023).

- Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), GDPR 35 (4) Mandatory DPIA List, List of Processing Operations Subject to DPIA GDPR 35 (4), points (2), (19), and (20), https://www.naih.hu/data-protection/gdpr-35-4-mandatory-dpia-list (last visited 29 September 2023).
- NOYB, European Commission Gives EU-US Data Transfers Third Round At CJEU, 10 July 2023, https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu (last visited 29 September 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 2 October 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 29 September 2023).
- 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 29 September 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 29 September 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 29 September 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 4 September 2023).
- Statista: Most popular social networks worldwide as of January 2023, 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 29 September 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 29 September 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 29 September 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 16 September 2023).
- The International Trade Administration (ITA), U.S. Department of Commerce, Data Privacy Framework Program, https://www.dataprivacyframework.gov/s/ (last visited 1 September 2023).
- The International Trade Administration (ITA), U.S. Department of Commerce, Data Privacy Framework Program, Data Privacy Framework (DPF) Program Overview, https://www.dataprivacyframework.gov/s/program-overview (last visited 1 September 2023).
- The New York Times, A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal, Published 21 August 2022, Updated 21 June 2023, https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html (last visited 29 September 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 29 September 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 29 September 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 29 September 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 16 September 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 16 September 2023).
- U.S. Department of State, Archive, Progress & Freedom Foundation https://2001-2009.state.gov/p/io/unesco/members/48807.htm (last visied 14 October 2023).
- Ügyfélkapu: https://ugyfelkapu.gov.hu/ (last visited 29 September 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 29 September 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 29 September 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 29 September 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 29 September 2023).
- Vodafone Privacy and Cookie Policy: International data transfer https://www.vodafone.com/cookie-policies (last visited 2 October 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 4 September 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 2 October 2023).
- 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 16 September 2023).
- 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 16 September 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 16 September 2023).
- YouTube Kids Privacy Notice: Information we share https://kids.youtube.com/t/privacynotice (last visited 4 September 2023).
- YouTube Kids: An application specially designed for children https://www.youtube.com/kids/ (last visited 4 September 2023).
- YouTube, Newsnercom channel: Barber Pranks Kid By Pretending He's Cut His Ear Off, https://www.youtube.com/watch?v=0TSNKp4Xs0U (last visited 29 September 2023).

- YouTube, Ryan's World Channel: Christmas Morning 2016 Opening Presents with Ryan ToysReview, https://www.youtube.com/watch?v=WyOkjW5FqBU (last visited 24 September 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 16 September 2023).
- YouTube, Storyhive Channel: Yoga for Kids!, https://www.youtube.com/watch?v=X655B4ISakg (last visited 16 September 2023).
- YouTube, Terms of Service, General Terms and Conditions: Who can use the service?, Age requirements https://kids.youtube.com/t/terms (last visited 29 September 2023).
- YouTube, Thesomebodytoknow channel: My story: Struggling, bullying, suicide, self-harm, available at: https://www.youtube.com/watch?v=vOHXGNx-E7E (29 September 2023).
- YouTube, Vlad and Niki's Channel: Vlad and Nikita play with Toy Cars - Collection video for kids, https://www.youtube.com/watch?v=NtzftGb0EcM (last visited 24 September 2023).