

## Does The GDPR Achieve Its Goal of “Protection of Youth”?



Ammar Younas<sup>1</sup>, Yulduz Akhtamovna Akhtamova<sup>2</sup>

<sup>1</sup>PhD(Candidate), School of Humanities, University of Chinese Academy of Sciences Beijing China

<sup>2</sup> Tashkent state university of law

**ABSTRACT:** The increasing ‘datafication of society’<sup>1</sup> and ubiquitous computing resulted in high privacy risks such as commercial exploitation of personal data, discrimination, identity theft and profiling (automated processing of personal data).<sup>2</sup> Especially, minor data subjects are more likely to be victims of unfair commercial practices due to their behavioral characteristics (emotional volatility and impulsiveness) and unawareness of consequences of their virtual activities.<sup>3</sup> Accordingly, it has been claimed that thousands of mobile apps utilized by children collected their data and used it for tracking their location, processed it for the development of child profiles so as to tailor behavioral advertising targeted at them and shared it with third parties without children’s or parent’s knowledge.<sup>4</sup> Following these concerns, recently adopted EU General Data Protection Regulation (679/2016) departed from its Data Protection Directive (DPD) in terms of children’s data protection by explicitly recognizing that minors need more protection than adults<sup>5</sup> and providing specific provisions aimed at protecting children’s right to data protection.<sup>6</sup> Unlike the GDPR, the DPD was designed to provide “equal” protection for all data subjects irrespective of their age.<sup>7</sup> This paper argues that consent principle along with the requirement of parental consent cannot effectively be implemented for the protection of children’s data due to the lack of actual choice, verification issues and complexity of data processing, and also the outcome of the privacy notices in a child-appropriate form is limited. However, there are other mechanisms and restrictions embodied in the GDPR, which provide opportunities for the protection of children’s data by placing burden on data controllers rather than data subjects.

### ALLOCATION OF YOUTH PROTECTION CONCERN WITHIN THE GDPR FRAMEWORK

The protection of children’s data is explicitly or implicitly specified in particular provisions and recitals of the GDPR. Article 8 of the GDPR provides ‘conditions applicable to a child’s consent in relation to information society services’ being directly offered to a child.<sup>8</sup> Under the GDPR “clear” consent and “explicit” consent of the data subjects is one of the legitimate grounds for processing personal data and special category data respectively.<sup>9</sup> Thus, if a data controller intends to use children’s data and relies on consent in order to legitimize potential data processing, he must satisfy conditions provided in article 8, which states that ‘the processing of the personal data of a child shall be lawful where the child is at least 16 years old’ or where the child is below the age of 16, the holder of parental responsibility over the child has given or authorized consent. Also, the data controller is obliged to undertake reasonable efforts so as to verify parental consent in the light of available technology.<sup>10</sup> Furthermore, the provision leaves a room

<sup>1</sup> Dana Volosevici, ‘Child Protection Under GDPR’ (2019) 6 (22) *Jus et Civitas : Journal of Social and Legal Studies* pp.17

<sup>2</sup> Ingrida Milkaite and Eva Lievens, ‘Children’s Rights to Privacy and Data Protection Around the World: Challenges in the Digital Realm’ (2019) 10 (1) *European Journal of Law and Technology*

<sup>3</sup> *Ibid*

<sup>4</sup> Jennifer Valentino-Devries and others, ‘How Game Apps That Captivate Kids Have Been Collecting Their Data’ *New York Times* (12 September 2008) < <https://www.nytimes.com/interactive/2018/09/12/technology/kids-apps-data-privacy-google-twitter.html> > accessed 25 February 2020

<sup>5</sup> The European Parliament and the Council Regulation (EU) 2016/679 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) [2016] OJ L 119/1, Recital 38

<sup>6</sup> *Ibid* Articles 8, 12, 17, 40

<sup>7</sup> The European Parliament and the Council Directive 95/46/EC 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] OJ L 281/31

<sup>8</sup> The GDPR (n 5) Art 8

<sup>9</sup> *Ibid* Art.6 (a), 9.

<sup>10</sup> *Ibid* Art. 8 (2)

## Does The GDPR Achieve Its Goal of “Protection of Youth”?

for maneuver enabling Member States to derogate from the general rule and set a lower age than 16, provided that it is not below 13 years.<sup>11</sup> Accordingly, age threshold for children’s consent varies between 13 and 16 in the EU in accordance with the private laws of Member States, with ten states requiring 16 years, three states 15 years, six states 14 years and nine states 13 years.<sup>12</sup> Another fundamental principle of the GDPR designed to strengthen child’s right to data protection is the provision of transparent information. The GDPR requires data controllers to provide data subjects with particular information prior to collecting personal data and obtaining consent in order to ensure fair and transparent processing.<sup>13</sup> According to article 29 Working Party (WP), the provision of information prior to obtaining data subject’s consent is important so as to allow them to make informed decisions and understand what they are consenting to, and if the data controller fails to comply with the requirements for informed consent, it becomes an invalid basis for processing.<sup>14</sup> Moreover, article 29 WP offers a minimum content of the information to be provided for valid ‘informed’ consent such as the contact details of the controller, the purpose of each of the processing operations for which consent is requested, the type of data being processed and information about the use of the data for automated decision making.<sup>15</sup>

As regards “transparency” of the information to be provided, recital 39 GDPR states that ‘it should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed’. Furthermore, article 12 requires data controllers to provide any information relating to processing activities ‘in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child’.<sup>16</sup> Accordingly, article 12 (7) suggests using ‘standardized icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing’.<sup>17</sup> Further clarification is provided by recital 58 GDPR stating that ‘any information and communication, where processing is addressed to a child, should be in such a plain and clear language that the child can easily understand’.<sup>18</sup> However, neither article 12 nor recital 58 specifies methods or designs for providing such transparent information to minor data subjects. Only article 29 WP notes that when transparency information is targeted at children specifically, different types of measures accessible to children should be considered by data controllers such as pictograms, comics/cartoons and animations among others.<sup>19</sup>

The right to erasure (right to be forgotten) is also one of the vital principles adopted by the GDPR, which is available to children. Under article 17, data subjects are entitled to obtain from the data controller the erasure of personal data relating to them without undue delay under certain.<sup>20</sup> Recital 65 states that ‘the 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’.<sup>21</sup> Moreover, the data subject is entitled to exercise that right regardless of the fact that he or she is no longer a child.<sup>22</sup>

Furthermore, the GDPR prohibits certain potentially detrimental data collection and processing operations by restrictions on the activities of data controllers. Recital 38 mentions that children should be provided specific protection against profiling or marketing.<sup>23</sup> However, article 22 of the GDPR, which regulates profiling, does not specify children’s protection. Nevertheless, Recital 71 provides that automated decision making based on profiling should not deal with children.<sup>24</sup> Therefore, it can be deemed that the profiling of children’s data is prohibited although such prohibition is not explicitly specified in the GDPR articles.<sup>25</sup>

### THE EFFECTIVENESS AND IMPLEMENTATION OF THE CONSENT PRINCIPLE

The requirement of parental consent or authorization prior to the processing of children’s personal data where ‘information society services’ is directly offered to children (Article 8) is probably most questionable and essential protective mechanism

---

<sup>11</sup> Ibid Art.8 para 1

<sup>12</sup> Volosevici (n1) pp.18

<sup>13</sup> The GDPR (n 5) Art.7,13, 14

<sup>14</sup> Article 29 Working Party, *Guidelines on Consent under Regulation 2016/679* (28 November 2017) pp.12

<sup>15</sup> Ibid pp.13

<sup>16</sup> The GDPR (n5) Art.12 (1)

<sup>17</sup> Ibid Art.12 (7)

<sup>18</sup> Ibid Recital 58

<sup>19</sup> 29 Working Party, *Guidelines on Transparency under Regulation 2016/679* ( 11 April 2018) pp.12

<sup>20</sup> The GDPR (n5) Art.17

<sup>21</sup> Ibid Recital 65

<sup>22</sup> Ibid

<sup>23</sup> Ibid Recital 38

<sup>24</sup> Ibid Recital 71

<sup>25</sup> Milda Macenaite ‘From universal toward child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation’ (2017) 19 (5) *New Media & Society* pp.771 <<https://doi.org/10.1177/1461444816686327>> accessed 25 February 2020

## Does The GDPR Achieve Its Goal of “Protection of Youth”?

adopted by the GDPR. Specifically, the principle of children’s and parental consent demonstrates theoretical uncertainties and practical implementation challenges.

Firstly, determination of the legal capacity of children to consent to data processing is a complicated task.<sup>26</sup> In particular, the complexity of setting an age specific capacity threshold is associated with the evolving nature of childhood, which means children’s needs and capacities change with their physical, emotional and cognitive development.<sup>27</sup> Therefore, although the protection and empowerment elements should be balanced in accordance with the child’s age and maturity, it is problematic to evaluate when an individual child is competent to take responsibility for his or her data protection.<sup>28</sup> Article 8 assumes that children above 16 (unless lower age is set by Member States) are able to give consent for lawful processing of their personal data. However, conclusive empirical evidence does not exist about specific age at which children comprehend these decisions and there is no any justification given by the European legislator as to why the ages 13 and 16 are selected in particular.<sup>29</sup> Moreover, the expected harmonization cannot be achieved within the EU as children are supposed to consent to data processing at various ages depending on the Member States that they live in. It results in uncertainty in relation to cross-border services as the data controllers will be confused about the age that they have to take into account when offering cross-border services throughout the EU.<sup>30</sup>

Secondly, the protection offered by the mechanism of consent is frequently found to be illusory. Specifically, consent suggests that the data subjects are entitled to control over their personal data, which means that the data subjects are given a meaningful choice and they comprehend data processing operations of the data controllers.<sup>31</sup> Also, the GDPR requires consent to be ‘freely given’<sup>32</sup> but if the data subjects want to sign up for online services, company’s privacy policies is offered on a take-it-or-leave-it basis, which means they do not have any other choice than consenting to the privacy policy as long as it is not negotiable.<sup>33</sup>

Thirdly, the requirement of parental consent is criticized to be over-protective, which can lead to the restriction of children’s opportunities and violation of their fundamental rights such as freedom of expression and rights to development.<sup>34</sup> In particular, the scope of the requirement of parental consent mechanism is very broad and there are no any exceptions to it. For example, an Information Society Service is ‘any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient services’<sup>35</sup>, which means that parental consent should be obtained for all types of services in various sectors including entertainment sites, online gaming, instant messaging, social media and email services.<sup>36</sup> In that sense, this mechanism may fail in two ways: where an excessive consent requests may lead to ‘consent fatigue’ among parents by making consenting process ‘a disturbing irritation’ rather than serious decision;<sup>37</sup> or where children and parents may frequently have conflicting interests and preferences, parental consent requirement will result in rejections of consent requests from parents thereby, restricting children’s freedom of expression<sup>38</sup>, the right to development<sup>39</sup> and participation (embodied in UNCRC).<sup>40</sup> Moreover, as a result of this mechanism, children can be deprived of using certain social media or other services as companies decide to set age limits for subscription so as to avoid troublesome parental consent requirement.<sup>41</sup> For instance, Google has banned the creation of accounts on its platforms by minor users for whom parental consent is needed.<sup>42</sup>

Lastly, under article 8 of the GDPR, the data controller is obliged to undertake reasonable efforts to verify parental consent or authorization taking into account the state of the art of the available technology.<sup>43</sup> However, it does not specify any acceptable

---

<sup>26</sup> Milda Macenaite and Eleni Kosta ‘Consent for processing children’s personal data in the EU: following in US footsteps?’ (2017) 26 (2) Information & Communication Law pp.151 <<https://doi.org/10.1080/13600834.2017.1321096>> accessed 27 February 2020

<sup>27</sup> Ibid

<sup>28</sup> Macenaite (n31) pp.767

<sup>29</sup> Milkaite and Lievens (n2)

<sup>30</sup> Hof and Lievens (n12) pp.9

<sup>31</sup> 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’ (2018) 23 (1) Communications Law pp.3

<sup>32</sup> The GDPR (n5) Art. 4 (11)

<sup>33</sup> Hof and Lievens (n37)

<sup>34</sup> Macenaite (n31) pp.772

<sup>35</sup> EU Directive 2015/1535 Art. 1 (1) (b)

<sup>36</sup> Macenaite (n31) pp.772

<sup>37</sup> Ibid pp.773

<sup>38</sup> The United Nations Convention on the Rights of the Child (UNCRC) 1989, Art.13

<sup>39</sup> Ibid Art.6

<sup>40</sup> Ibid Art.12

<sup>41</sup> Hof and Lievens (n37) pp.35

<sup>42</sup> Ibid

<sup>43</sup> The GDPR (n5) Art.8 (2)

## Does The GDPR Achieve Its Goal of “Protection of Youth”?

methods for obtaining verifiable parental consent. This uncertainty causes implementation difficulties in terms of parental consent verification. Furthermore, the GDPR does not impose any obligation on the data controllers with regard to age verification of minor data subjects. It allows the data subjects to provide a false age thereby, making this protection tool ineffective.<sup>44</sup> As the EU imported parental consent requirement from the US Children’s Online Privacy Protection Act (COPPA), which has practiced this principle for two decades, its efficacy can be assessed in the light of the US case. It is claimed that lack of age verification principle along with appropriate methods undermined the effectiveness of the COPPA to a great extent in terms of youth protection<sup>45</sup> Therefore, it is suggested that innovative methods of age verification must be adopted by the GDPR so as to strengthen the effective of its consent principle.<sup>46</sup>

### THE EFFECTIVENESS AND IMPLEMENTATION OF PROVISION OF CHILD-FRIENDLY INFORMATION

Under the GDPR, the data controllers are required to provide minor data subjects with transparent information about data processing prior to obtaining valid consent.<sup>47</sup> Transparent information plays a vital role in the protection of children as they will only be able to use their right if they know and comprehend what those rights are.<sup>48</sup> However, satisfying the requirements of ‘informed consent’ is complicated in case of minor data subjects owing to their level of comprehending and ability to predict possible consequences of the data processing.<sup>49</sup> Recital 58 GDPR mentions that ‘any information and communication, where processing is addressed to a child, in such a clear and plain language that the child can easily understand.’<sup>50</sup> Accordingly, the UK Data Protection Authority namely, the Information Commissioner’s Office recommends to deploy cartoons, graphics, diagrams, video and audio content and symbols to help children understand.<sup>51</sup>

Commonly, privacy policies are used by service providers as a means of providing information to the data subjects before collecting and processing the data. Milkaite and Lievens analyzed privacy policies of services that are very popular among minor data subjects in order to find out whether they comply with the requirements of transparency of the GDPR.<sup>52</sup> In particular, the list of information specified in articles 13 and 14 along with the language (child-friendly transparency level) provided by article 12 have been examined in the light of data processing policies of Instagram, Snapchat and TikTok.<sup>53</sup> The results of analysis in the context of article 12 revealed that although the text is structured by spacing, use of bullet points and bold headings, generally the text of policies remains long with more than 3000 words in all three cases and fairly difficult to understand (estimated age of the reader is 15-17 and 18-19 years).<sup>54</sup> They do not deploy visualization or icons as provided by the GDPR or other mechanisms as suggested by the ICO or 29 WP.<sup>55</sup> As regards analysis in relation to article 13, the most of the information specified in article 13 is provided by all three services.<sup>56</sup> Concerning the compliance with article 14, although the services mention that they obtain personal information about their users from other sources, they do not provide details of “third parties” or “business partners”.<sup>57</sup> Thus, it can be summarized that the provision of transparency information is not effectively implemented.

According to some commentators, the provision of information about data processing prior to obtaining informed consent is an ineffective mechanism for reinforcing the protection of children since children’s data is frequently collected and processed by systems in ‘proprietary black boxes’.<sup>58</sup> It is claimed that even the data controllers or designers themselves do not completely

---

<sup>44</sup> Hof and Lievens (n12) pp.10

<sup>45</sup> Macenaite and Kosta (n32) pp.191

<sup>46</sup> Ibid

<sup>47</sup> The GDPR (n5) Art. 12

<sup>48</sup> Hof and Lievens (n12)

<sup>49</sup> Macenaite and Kosta (n32) pp.157

<sup>50</sup> The GDPR (n5) Recital 58

<sup>51</sup> Information Commissioner’s Office ‘Age Appropriate Design: a code of practice for online services’ (2019) <<https://ico.org.uk/media/about-the-ico/consultations/2614762/age-appropriate-design-code-for-publicconsultation.pdf>> accessed 27 February 2020

<sup>52</sup> Ingrida Milkaite & Eva Lievens ‘Child-friendly transparency of data processing in the EU: from legal requirements to platform policies’ (2020)

14 (1) Journal of Children and Media <<https://doi.org/10.1080/17482798.2019.1701055>> accessed 28 February 2020

<sup>53</sup> Ibid pp.14

<sup>54</sup> Ibid

<sup>55</sup> Ibid

<sup>56</sup> ibid

<sup>57</sup> ibid

<sup>58</sup> Nathan Fisk ‘The Limits of Parental Consent in an Algorithmic World’ (LSE, *Media Policy Project Blog*, 28 November 2016) <<https://blogs.lse.ac.uk/medialse/2016/11/28/the-limits-of-parental-consent-in-an-algorithmic-world/>> accessed 27 February 2020

## Does The GDPR Achieve Its Goal of “Protection of Youth”?

understand algorithmic processing and do not know how and why some forms of output is produced by complicated systems.<sup>59</sup> Therefore, children and parents cannot be expected to be able to make informed decisions even under perfect conditions.<sup>60</sup>

### GENERAL MECHANISMS FOR CHILD PROTECTION IN THE GDPR

There are certain provisions included in the GDPR, which do not explicitly mention children but can be employed for reinforcing the protection of their data including the principles of privacy by design and privacy by default and data protection impact assessments.<sup>61</sup>

The principles of data protection by design and data protection by default require the controllers to integrate data protection requirements and safeguards into the design of their data processing systems.<sup>62</sup> Firstly, they can guarantee that data protection becomes an integral part of data processing systems without the data subjects necessarily needing to completely understand the complexities associated with internal data processing operations of controllers. Secondly, they give opportunities to incorporate individual control rights into the data systems operation thereby, making them effective and transparent.<sup>63</sup> These principles are regulated by article 25 GDPR, which specifies general data protection principles provided in article 5 to be implemented by these mechanisms.<sup>64</sup> However, it does not explicitly refer to children’s data protection or make any connection between them.<sup>65</sup> Although children still can enjoy the same level of data protection as afforded to adults, taking into account their vulnerability, specific children-oriented privacy by design and privacy by default measures will be needed.

As regards data protection impact assessments (DPIA), article 35 of the GDPR requires data controllers to assess the impact of processing operations, which are supposed to result in a high risk in relation to the rights and freedoms of data subjects before processing.<sup>66</sup> Although the GDPR does not explicitly mention the processing of children’s data as a processing operation that carries a high risk, a DPIA can be requested in the light of recital 38, which provides that ‘children merit a specific protection’.<sup>67</sup>

### CONCLUSION

In conclusion, provisions adopted by the GDPR can be classified as “child-focused instruments” and “general instruments” in the context of youth protection. As it is discussed in detail, child-focused mechanisms are those specifically designed to protect children’s personal data in the digital environment such as parental consent requirement, children’s consent and the provision of transparent information. The effective protection of children’s data cannot be achieved by these provisions due to their legal uncertainty, practical implementation challenges and adverse effects on fundamental rights of children. However, prohibition of the use of children’s data for profiling purposes and the provision of right to erasure can contribute to the protection of children to certain extent. In order to strengthen youth protection, the responsibility placed on the data subjects (parents and children) should be shifted to the data controllers by developing existing mechanisms of the GDPR. In particular, the application of general provisions such as data protection by design and data protection by default as well as DPIA to the protection of children’s data should be explicitly specified in the relevant articles of the GDPR.

### BIBLIOGRAPHY

- 1) Dana Volosevici, ‘Child Protection Under GDPR’ (2019) 6 (22) *Jus et Civitas : Journal of Social and Legal Studies* pp.17
- 2) Ingrida Milkaite and Eva Lievens, ‘Children’s Rights to Privacy and Data Protection Around the World: Challenges in the Digital Realm’ (2019) 10 (1) *European Journal of Law and Technology*
- 3) Jennifer Valentino-Devries and others, ‘How Game Apps That Captivate Kids Have Been Collecting Their Data’ *New York Times* (12 September 2008) < <https://www.nytimes.com/interactive/2018/09/12/technology/kids-apps-data-privacy-google-twitter.html> > accessed 25 February 2020
- 4) The European Parliament and the Council Regulation (EU) 2016/679 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) [2016] OJ L 119/1, Recital 38

---

<sup>59</sup> Ibid

<sup>60</sup> Ibid

<sup>61</sup> Macenaite (n31) pp.771

<sup>62</sup> Hof and Lievens (n37) pp.36

<sup>63</sup> Ibid

<sup>64</sup> The GDPR (n5) Art.25

<sup>65</sup> Hof and Lievens (n37) pp.37

<sup>66</sup> Ibid pp.38

<sup>67</sup> Ibid

## Does The GDPR Achieve Its Goal of “Protection of Youth”?

- 5) The European Parliament and the Council Directive 95/46/EC 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] OJ L 281/31
- 6) Article 29 Working Party, Guidelines on Consent under Regulation 2016/679 (28 November 2017) pp.12
- 7) 29 Working Party, Guidelines on Transparency under Regulation 2016/679 ( 11 April 2018) pp.12
- 8) Milda Macenaite ‘From universal toward child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation’ (2017) 19 (5) *New Media & Society* pp.771  
<<https://doi.org/10.1177/1461444816686327>> accessed 25 February 2020
- 9) Milda Macenaite and Eleni Kosta ‘Consent for processing children’s personal data in the EU: following in US footsteps?’ (2017) 26 (2) *Information & Communication Law* pp.151 <<https://doi.org/10.1080/13600834.2017.1321096>> accessed 27 February 2020
- 10) Turdialiev, M. A., & Komilov, B. (2020). The Legal Issues Of International Investment Activity In Uzbekistan: Critical Analysis And Legal Solutions. *The American Journal of Political Science Law and Criminology*, 2(12), 16-21.
- 11) Akramov, A., Mirzaraimov, B., Akhtamova, Y., & Turdaliyev, M. A. (2020). Prospects For The Development Of Trust Management In Uzbekistan. *Psychology and Education Journal*, 57(8), 530-535.
- 12) Narziev, O. (2021). The Perspectives Of The Establishment Of International Financial Centers In Uzbekistan And The Implementation Of English Law. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(4), 1104-1108.
- 13) ТУРДИАЛИЕВ, Мухаммад Али. "ЭРКИН ИҚТИСОДИЙ ЗОНАЛАР ДОИРАСИДА ИНГЛИЗ ҲУҚУҚИНИ ЖОРИЙ ЭТИШНИНГ ХОРИЖ ВА МИЛЛИЙ ТАЖРИБАСИ." *ЮРИСТ АХБОРОТНОМАСИ* 1.6 (2020): 151-158.
- 14) Akhtamova, Y., 2016. Protection of International Investments. Analysis of Certain Clauses in International Agreements. Uzbekistan Case Study. Analysis of Certain Clauses in International Agreements. Uzbekistan Case Study (March 25, 2016).
- 15) Yulduz Akhtamova , Akramov Akmal and Bakhodir Mirzaraimov, and. "Foreign experience related to the legislation and practice of trust management of property in business activities." *Збірник наукових праць ЛОГОΣ* (2020): 12-14.
- 16) Yulduz, Akhtamova. "BALANCING INVESTMENT PROTECTION AND STATE’S REGULATORY SPACE IN THE LIGHT OF INVESTMENT TREATY REGIME ABSTRACT." *Review of law sciences* 1. Спецвыпуск (2020).
- 17) Akramov, Akmal, Bakhodir Mirzaraimov, Yulduz Akhtamova, and Mukhammad Ali Turdaliyev. "Prospects For The Development Of Trust Management In Uzbekistan." *Psychology and Education Journal* 57, no. 8 (2020): 530-535.
- 18) Yulduz Akhtamova “EU Freedom Of Establishment And The Theories Of Incorporation In The Context Of Free Movement Of MNEs” *The American Journal of Social Science and Education Innovations* 2 (12) 2020: 303-312
- 19) Akramov, Akmal, et al. "Prospects For The Development Of Trust Management In Uzbekistan." *Psychology and Education Journal* 57.8 (2020): 530-535.
- 20) Akramov, Akmal, Bakhodir Mirzaraimov, and Yulduz Akhtamova. "Foreign experience related to the legislation and practice of trust management of property in business activities." *Збірник наукових праць ЛОГОΣ* (2020): 12-14.
- 21) Mirzaraimov B., 2020. Effective Measures Of Preventing Due Process Paranoia In International Arbitration. *The American Journal of Political Science Law and Criminology*, 2(11), pp.72-80.
- 22) 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’ (2018) 23 (1) *Communications Law* pp.3
- 23) Ingrida Milkaite & Eva Lievens ‘Child-friendly transparency of data processing in the EU: from legal requirements to platform policies’ (2020) 14 (1) *Journal of Children and Media* <<https://doi.org/10.1080/17482798.2019.1701055> > accessed 28 February