SRC 2016, November 30, 2016, The Netherlands.

Is EU regulation effective in ensuring children's online privacy and data protection?

Andrada-Cristina Mateiciuc
The Hague University of Applied Sciences
crist_andra@yahoo.com

ABSTRACT
Following the rationale of the current EU legal framework protecting personal data, children are entitled to the same privacy and data protection rights as adults. However, the child, because of his physical and mental immaturity, needs special safeguards and care, including appropriate legal protection. In the online environment, children are less likely to make any checks or judgments before entering personal information. Therefore, this paper presents an analysis of the extent to which EU regulation can ensure children's online privacy and data protection.

Keywords
EU, data protection, online privacy, minors

INTRODUCTION

The Internet made its debut in 1991, with easy-to-use browsers widely accessible a few years later.[1] Since then, no major aspect of modern life remained untouched by IT. The most exposed to its rapid development are those born after the brink of the new millennium, *i.e.* minors and young adults. In 2012, it was estimated that 38% of 9-12 year-olds and 77% of 13-16 year-olds use the internet in Europe, and 59% of all minors have their own social media profile.[2] Since the IT development is at its highest in the last decade, the number of children who utilize the internet grows continuously.

This digital revolution has brought many benefits, such as speed and reliability, but everything comes at a cost. Nowadays, the intensity of communication and digitalization triggered a situation in which most individuals find themselves powerless in managing their personal data and digital records. Children require special attention concerning their online activities. Their vulnerability lies in the fact that they are incapable of discerning online risks.[3] Giving-out personal information was found to be the most common risk.[4] Researchers show that children are incapable to distinguish between online and offline environments when sharing personal information.[5]

In view of this situation, it is important to evaluate the EU's approach to children's online protection.

EU legislation that concerns the processing and protection of personal data includes The Data Protection Directive[6] (DPD), now repealed by The General Data Protection Regulation[7] (GDPR) which enters into force in 2018.

Also, concerning the protection of children in the on-line/media environment, the EU has adopted a number of non-binding policies.

This paper focuses on an effectiveness analysis of the DPD and GDPR in what regards the protection they afford children in the online environment. Further, the added-value of soft laws, such as the EU Strategy for a Better Internet for Children[8] in this area is assessed.

SECTION 1: Effectiveness of the DPD in protecting children's rights to privacy and data protection

The effectiveness principle was established by the CJEU in a 1995 judgment.[9] Accordingly, the DPD's effectiveness analysis is performed as follows: firstly, its objectives are identified; secondly, the Directive's achievements are assessed to establish whether it has met its objectives.

The DPD was adopted using as legal basis an internal market provision, the now Article 114 TFEU, albeit with a dual objective, stated in Article 1 of the Directive: to ensure that States protect the individuals' fundamental rights and freedoms, while forbidding restrictions on the free-flow of personal data between Member States.

The DPD does not include a specific provision on the protection of children's rights. However, there is no doubt that children fall under its scope. DPD's objective of fundamental rights protection is intended to *every natural person* (Article 1.1). A child, although awarded with limited legal autonomy, is a natural person; thus, any minor who has his/her data processed under the DPD's scope is entitled to become subject to its provisions.

The content of the Directive is expressed in terms of **6 main principles** underlying it, and implemented in its provisions.[10] It is through these principles that the DPD attains its objectives:

- *Purpose limitation* (Article 6.b): personal data may only be collected and further processed for specified, explicit and legitimate purposes. This principle is designed to establish the boundaries within which data may be processed.
- *Legitimate purposes*: data can be processed only if one of the six potential legal bases in Article 7 is met by the controller.
- *Proportionality* (Articles 6.c, 6.d, 6.e): personal data must be adequate, relevant, and non-excessive in relation to the purposes of processing; it must be accurately kept up-to-date in a form which permits the identification of the subject only as long as necessary for the purposes of collection.
- *Transparency* (Articles 10, 12) refers to the information which the data subject must receive in relation to his collected data and to the right of the subject to access basic information about his/her personal data.
- *Security* (Article 17)*:* the controller must take measures appropriate to the risks presented by the processing.
- *Control* (Article 28)*:* Member States must establish National Data Protection Authorities (NDPA) tasked with the supervision of controllers' activities.

These provisions are relevant for the child's fundamental rights protection. Upon analysis, it was found that the DPD's principles ineffectively offer protection in the online environment, for the following reasons:

1. DPD's incompleteness negatively impacted the principles of purpose limitation, legitimate interest and proportionality

The Directive adopted generally-formulated concepts and open-standards. It was not a 'single-case-law', which aimed to apply to a specific case in a short timeframe. In contrast, it is general law, designed to serve a larger number of addressees, to cover a greater variance of cases, and typically have long duration. [11]

Nevertheless, the Directive was described as 'incomplete' because of its neutrality and open-ended terms.[12] It has not captured 'all possible situations' in which a subject's rights can be violated. DPD's incompleteness/neutrality means that key-provisions could work-out differently across jurisdictions, resulting in diverging levels of data protection.

The Article 29 Working Party's (WP) opinions were therefore necessary to provide practical guidance on the DPD. One of the WP's main concerns refers to the Directive's incompleteness: none of its provisions acknowledge the particularities of children's lives, and thus numerous

questions remain concerning the protection of children's privacy within the DPD-framework.

The WP voiced concerns about the safeguards offered by the **purpose limitation** principle. The WP identified a lack of harmonized interpretation of the principle, which weakens data subjects' position.[13]

Particularly in the case of children, the **legitimate purposes** principle is also seriously undermined. Under DPD, there are no specific rules on obtaining consent from individuals lacking full legal capacity.[14] Consent is one of the legal grounds for legitimate data processing.

It was the WP's view that absence of harmonizing rules for obtaining consent has consequences in terms of legal certainty, as the conditions for delivering underage, valid consent vary between States.[15] Further, this causes the DPD to ineffectively protect the interests of children, as it does not recognize their vulnerability.

As the purpose limitation and legitimacy principles are undermined, it threatens the safeguards of other principles, such as **proportionality**. The WP found that in the special case of children, when applying proportionality, in particular as regards the relevance of the collected data, controllers do not pay attention to the child's best interest.[16]

2. Information imbalances impacted the effectiveness of the transparency principle

Critics identified a further 'loophole' in the DPD: it gives rise to information asymmetries in the data subject-controller relationship.[17] An information asymmetry arises when one party possesses more information relative to the other. As a result of such imbalance, the individual is almost always in a weaker position, unable to protect his/her interests without state-intervention.

Where consent is required, the following problem emerges: information given is not adapted to children's understanding-level, and thus, they mostly deliver uninformed consent.[18] According to the transparency principle, individuals must be aware by whom, on what grounds, from where, why, and for how long their personal data are processed and what their rights are in relation to this. In practice, the European Commission observed that the duty to inform the subject does not cover each of those elements, and even when it does, the information is not easily understandable for the individual.[19]

This is particularly relevant to children, who tend to underestimate risks and consequences when making their data available online. Therefore, an information asymmetry arises when consent is used as a basis for processing data, leading to the undermining of the **transparency principle**.

3. Incorrect transposition impacted the security and control principles

Despite its aspiration to harmonize Member States data protection laws, the DPD left ample room for national implementation, yielding 28 distinct and conflicting regimes. Critics portrayed the DPD as rather unsuccessful, since there is a noticeable gap between European data protection law in the books and on the ground: enforcement has been fickle and sanctions weak. Further, scholars argued that whilst digitalization of all areas of life increases continuously, legislation has remained within its national borders.[20]

Forum-shopping is easily done by IT-companies that have no specifically-determined production location.[21] They could choose the location where they would be most leniently treated by the national enforcement of EU legislation. This raises concerns for the **security principle**'s effectiveness.

Lack of harmonization and incorrect transposition of the DPD provisions across States also raises issues of direct effect. While vertical direct effect does not raise any problems, horizontal direct effect does not exist in the case of EU Directives.[22]

Therefore, in case of a data protection issue, an individual, including a child through his/her legal guardian, cannot rely on the DPD directly to support his/her claim. The claimant may rely on EU Primary Law, which confers horizontal direct effect, or on national data protection laws. However, the Commission found that in many States, judicial remedies, while available, are rarely pursued, since 63% of individuals are not even aware of the existence of NDPAs.[23] Further, the Commission stated that children are exposed to immense social and mental harm due to accidental disclosure of personal data. These problems, in turn, raises questions about the **control principle**'s effectiveness.

SECTION 2: GDPR's attempts to remedy DPD's loopholes

As demonstrated in the above-section, neither of the DPD's 6 principles proved effective in protecting children's online privacy and data protection. In 2010, the Commission announced its intention to revise the EU-framework on data protection.

In the specific case of children, the Commission reported that the reform-package considers enhancing the principle of transparency, clarifying and strengthening the rules of consent, and drawing-up EU standard-forms (privacy information notices) to be used by controllers. The Commission stated that these measures could increase transparency for children; they could be informed in an understandable and accessible manner about the usage of their personal data.[24]

Further, the Commission stated that children would also benefit from awareness-raising regarding their rights and risks of personal data processing.[25] It proposed co-financing awareness-raising activities on data protection via the Union-budget, and establishing an obligation to carry out awareness-raising activities by States.

In the following, an assessment is provided of how the GDPR attempts to address the DPD's above-identified lacunae.

1. Remedies to incompleteness: enhancing the principles of purpose limitation and legitimate purpose

The interlinked **principles of purpose limitation and transparency** are enhanced by the GDPR.

The GDPR includes specific conditions for consent (Article 7). The Recitals clarify this concept and its requirements: consent is *'a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement'*; consent should be opted-in by a written/oral statement. Further, the Recital emphasizes that explicit, and not implicit, consent is the primary means of legitimizing data processing. The controller has the burden of proving that consent was actually given; it is 'freely given' when the subject has genuine free-choice and not when e.g. he/she can no longer refuse/withdraw.

Moreover, the GDPR, in Article 8, specified conditions applicable to a child's consent: processing is lawful when consent is given by someone older than 16; otherwise, it must be given/authorized by the legal guardian. States may provide for a lower age, but not lower than 13.

The WP opined that the States' liberty to provide for a lower age could lead to harmonizing constraints.[26]

The Regulation's new approach towards consent was also met with scholarly critiques. Accordingly, in many instances, the opt-in consent is neither more voluntary nor informed than

implied consent. Reliance on opt-ins disrupts user-interfaces and encumbers individuals with repetitive prompts, which they are eager to click through.[27] Moreover, even assuming perfect information, consumers' freedom is relative.[28] Individuals are free to accept/reject terms offered, but it is the vendor who decides the terms. Thus, surrendering personal information is often non-negotiable. This concern is relevant for minors, as they are less likely to make comprehensive checks when providing consent/information over the internet.

It is therefore yet unclear whether the Regulation will succeed in remedying DPD's incompleteness towards purpose limitation and legitimacy.

2. Remedies to information imbalances: enhancing the principle of transparency

According to GDPR's Article 12, controllers are required to take appropriate measures in providing data-processing information to the subject in a concise, transparent, intelligible and easily-accessible form, using clear and plain language, particularly where information is addressed specifically to children. Therefore, GDPR attempts to remedy DPD's information imbalances, as it specifically requires controllers to make language easily-understandable to children. It is however yet uncertain whether clearer information empowers children, since, as concluded in the previous sub-section, opted-in consent by means of repetitive prompts could actually encumber minors.

3. Remedies to harmonization constraints: enhancing the principles of security and control

One of the reasons of reforming the DPD was to ensure a consistent level of protection for all EU-citizens. A Regulation was deemed necessary to increase legal certainty and transparency, to ensure consistent monitoring, and equivalent sanctions. This Regulation provides a margin of maneuver: it does not exclude national law for specific processing situations, but intends to solve the consistency issues created under the DPD, by being directly-applicable.

Further, regarding the **security principle**, the GDPR puts forward 'accountability'. There was no specific reference to this principle in the DPD,[29] but less explicit elements compounding accountability existed in it. Accordingly, controllers must employ effective and explicit data-governance programs to protect individuals' data against risks and to demonstrate how they protect data (Art 24 GDPR).

While individuals must continue to make informed choices, they cannot be held accountable for detailed decisions about vastly-complex technologies and data-uses.[30] This is relevant to children, as their lack of discernment may lead to giving away data without making intricate exploration on its further usage.

Effective accountability framework relieves children of the burden of policing the marketplace against bad actors. It heightens the individuals' confidence that their stored/processed data is protected. However, the security principle's effectiveness depends on national enforcement, i.e. on the **control principle**.

Accordingly, the GDPR requires controllers/processors to designate a Data Protection Officer, tasked with monitoring and ensuring that data processing is done compliant to the Regulation (Art 39). Another novelty of the Regulation concerning the control principle is the creation of the EDPB, an independent EU-body, tasked with monitoring NDPA compliance, and providing guidance to the Commission on issues of data protection (Art 70).

Further, control is enhanced by more explicit rights of individuals to lodge complaints to/against the NDPAs (Art 77), and to an effective judicial remedy against supervisory authorities/controllers and processors (Arts 78, 79).

Thus, GDPR enhances the control and security principles by providing more comprehensive rules. Their effectiveness however will be proved in practice.

SECTION 3: The added-value of EU policies in regulating child online privacy and data protection

Notwithstanding the positive aspects of legislation, e.g. that it is based on a democratic mandate and the legislator is subject to democratic scrutiny, scholars identified that binding laws suffer from a number of drawbacks: [31]

The first problem, instrument failure, implies that legislation is inappropriate and unsophisticated, because it cannot cover all possible situations. This is one of DPD's issues, through its incompleteness. Secondly, legislation is often ineffective in implementation, as seen for example with the DPD harmonizing-issue. Thirdly, it was found that regulation often does not provide incentives for subjects to comply (motivation failure). This has been identified in the DPD, regarding the security and control principles. Further critiques are that it is slow, costly, and it stifles innovation.

A shift from binding laws to de-centered regulation seems appropriate in sectors such as ICT, due to its rapid change and constant development. De-regulation implies less restrictive regulation, a search for ways of achieving objectives by less-burdensome methods of government-intervention.

The Commission launched the European Strategy for a Better Internet for Children, soft-law designed to offer guidance on enhancing child on-line protection. The expectation here is that children, under this empowerment model, will eventually gain control over their personal data.

Often-cited assets of data protection soft-law are: flexibility, capacity to adapt to fast developing technologies, higher degree of incorporated-expertise, and lower cost; it was claimed that incentives for commitment and compliance are higher, because actors are closely-involved in creating the rules.[32]

Drawbacks of non-binding policies do however also exist. Firstly, they lack effective enforcement. Such policies are also known for suffering from a low transparency level.[33]

For example, the EU Strategy contains some measures regarded as adequate safeguards to possible problems resulting from child-empowerment. There is, first of all, an acknowledgment that industry, States and the Commission need to collaborate to ensure that personal data is fairly-collected and used, and that businesses fully-engage with children and equip them to make meaningful choices/decisions.[34] Therefore, a form of binding intervention is necessary to ensure compliance with soft-laws.

Another concern of the EU Strategy is its premise that information self-management facilitates empowerment. It is known that network-environments are far from neutral: they have *ex ante* features, which favor businesses' interests and constrain individuals' choices and their ability to assert control.[35] Increased awareness of the value of privacy and skills to manage personal data can empower children in the sense that they may be able to make informed decisions about which information they should disclose, to whom and when.[36] However, some degree of effective regulatory oversight is still needed to ensure that these networks do not violate children's reasonable expectations.

Therefore, it is apparent that non-binding recommendations such as the EU Strategy cannot survive the rigors of the present technologies by themselves. A combined approach, between binding rules and establishment of codes of conduct, and awareness-rising activities backed by enforceable laws, seems to be the most effective in protecting children's

fundamental rights, because binding legislation has many drawbacks that could be remedied by non-binding policies and vice-versa.

CONCLUSION

The goal of this paper was to assess whether EU data protection regulation offers effective privacy and personal data protection to children in the online environment. It contributed to the broader topic of debate between academics regarding the effectiveness of the EU framework in ensuring fundamental rights protection.

The paper showed that children's right to privacy and data protection online is a present-day issue, which merits increasingly more attention at EU level.

From the above-findings, it can be concluded that the DPD provides ineffective protection for children. Further, the GDPR could offer children a more comprehensive online protection compared to its predecessor, but a certain measurement of its effectiveness cannot be yet achieved. However, the EU found an innovative way to address possible further loopholes, through non-binding policies. Therefore, a combined approach towards child online protection could prove effective in protecting children's online privacy and data protection.

ROLE OF THE STUDENT

Andrada Mateiciuc was and undergraduate student working under the supervision of Dr. Maria Eva Foldes when the research in this report was performed. The topic was proposed by the student for her LLB Thesis. The design of the thesis, the research, writing, as well as the formulation of the conclusions were done by the student.

REFERENCES

1. John Palfrey and Urs Gasser, *Born Digital – Understanding the First Generation of Digital Natives* (Basic Books 2008) 3
2. Sonia Livingstone, 'Towards a better internet for children: findings and recommendations from EU Kids Online to inform the CEO coalition' (2012) EU Kids Online, The London School of Economics and Political Science
3. Julia Davidson and Julie Grove-Hills, 'Online Abuse: Literature Review and Policy Context' (2011) prepared for the European Commission Safer Internet Plus Programme
4. J. Palfrey (n 1) 15
5. S. Livingstone (n 3)
6. 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 [1995] OJL281/003
7. 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 [2016] OJ L 119/1
8. European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of The Regions, European Strategy for a Better Internet for children COM(2012) 196 final
9. Case C-261/95 *Rosalba Palmisani and Instituto Nazionale della Previdenza Sociale (INPS)* [1997] ECR I-4037
10. Cristopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (2nd edition, Oxford University Press, 2007) 20
11. Z. Kunbei, 'Incomplete Data Protection Law', 15(6) German law journal: review of developments in German, European and international jurisprudence 1071-1104
12. ibid
13. Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2 April 2013, 00569/13/EN WP203
14. Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, 13 July 2011, 01197/11/EN WP187 27
15. ibid
16. Article 29 Data Protection Working Party, Opinion 2/2009 on the protection of children's personal data, 11 February 2009, 398/09/EN WP160 7
17. Orla Lynskey, 'Deconstructing Data Protection: the added value of a right to data protection in the EU legal order', [2014] 63 The international and Comparative Law Quarterly 569-597, 592
18. Article 29 Data Protection Working Party, Opinion 15/2011 (n 14) 38
19. European Commission, Commission Staff Working Paper, Impact Assessment SEC(2010) 72 final
20. J.P. Albrecht, 'Uniform Protection by the EU – the EU Data Protection Regulation salvages Informational self-determination' in H. Hijmans and H. Kranenborg (eds.), *Data Protection Anno 2014: How to restore trust?* (Antwerp, Intersentia Publishing 2014) 119-128, 124
21. ibid
22. Case 152/84 *Marshall v. Southampton and South-West Hampshire Area Health Authority* [1986] ECR I-737, para 48
23. European Commission, Impact Assessment (n 19) 28
24. European Commission, Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal Data Protection in the European Union COM(2010c) 609 final
25. ibid
26. Article 29 Data Protection Working Party, Opinion 01/2012 on the data protection reform proposals, 23 March 2012, 00530/12/EN WP191, 13
27. Omer Tene, 'Reforming data protection in Europe and beyond: a critical assessment of the second wave of global privacy laws' in A.R. Lombarte and R.G. Mahamut (eds.) *Towards a new European Data Protection Regime* (Tirant Lo Blanch, 2015) 184
28. J.E. Cohen, 'Examined Lives: informational privacy and the Subject as Object', [2008] 52 Stan. L. Rev. 1373, 1397
29. P. de Hert and D. Stefanatou, 'The accountability culture in its European Union dress. Sticks but no carrots to make the proposed regulation work' in A.R. Lombarte and R.G. Mahamut (eds.) *Towards a new European Data Protection Regime* (Tirant Lo Blanch, 2015)
30. Richard Thomas, 'Accountability – a modern approach to regulating the 21st century data environment' in H. Hijmans and H. Kranenborg (eds.), *Data Protection Anno 2014: How to restore trust?* (Antwerp, Intersentia Publishing 2014) 135-147, 138
31. Eva Lievens, *Protecting children in the Digital Era: the use of Alternative Regulatory Instruments* (Martinus Nijhoff Publishers, Leiden 2010) 149
32. Monroe Price and Stefaan Verhulst, 'In search of the self: charting the course of self-regulation on the Internet in a global environment' in C. Marsden (ed.) *Regulating the Global Information Society* (London, Routledge, 2000) 75
33. Michael Latzer, 'Trust in the industry – Trust in the users: self-regulation and self-help in the context of digital media content in the EU' (2007) available at http://www.leipzig-eu2007.de/en/downloads/dokumente.asp last accessed May 2017
34. Joseph Savirimuthu, 'Networked Children, Commercial Profiling and the EU Data Protection Reform Agenda: in the Child's Best Interests?' in I. Iusmen et al (eds.) *The EU as a Children's Rights Actor: Law, Policy and Structural Dimensions* (Barbara Budrich Publishers 2016) 226
35. J.E. Cohen, 'Examined Lives: informational privacy and the Subject as Object', [2000] 52 Stan. L. Rev. 1373, 1397
36. J. Savirimuthu (n 34)