Przegląd Prawa Konstytucyjnego
-----ISSN 2082-1212-----
DOI 10.15804/ppk.2022.06.36
-----No. 6 (70)/2022-----

Dominika Kuźnicka-Błaszkowska[1]

Protecting Children's Personal Data under General Data Protection Regulation and California Consumer Privacy Act in Relation to Information Society Services – European Perspective[2]

Keywords: children privacy, online privacy, children rights, California Consumer Privacy Act (CCPA), Children's Online Privacy Protection Act (COPPA), General Data Protection Regulation (GDPR)
Słowa kluczowe: prywatność dzieci, prywatność online, prawa dziecka, Kalifornijska Ustawa o Ochronie Prywatności Konsumentów (CCPA), Ustawa o Ochronie Prywatności Dzieci w Internecie (COPPA), Rozporządzenie o Ochronie Danych Osobowych (RODO)

Abstract

The protection of children's personal data as part of their right to privacy and information autonomy is extremely important. Year in, year out, the number of children using the Internet and services increases. This means that there need to be special tools and techniques established to protect children's right to privacy. It is particularly important when children use services provided by companies after other, than local, jurisdiction. As they may not fully understand risk associated with exposing themselves in the Intranet, this is crucial for governmental authorities to ensure that children are protected.

[1] ORCID ID: 0000-0001-8804-569X, Ph.D., University of Wroclaw. E-mail: dominika.kuznicka-blaszkowska@uwr.edu.pl.

[2] This research was funded in whole National Science Center PRELUDIUM 20, no. 0209/0037/22. For the purpose of Open Access, the author has applied a CC-BY public copyright licence to any Author Accepted Manuscript (AAM) version arising from this submission.

The aim of the article is to review current legislation protecting children's personal data both in European Union and State of California. This particular state has been chosen for two reasons: firstly dozens of internet services providers are based in this state, secondly it would be difficult to ignore that this state was the first to introduce new data protection regulation which in many aspects brings US data protection law closer to European standards. Taking into consideration European Union regulation it is necessary to assess whether the current data protection regime in California answers adequacy requirements and whether data may be freely transferred to this territory.

Streszczenie

Ochrona prawa do prywatności dzieci w środowisku usług społeczeństwa informacyjnego w świetle Rozporządzenia o Ochronie Danych Osobowych i Kalifornijskiej Ustawy o Ochronie Prywatności Konsumentów – perspektywa europejska

Ochrona danych osobowych dzieci w ramach ich prawa do prywatności i autonomii informacyjnej jest coraz bardziej istotna. Z roku na rok wzrasta liczba dzieci korzystających z Internetu i usług społeczeństwa informacyjnego. Konieczne stało się zatem wprowadzenie regulacji prawnego gwarantujących odpowiedni poziom ochrony praw i wolności najmłodszych użytkowników globalnej siedzi. Jest to szczególnie istotne, gdy dzieci korzystają z usług świadczonych przez firmy podlegające innej, niż miejscowa, jurysdykcji. Dzieci nie zawsze są w pełni świadome ryzyka, jakie wiążą się z korzystaniem przez nich z Internetu, a rolą państwa jest wprowadzanie takich rozwiązań, które zapewnią odpowiednią ochronę ich prawa do prywatności.

Celem artykułu jest przegląd obowiązujących przepisów chroniących dane osobowe dzieci zarówno w Unii Europejskiej, jak i w stanie Kalifornia. Ten konkretny stan został wybrany z dwóch powodów: po pierwsze w tym stanie ma swoje siedziby dziesiątki dostawców usług internetowych, po drugie trudno byłoby zignorować fakt, że ten stan jako pierwszy wprowadził nowe przepisy o ochronie danych, które pod wieloma względami zbliżają amerykańskie przepisy o ochronie danych bliżej standardów europejskich. Biorąc pod uwagę regulacje Unii Europejskiej, należy ocenić, czy obecny system ochrony danych w Kalifornii spełnia wymogi adekwatności i czy dane mogą być swobodnie przekazywane na to terytorium.

*

I. Foreword

Year in, year out, the number of children using the Internet and services increases. When General Data Protection Regulation[3] came into force in 2018 it changed not only European rules of personal data processing, but more importantly altered the ways business can operate in the entire Europe. The European Union has implemented several mechanisms to allow third countries (those outside the European Economic Area) to continue providing services on the European market and ensure that an adequate level of data protection is in place[4]. The new law may bring significant difference and simplify the transfer of data between the EU and the State of California. Hence the importance of an adequacy decision which may be adopted by the Europe-

[3] The Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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 (further General Data Protection Regulation, GDPR).

[4] The EU legislator has decided to establish several mechanisms for the transfer of personal data to third countries, taking into account, above all, ensuring an adequate level of protection. The methods of data transfer include:

a) the transfer of data on the basis of a decision establishing an adequate level of protection (Art. 45);
b) transfers subject to appropriate safeguards through a legally binding and enforceable instrument between public authorities or bodies (Art. 46 (2) (a);
c) binding corporate rules (Art.46 (2) (b);
d) standard data protection clauses adopted by the European Commission in accordance with the examination procedure (Art. 46 (2) (c);
e) standard data protection clauses adopted by the supervisory authority and approved by the European Commission in accordance with the examination procedure (Art. 46 (2) (d);
f) approved codes of conduct in accordance with Art. 40 together with binding and enforceable commitments of the controller or processor in a third country to apply appropriate safeguards, including as regards data subjects' rights (Art. 46 (2) (e);
g) approved certification mechanisms in accordance with Art. 42 together with binding and enforceable commitments of the controller or processor in a third country to apply appropriate safeguards, including with regard to the rights of data subjects (Art. 46 (2) (f);
h) contractual clauses between the controller or processor and the controller, processor or recipient of personal data in a third country or international organization (Art. 46 (3) (a);
i) the provisions of administrative arrangements between public authorities or bodies providing for enforceable and effective rights of data subjects (Art. 46 [3] [b]).

an Commission to allow in practice a free transfer of data between designed states or territories. This may possibly happen only with the State of California and in conclusions included in the last part of this paper I try to indicate whether this is possible at all. The main objective of this article is to examine whether the State of California by implementing the Consumer Protection Act has steered a course to provide an adequate level of personal data protection. Discussing or explaining all the aspects of granting an adequacy decision may stretch the scope of this article a step too far. Therefore, for the reasons spelled out broadly below, I will only focus on one specific aspect of both regulations i.e. processing children's data under the CCPA and the GDPR.

II. Protecting children's personal data under the GDPR

Recital 38 of the Regulation notes that children need special protection in the processing of 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. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The EU legislator deals with the above problem directly in Art. 8 of GDPR. Pursuant to this provision, in the case of information society services offered directly to a child, the processing of personal data of a child who has reached the age of 16 is legal. If the child is under 16 years of age, such processing is lawful only if and to the extent that the consent is given or authorised by a person who exercises the parental authority over a child or acts as a child's custodian. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child. Member States may set a lower age limit in their legislation providing they abide by the rule of the minimum age of 13. However, there are serious doubts whether such consent/the choice may be effective or not due to the lack or limitation of legal capacity[5]. Data controller providing a cross-border

[5] M. Giermak, M. Sofronów, *Zgoda na przetwarzanie danych osobowych dzieci w serwisach społecznościowych w kontekście zmian prawa europejskiego,* "Monitor Prawniczy" 2017, no. 2, p. 12.

service may not always rely on complying with only the law of the Member State in which it has his main establishment, but may need to comply with the respective national laws of each Member State in which he offers the information society services[6].

The obligation to check whether the child consenting to the processing of data has the authority to do so or not is a logical consequence of the accountability principle and manifests itself in the double opt-in model, i.e. obtaining the consent of a custodial parent or guardian by telephone, using traditional correspondence or other authorization methods (registration, giving date of birth, etc.)[7].

Regulations contained in Art. 8 refer only to information society services in the meaning of Art. 1.1 (b) of Directive (EU) 2015/1535 of the European Parliament and of the Council of September 9, 2015. Nonetheless, Art. 8 does not apply to all information society services, but only those offered directly to children. The literature indicates that services offered directly to the child are only those aimed directly or exclusively at children and intended to arouse their interest. What is instrumental in this case is the provider's attitude to the interaction with children rather than a theoretical possibility of linking the subject of the service with a child[8]. In practice, it cannot be expected of every service provider to explicitly state on their websites that a specific service is directed at adults only. Such a stipulation is justified only when it is required by law, i.e. in the case of selling alcohol and tobacco, gambling or betting-related services or in the case of content unsuitable for children (including vulgarisms, nudity, violence). At the same time, Art. 8 will apply to services targeted at both children and adult users[9].

Actions are also needed to raise parents' awareness and take an appropriate steps to prevent them from violating the child's privacy online. Browsing social networking sites, one can find thousands of photos depicting children

---

[6] Art. 29 Working Party, Guidelines on consent under Regulation 2016/679, WP259 rev. 01.

[7] D. Lubasz, *Komentarz do art 6,* [in:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, eds. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, Lex.

[8] S. Schulz, *Article 6,* [in:] *DS-GVO Datenschutz-Grundverodung VO (EU) 2016/679. Kommentar,* ed. P. Gola, C.H. Beck 2017, p. 39.

[9] Ibidem.

in embarrassing situations or parents sharing stories about "funny" situations involving minors[10]. When, prior to publishing, editors asked a child if he or she would want to become a social media hero of the day on the Internet, the child did not seem to have the full understanding of the decision that he or she was making. Children tend to protect their privacy and intimacy in a very natural way even though they are ignorant of mechanisms of social networking. The publication of a child's image by the parent on the Internet leads to the conclusion that many parents assume that they own their child's privacy and control it to the same degree they control their own privacy, and that the privacy of a child and that of his or her parent is of the same nature.

The EU legislator is also trying to tackle this problem by pointing out in Recital 65 of the Regulation that the right to have one's personal data erased (the right to be forgotten) is particularly important when the data subject has given his or her consent as a child and is not fully aware of the risks involved in the processing and later wants to remove such personal data, especially on the Internet. Using the *minori ad maius* as the rule of interpretation, it can be stated that recital 65 will also apply in the event of the individual who being a child did not consent to the processing of his personal data whilst the entity which indirectly provided the data to the data controller was his or her parent or legal guardian. With regard to all personal data which were shared by a child's parents, the right to request erasing personal data follows directly from Art. 17.1(d) on the account of one's right to have unlawfully processed data erased.

III. Protecting children's personal information under the California Consumer Privacy Act

The California Consumer Privacy Act is a new regulation that took effect from January 1st, 2020 in the state of California. For the first time, a matter of protecting personal information[11] has been regulated in a comprehensive man-

[10] Nominet, *Today's children will feature in almost 1,000 online photos by the time they reach age five*, https://www.nominet.uk/todays-children-will-feature-in-almost-1000-online-photos-by-the-time-they-reach-age-five (10.10.2022).

[11] It is important to mention on the side note that definition of personal data used in GDPR and definition of personal information included in CCPA are slightly different. Personal

ner in a single legal act. At the same time, it should be emphasized that its scope is limited and applies to businesses that collect information from California residents and meet at least one of the very specific thresholds[12]. The law is enforceable in California and applies to California users, but given the nature of data processing, most companies will need to consider whether to apply the rules to all users.

The CCPA also introduces special regulations relating to the processing of children's personal data. They complement the provisions of the Children's Online Privacy Protection Act (COPPA), which applies throughout the United States and imposes special obligations on entrepreneurs when processing personal data of children aged 13–16.

The COPPA mainly applies to commercial websites and online services targeting children aged under 13. Websites not targeting children – the so-called general audience websites – having 'actual knowledge' that they collect personal data from a child also fall within the scope of the COPPA. Service providers who are subjects of the COPPA regulations are obliged to: '(i) to provide notice on the website on what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information; and (ii) to obtain verifiable parental consent for the collection, use, or disclosure of personal information from children'. A website shall also include clear information that children's personal data may be collected. Additionally, parents or guardians

Information includes not only traditional forms of personally identifiable information, but also IP addresses, geolocation, and "unique identifiers" such as device IDs, cookie IDs, and Internet activity information including browsing history and search history. Inferences drawn from the types of information described above "to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behaviours, attitudes, intelligence, abilities, and aptitudes" are also included under the definition of personal information, similar to the definition of 'profiling' under GDPR which restricts the use of personal data to analyse or predict aspects a person's personal preferences, interests, reliability, behaviour, location or movements. What is different and perhaps more expansive than the GDPR is that CCPA would treat information relating to "a household" as personal information.

[12] (1) have over $25 million in annual gross revenue; (2) buy, receive, sell, or share for commercial purposes the personal information of 50,000 or more consumers, households, or devices; or (3) derive 50 percent or more of their revenue from the sale of consumers' personal information.

shall be informed of data processing including what the website owners intend to do with the information and whether or not they intend to disclose the children's personal information to third parties. This obligation can be fulfilled by including a 'clear and prominent' notice online of the site's information practices[13].

It is also important to mention that under the laws of the State of California, there has also been legislation geared toward protecting children, such as Section 22581 of California's Business and Professions Code, which "requires that websites and apps allow minors to take down content they previously posted". Although this is progress, the issue still remains that even if a website such as Facebook allows a minor to remove a photo that he or she had put up earlier, the photo may have been disseminated to third-party websites already by the time the user removes it[14].

In addition to the above regulations, the CCPA requires that businesses that have actual knowledge that they collect personal information from children under 13 must "establish, document, and comply with a reasonable method" for verifying that the personal authorizing the sale of a child's data is actually that child's parent or guardian. Furthermore, the regulation lists several methods which are "reasonably calculated" to ensure that is the case including providing a signed consent form under penalty of perjury; requiring parents or guardians to use payment methods such as credit cards that provide notification of each transaction; asking the parent or guardian to communicate in person with trained personnel, either through a toll-free line or videoconference; or verifying the parent or guardian against a government database, and then promptly deleting their personal data from the business's database. Business is also obliged to notify parents of their rights to opt out of the sale of their child's personal information. The CCPA does not clarify whether actual knowledge is sufficient or not. Hence businesses shall consider looking to COPPA standards in this situation.

Under the CCPA businesses need to fulfil the obligation to establish, document, and comply with a reasonable process to allow minors to opt in to the

---

[13] E. Bartoli, *Children's Data Protection vs Marketing Companies*, "International Review of Law, Computers and Technology" vol. 23, iss. 1–2, pp. 35–45.

[14] D. Park, *Mining for Children's Data in Today's Digital World*, "Journal of Association of Administrative Law Judiciary" vol. 28, iss. 1, pp. 321–352.

sale of their personal information, and inform them of their right to opt out of such sale at a later date. On the other hand, even if businesses exclusively target offers of goods or services directly to consumers under 16 years old though sell their personal information without affirmative authorization, or the affirmative authorization of the child's parent or guardian, there is no need to fulfil the obligation to provide notice of the right to opt out.

The question remains whether, in the light of European regulations, the solutions adopted by the legislator in California are sufficient to provide children with an adequate level of protection.

IV. Is the protection adequate?

The provision of Art. 45 of the GDPR gives the European Commission the competence to recognize that a third country or an international organization ensures an adequate level of protection of personal data. The Commission shall then make a decision to this effect. Once an adequacy decision has been adopted, the transfer of data to the third country or international organization indicated in the decision does not require fulfilment of the other conditions. According to Recital 103, the Commission may conclude with effect for the whole of the Union that a third country – or a territory or a particular sector in a third country – or an international organization ensures an adequate level of data protection. This is to guarantee certainty and uniformity in the application of the law throughout the Union in relation to third countries or international organizations which have been recognized as providing such a degree of protection.

Clearly, on making its decisions, the Commission does not take into account the issue relating strictly to the matter of the personal data protection in a given third country or international organization. The EU legislator has rightly strived to ensure that a genuine guarantee of an adequate level of personal data protection can only be offered by the third countries and international organizations which fully recognize the principles of the rule of law and those of human rights, as well as honour their international commitments. It is also important that one of the conditions of the adequacy decision is to establish an independent personal data protection authority by the applicant state.

In the context of the issue of processing personal data of children in the digital services discussed in this paper, it should be stated that except for the minimum age factor in endorsing a child's data protection consent, the other regulations differ significantly. The CPPA requires parental consent for personal information sale, while GDPR makes it a condition applicable to all processing consent requests. In this respect, the solutions adopted in the CCPA do not provide a level of protection that would be close to the one laid down in the GDPR. From the perspective of the European model, the protection granted in the CCPA in this respect does not guarantee the security of a child's privacy and his or her personal data. After all, it is possible that a child's personal information may even if not destined for sale be used for such purpose as profiling, and as a consequence, lead to discrimination or manipulation.

Importantly, the CPPA offers a greater clarity as regards the rules on the methods of obtaining the parent or guardian authorization as businesses are landed with the obligation to take reasonable steps to ensure that the person authorizing consent for the sale of a child's data on his or her behalf is their actual parent or legal guardian. However, this applies only for selling children's data, which is generally forbidden (in relation to all categories of data) under the GDPR. This takes aim at the ease with which children can forge parental signatures or other means of giving consent, and prevents businesses to turn a blind eye to the reasonableness of their consent mechanisms, if they have actual knowledge that children under 13 use their websites. The requirements apply to businesses having actual knowledge that they collect personal information from children and minors, so this may discourage mixed age websites from age-gating or otherwise asking the age of their to escape the compliance with the above requirements.

It should be noted that the CCPA applies to consumer-entrepreneur relations only and ignores an adequate protection to the individual (including children) in relations with state authorities. Doubts are also raised by the fact that in many cases state and federal authorities have so far taken measures to weaken, rather than protect, children's rights in this respect[15]. The Elec-

[15] S. Hunt, *Data Collection on School-Aged Children through Common Core*, "Journal of Law and Policy for the Information Society" vol. 12, iss. 2, pp. 306–326.

tronic Privacy Information Centre also emphasizes that authorities whose purpose should be to protect children's rights are promoting regulations that undercut student privacy and parental consent[16].

It should be pointed out, in the context of ensuring extensive guarantees of children's rights to privacy and personal data protection, that the United States have not ratified the Convention on the Rights of the Child yet. This is one of the most important international laws guaranteeing the protection of children's privacy. It is obvious that this premise cannot be regarded as the only one which may itself prevent the European Commission from giving an adequacy decision to California although it will certainly be taken into account and hardly support the case in any positive way.

V. Conclusions

In summary, the regulations adopted in the CCPA are admittedly in many respects similar to those contained in the GDPR, but they cannot be considered sufficient to assume that the State of California has provided an adequate level of personal data (information) protection. From the point of view of the European model, the regulation introduced in California may head in the right direction, but it is still not enough for the European Commission to give an adequacy decision. First of all, the CCPA only deals with the relationship between private law entities and in no way protects the individual in its relations with public authorities. In addition, the introduced solutions do not provide for the existence of a dedicated body that would protect the enjoyment of the freedoms and rights in the area of the right to privacy. It is worth noting, however, that in terms of the authorization mechanisms for the sale of children's personal information, the CCPA contains safer solutions than those introduced in the GDPR. First of all, with the methods of checking the origin of consent specified in the law, businesses have a greater peace of mind. However, there are doubts whether such consent may only

[16] J. Reidenberg et al., *Children's Educational Records and Privacy: A Study of Elementary and Secondary School State Reporting Systems,* CLIP REPORT (Fordham Ctr. on Law and Info. Policy), October 28, 2009, http://aw.fordham.edu/assets/CLIP/CLIP Report Childrens Privacy Final.pdf (10.10.2022).

applies to situations in which personal data is sold, and therefore it would not be necessary for other data processing activities.

It seems that until the United States adopts a regulation that protects the rights of the individual to a greater extent, and above all, ensure the protection in the individual's relations with the state, the transfer of data shall rely on standard transfer mechanisms (wherever possible according to CJEU ruling in Schrems II), as adequacy decision cannot be released by European Commission.

Literature

Bartoli E., *Children's Data Protection vs Marketing Companies*, *Children's Data Protection vs Marketing Companies*, "International Review of Law, Computers and Technology" vol. 23, iss. 1–2.

RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, eds. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018.

Giermak M., Sofronów M., *Zgoda na przetwarzanie danych osobowych dzieci w serwisach społecznościowych w kontekście zmian prawa europejskiego*, "Monitor Prawniczy" 2017, no. 2.

DS-GVO Datenschutz-Grundverodung VO (EU) 2016/679. Kommentar, ed. P. Gola, C.H. Beck 2017.

Hunt S., *Data Collection on School-Aged Children through Common Core*, "Journal of Law and Policy for the Information Society" vol. 12, iss. 2.

Nominet, *Today's children will feature in almost 1,000 online photos by the time they reach age five*, https://www.nominet.uk/todays-children-will-feature-in-almost-1000-online-photos-by-the-time-they-reach-age-five.

Park D., *Mining for Children's Data in Today's Digital World*, *Mining for Children's Data in Today's Digital World*, "Journal of Association of Administrative Law Judiciary" vol. 28, iss. 1.

Reidenberg J. et al., *Children's Educational Records and Privacy: A Study of Elementary and Secondary School State Reporting Systems*, CLIP REPORT (Fordham Ctr. on Law and Info. Policy), October 28, 2009, http://aw.fordham.edu/assets/CLIP/CLIP Report Childrens Privacy Final.pdf.