Published in International Journal of Human Rights on 25 July 2023

SAFEGUARDING THE CHILD'S RIGHT TO PRIVACY AND DATA PROTECTION IN THE EUROPEAN UNION AND CHINA: A TALE OF STATE DUTIES AND BUSINESS RESPONSIBILITIES

Keywords:

Children's rights; privacy; data protection; UNCRC; EU; China

Abstract:

The importance of strong legislative frameworks to guarantee children's privacy, agency and safety in the digital environment has been emphasised by the Committee on the Rights of the Child in its most recent General Comment. Both the EU and China, who(se Member States) are Parties to the United Nations Convention on the Rights of the Child, have adopted their own legislative frameworks for protecting children's rights to privacy and data protection in recent years. This article compares how these two distinct legislative frameworks safeguard these rights. The analysis focuses on the constitutional protection as well as on a comparison of the legislation that is currently in place, such as the General Data Protection Regulation in the EU and the Personal Information Protection Law, the Provisions on Online Protection of Children's Personal Data and other relevant regulations in China. More specifically, the article zooms in on the responsibilities emerging from these regulatory frameworks for private companies and platforms that process children's personal data. It ultimately aims to draw conclusions as to whether and how the child's rights to privacy and data protection are protected in different parts of the world where children use similar commercial apps and services.

Word count:

10571

Names of all authors: Valerie Verdoodt[1], Yueming Zhang [2], Eva Lievens [3]

Author details:

1. Dr. Valerie Verdoodt, valerie.verdoodt@ugent.be , Law & Technology research group, Department of Interdisciplinary Study of Law, Private Law and Business Law, Faculty of Law and Criminology, Ghent University, Belgium
2. Yueming Zhang, yueming.zhang@ugent.be , Law & Technology research group, Department of Interdisciplinary Study of Law, Private Law and Business Law, Faculty of Law and Criminology, Ghent University, Belgium
3. Prof. Dr. Eva Lievens, eva.lievens@ugent.be , Law & Technology research group, Department of Interdisciplinary Study of Law, Private Law and Business Law, Faculty of Law and Criminology, Ghent University, Belgium

Corresponding author: Yueming Zhang, Volderstraat 5, 9000 Ghent, Belgium. yueming.zhang@ugent.be

Declarations: The authors' funding sources had no involvement in the study design, the interpretation of the data, the writing of the article nor in the decision to submit the article for publication. Valerie Verdoodt's contribution for this article was funded and created in the context of the BOF Postdoctoral Research Project "Children's rights and the monetisation of play in the digital environment", funded by the Special Research Fund of Ghent University (no. BOF.PDO.2021.0034.01). Yueming Zhang's contribution for this article was funded and created in the context of the research project "The protection of EU consumer data transferred to China", cofounded by the scholarship program of China Scholarship Council and the Special Research Fund of Ghent University (no. BOF.CHN.2019.0009.01).

I. Introduction

Children growing up today are argued to be a 'datafied' generation.[1] They have an online presence from a very young age and digital technologies play a role in every aspect of their lives. Social media platforms in particular have become central to children's social lives,[2] as an avenue for information, creation, socialisation and entertainment. However, through their social media engagement, children take part of a vast global ecosystem in which immense amounts of their personal data are continuously collected and processed.[3] This affects a number of children's rights that are laid down in the United Nations Convention on the Rights of the Child (UNCRC), such as the right to privacy (Article 16 UNCRC)[4] and the right to protection from economic exploitation (Article 32 UNCRC).[5] On 4 March 2021, the UN Committee on the Rights of the Child (CRC Committee) adopted its General Comment no. 25 on children's rights in relation to the digital environment (GC 25),[6] officially recognising that children's rights apply online as well as offline.[7] It sets out why and how State Parties should act to realise children's rights in a digital world. The section on the right to privacy is extensive and starts by acknowledging that privacy is vital to children's agency, dignity and safety and for the exercise of their rights. In that regard, the Committee pays a lot of attention to the benefits and risks of processing of children's personal data. Commercial risks related to datafication, profiling and advertising, in particular, are highlighted, as well as the important role businesses play in realising children's rights online.[8]

The UNCRC is ratified by 196 State Parties,[9] in all of which – to a greater or lesser extent – children's lives are enriched and challenged by digital technologies.[10] Yet, scientific research related to children's digital rights has mostly focused on Western countries, and more specifically Europe and the United States (incidentally the only country that has not ratified the UNCRC). The Global Kids Online project[11] does extend research to countries in other continents, such as Brazil and India. However, research comparing how children's rights are protected in the EU and China remains scarce. Statistics from December 2020 show that there are 989 million Internet users in China, of which 16.6% are younger than 19, and 3.1% are

[1] Deborah Lupton and Ben Williamson, 'The Datafied Child: The Dataveillance of Children and Implications for Their Rights' (2017) 19 New Media & Society 780.
[2] David Smahel and others, *EU Kids Online 2020: Survey Results from 19 Countries* (2020) 28.
[3] Kathryn C Montgomery and Jeff Chester, 'Data Protection for Youth in the Digital Age' (2015) 1 European Data Protection Law Review (EDPL) 277.
[4] Ingrida Milkaite and Eva Lievens, 'Children's Rights to Privacy and Data Protection Around the World: Challenges in the Digital Realm' (2019) 10 European Journal of Law and Technology <https://ejlt.org/index.php/ejlt/article/view/674> accessed 17 June 2022. According to Article 16 UNCRC, '*no children 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*'.
[5] Simone Van der Hof and others, 'The Child's Right to Protection against Economic Exploitation in the Digital World' (2020) 28 The International Journal of Children's Rights.
[6] United Nations Committee on the Rights of the Child, 'General Comment No. 25 on the Rights of the Child in the Digital Environment' (2 March 2021).
[7] Sonia Livingstone, 'Children's Rights Apply in the Digital World!' (*Media@LSE*, 4 February 2021) <https://blogs.lse.ac.uk/medialse/2021/02/04/childrens-rights-apply-in-the-digital-world/> accessed 20 December 2022.
[8] United Nations Committee on the Rights of the Child (n 6). See paras 35-42, 61, 68, 75, 103 and 110.
[9] For more information about the status of ratification, see Livingstone (n 7).
[10] UNICEF, 'The State of the World's Children 2017: Children in a Digital World' (*UNICEF*, 2017) <https://www.unicef.org/publications/index_101992.html> accessed 20 December 2022.
[11] For more information see'Global Kids Online | Children's Rights in the Digital Age' <http://globalkidsonline.net/> accessed 20 December 2022.

younger than 10 years old.[12] As a result of the fast globalisation of China's IT industry, the products and services of Chinese companies such as Huawei, Alibaba or Tencent have become omnipresent in other parts of the world. Among children, for instance, TikTok, a video-sharing platform owned by the Chinese parent company ByteDance, has become very popular. While TikTok is the app that is known to children across the world, children in China know this app as Douyin.[13] The platform's strategy - a combination of easy access and addictive scrolling - has proven to be a big hit.[14] By June 2021, the TikTok app surpassed 2.6 billion downloads worldwide, with 62% of its users aged between 6 and 24 years old.[15] In China, up to 42 million users younger than 19 use Douyin every day.[16] Considering that both EU and Chinese children are using similar apps and services offered by globally operating platform providers, this article investigates how the child's rights to privacy and data protection are protected in the EU and in China. Equal attention is paid to both frameworks to shed a comparative light on the realisation of these rights and the corresponding responsibilities for platform providers. In doing so, the article aims to uncover whether and how Article 16 UNCRC leads to divergent legislative frameworks across continents.

This article explores the UNCRC and the regulatory frameworks in the EU and China regarding the child's rights to privacy and data protection. The analysis focuses on the constitutional protection as well as on a comparison of the legislation that is currently in place, such as the General Data Protection Regulation (GDPR) in the EU and the Personal Information Protection Law (PIPL), the Provisions on Online Protection of Children's Personal Data and other relevant regulations in China. Its main focus is on the processing of children's personal data by private companies and platforms, and their responsibilities under these regulatory frameworks in respect of children.[17] It ultimately aims to draw conclusions as to whether and how the child's rights to privacy and data protection are protected in different parts of the world where similar commercial apps are being used.

II. The UNCRC and the General Comment No. 25

A. The UNCRC and its Legal Status in the EU and China

More than 30 years after its adoption in 1989, the UNCRC remains the key framework for the fulfilment of children's rights across the world. Although the European Union itself is not a party to the UNCRC, all Member States (MS) have ratified the Convention.[18] Moreover, over

[12] CNNIC, 'The 47th Statistical Report on China's Internet Development' (2021) <https://www.cnnic.com.cn/IDR/ReportDownloads/202104/P020210420557302172744.pdf> accessed 20 December 2022.

[13] TikTok does not allow users in China to access the app and instead places them in the separate Douyin platform.

[14] Jacqueline M Beutell, 'Children's Rights and Social Media: An Analysis of TikTok's Terms of Service through the Lens of a Young User' <https://www.ideals.illinois.edu/handle/2142/106069> accessed 22 November 2021.

[15] Wallaroo Media, 'TikTok Statistics - Everything You Need to Know' (*Wallaroo Media*, 1 January 2021) <https://wallaroomedia.com/blog/social-media/tiktok-statistics/> accessed 22 November 2021. Research in the UK and Spain for example, has shown the average time children (4-15 years) spend on TikTok per day is up to 95 minutes. 'TikTok Engagement Among Kids Surges During the Pandemic' (*Marketing Charts*, 1 July 2020) <https://www.marketingcharts.com/demographics-and-audiences/teens-and-younger-113749> accessed 23 November 2021.

[16] See 从青少年到老年人都爱，抖音如何坐上娱乐社交时长第一把交椅(How Douyin, loved by everyone from teens to olders, became the number one app of entertainment social hour) <https://www.sohu.com/a/485602905_104421> accessed 21 November 2021.

[17] Government access to such data falls outside of the scope of this article.

[18] Only States can be signatories to the Convention, but the EU as an institution could bind itself through unilateral declaration or the conclusion of an accession Protocol. However, this has not happened yet. Emanuela Canetta and others, 'EU Framework of Law for Children's Rights' (European Parliament) 9 <

the years, the EU has been relying on the guidance of the UNCRC when adopting and interpreting fundamental human rights and other policy instruments.[19] This is demonstrated for instance in Article 24 of the Charter of Fundamental Rights of the EU (CFEU)[20] which contains language that is very similar to that of the UNCRC. The EU's commitment to the UNCRC was again confirmed in the most recent EU Strategy on the Rights of the Child, built on six key pillars of which the digital and information society is one.[21]

China formally ratified the UNCRC in 1991 and protects children's rights through domestic legislation and the ratification of relevant international treaties.[22] China's Constitution states in Article 49 that 'children are protected by the State, and abuse of children is prohibited'. Additionally, China undertook efforts to enact the UNCRC provisions into domestic law. The primary law in this area is the Law on the Protection of Minors. [23] This law sets out the various responsibilities of different actors regarding the protection of children's rights, including families, the government, schools as well as product and service providers. During the latest revision of the law in 2020, a new chapter was included focusing on the protection of minors in the digital environment (*infra*).

The UNCRC is legally binding for all State Parties who have ratified it. This means that they must respect and ensure all rights set forth in the Convention, including the right to privacy laid down in Article 16 UNCRC. Although 'data protection' is not mentioned in the text of the UNCRC, there are references to its link with the right to privacy in a number of UN guidance documents[24] and reports, such as the report of the Special Rapporteur on the Right to Privacy on children's privacy,[25] and, most recently the GC25[26].

---

https://www.europarl.europa.eu/RegData/etudes/note/join/2012/462445/IPOL-LIBE_NT(2012)462445_EN.pdf > accessed 20 December 2022.

[19] European Union Agency for Fundamental Rights, 'Handbook on European Law Relating to the Rights of the Child' (2015) 30 <http://fra.europa.eu/en/publication/2015/handbook-european-law-child-rights> accessed 20 December 2022.

[20] Article 24 CFEU. '*1. Children shall have the right to such protection and care as is necessary for their well-being. They may express their views freely. Such views shall be taken into consideration on matters which concern them in accordance with their age and maturity. 2. In all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration. […].*'

[21] European Commission, 'The EU Strategy on the Rights of the Child and the European Child Guarantee' (2021) <https://ec.europa.eu/info/policies/justice-and-fundamental-rights/rights-child/eu-strategy-rights-child-and-european-child-guarantee_en> accessed 20 December 2022.

[22] 中华人民共和国外交部(Ministry of Foreign Affairs of the People's Republic of China), '中华人民共和国关于《儿童权利公约》执行情况的第三、四次合并报告(The Third and Fourth Combined Report of the People's Republic of China on the Implementation of the Convention on the Rights of the Child)' <https://www.fmprc.gov.cn/web/ziliao_674904/tytj_674911/tyfg_674913/t738182.shtml> accessed 17 June 2022. China's Constitution does not elaborate on points of international law, and in general treaties are of the same rank as laws adopted by the state organ that participates in the process of treaty making. For more information, see Hongwei Zhang, 'Incorporating the CRC in China', *Incorporating the UN Convention on the Rights of the Child into National Law* (Intersentia 2021) <https://intersentia.be/nl/incorporating-the-un-convention-on-the-rights-of-the-child-into-national-law.html> accessed 17 June 2022.

[23] 《中华人民共和国未成年人保护法》(The Law on the Protection of Minors of the People's Republic of China) National People's Congress Standing Committee. The Law on the Protection of Minors was firstly adopted in 1991, revised in 2006, 2012 and 2020.

[24] UN General Assembly (UNGA), Resolution the right to privacy in the digital age (A/RES/73/179), < https://digitallibrary.un.org/record/1661346> accessed 20 December 2022.

[25] United Nations Special Rapporteur on the right to privacy (2021), Artificial intelligence and privacy, and children's privacy, <https://undocs.org/A/HRC/46/37> accessed 20 December 2022.

[26] A general comment is 'a treaty body's interpretation of human rights treaty provisions, thematic issues or its methods of work': See 'OHCHR | Human Rights Treaty Bodies - General Comments' <https://www.ohchr.org/EN/HRBodies/Pages/TBGeneralComments.aspx> accessed 20 December 2022.

B. The General Comment No. 25 on the rights of the child in relation to the digital environment

In relation to the latter document, it is important to note that ratification of the Convention also entails recognition of the key role of the CRC Committee in (1) interpreting the substantive provisions of the UNCRC,[27] and (2) monitoring the proper implementation of corresponding rights and obligations by the State Parties' in their national legal orders.[28] Regarding the first aspect, State Parties are expected to pay close attention to GC25, which although not a legally binding instrument per se, does constitute an important interpretation of their CRC obligations in the digital realm and a source of inspiration towards (greater) compliance. In GC25, State Parties (hence including EU Member States and China) are urged to

> take legislative, administrative and other measures to ensure that children's privacy is respected and protected by all organisations and in all environments that process their data. [… and to] regularly review privacy and data protection legislation and ensure that procedures and practices prevent deliberate infringements or accidental breaches of children's privacy.[29]

Regarding the second aspect, GC25 also shapes State Parties' reporting duties under the UNCRC. The reporting procedure provides State Parties with 'an opportunity to evaluate any progress made, to identify gaps and challenges in respect of relevant human rights obligations, and to develop and adopt the policies and measures needed to enhance compliance'.[30] The CRC Committee acts as both an assessor and a facilitator during this process and can adopt concluding observations at the end, containing positive elements, areas for concern and/or recommendations. Similar to General Comments, such concluding observations are not legally binding, but they do have a special status (i.e. as 'an authoritative pronouncement by the body mandated to monitor State Parties' compliance').[31] As such, in our opinion, this review process could also contribute towards greater awareness of and compliance with obligations concerning children's rights to privacy and data protection in the digital sphere.[32] In addition, monitoring the impact of GC25 on data protection frameworks around the world in the years to come could also offer interesting insights more generally into the effectiveness of soft law instruments like General Comments of treaty bodies.

In line with recommendations issued by other human rights bodies, for instance at the level of the Council of Europe, and the UN Guiding Principles on Business and Human Rights, the GC 25 makes it abundantly clear that also private sector actors, such as platforms providers, must

---

[27] OETTE explains about the UN treaty bodies in general that although they have not been given '*any explicit powers to interpret authoritatively the respective treaties or to reach binding decisions*', in reality they do '*play an important role in interpreting their respective treaties and international human rights law more broadly*' and by exercising their functions in this manner they '*developed legitimacy in so doing'*. Lutz Oette, 'The UN Human Rights Treaty Bodies: Impact and Future' in Gerd Oberleitner (ed), *International Human Rights Institutions, Tribunals, and Courts* (Springer 2018) 100–101.

[28] Article 43(1) UNCRC awards the CRC Committee with a mandate to review '*realisation of the obligations undertaken*' by State Parties.

[29] United Nations Committee on the Rights of the Child (n 6).

[30] Oette (n 28).

[31] ibid.

[32] It is worth nothing that the latest reporting to the CRC Committee by China dates back to 2013 and does not contain an assessment of the rights to privacy and data protection. Considering the substantial changes that have occurred in the interim period of 10 years, it is timely that a new report is drafted containing a detailed assessment, including on the implementation of the PIPL. Committee on the Rights of the Child, Concluding observations on the combined third and fourth periodic reports of China, adopted by the Committee at its sixty-fourth session (16 September–4 October 2013), https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC%2FC%2FCHN%2FCO%2F3-4&Lang=en, accessed 6 June 2023.

fulfil their *responsibilities* to respect children's rights.[33] In the digital environment, this includes *inter alia* that platform providers should refrain from violating children's rights through abusive privacy and data processing practices (article 16 UNCRC), and actively avoid all forms of economic exploitation (article 32 UNCRC), discrimination (article 2 UNCRC) and infringements of all types of freedoms (e.g. articles 10, 11 UNCRC).[34] As primary duty bearers under the UN human rights system, State Parties have a *duty* to ensure that these providers comply with children's rights standards through appropriate legislative, regulatory, and supervisory frameworks.[35] As regards children's rights to privacy and data protection, this includes adopting and enforcing data protection legislation that contains specific protections for children, without arbitrarily restricting limiting other rights, such as children's right to freedom of expression or their right to play;[36] requiring the integration of privacy-by-design into digital products and services that affect children; ensuring that children are awarded data subject rights that can be exercised against platform providers, and more generally, a right to an effective remedy for violations of their rights (including but not limited to) privacy and data protection).[37]

III. The Child's Rights to Privacy and Data Protection in the EU and China

As the UNCRC sets out important obligations for the EU MS and China regarding children's privacy, this section analyses their respective legislative frameworks. The development of European children's rights law has been driven by both the Council of Europe and the European Union, resulting in two frameworks[38] that are influenced by the international children's rights

[33] For example see Council of Europe, Committee of Ministers, 'Recommendation CM/Rec(2016)3 on Human Rights and Business' <http://edoc.coe.int/en/fundamental-freedoms/7302-human-rights-and-business-recommendation-cmrec20163-of-the-committee-of-ministers-to-member-states.html> accessed 28 June 2018; UN Committee on the Rights of the Child, 'General Comment No. 16 (2013) on State Obligations Regarding the Impact of the Business Sector' (2013); United Nations General Assembly, 'Protect, Respect, and Remedy: A Framework for Business and Human Rights Doc A/HRC/8/5' <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G08/128/61/PDF/G0812861.pdf?OpenElement> accessed 6 August 2018.

[34] Pedro Hartung, 'The Children's Rights-by-Design Standard for Data Use by Tech Companies' (UNICEF, Office of Global Insight and Policy 2020) <https://www.unicef.org/globalinsight/media/1286/file/%20UNICEF-Global-Insight-DataGov-data-use-brief-2020.pdf> accessed 7 June 2023. Of course platforms providers also have wider responsibilities for children's rights online, including to protection against harmful content (see for example Lievens E. and Verdoodt V. "The protection of children by videosharing platforms under the Audiovisual Media Services Directive: Codifying platforms' responsibility to respect children's rights", Edgar Elgar, (accepted)) and to health and well-being (see for example Louise Holly, 'PERSPECTIVE Health in the Digital Age: Where Do Children's Rights Fit In?' <https://www.hhrjournal.org/2020/12/perspective-health-in-the-digital-age-where-do-childrens-rights-fit-in/> accessed 5 June 2023.

[35] This is made explicit in various international standards:

[36] United Nations Committee on the Rights of the Child (n 6).

[37] In this regard, the Council of Europe underlines that "*accessible, affordable and child-friendly avenues to submit complaints and seek remedies, both judicial and non-judicial, should be ensured for children and their representatives*". Council of Europe, Committee of Ministers, 'Recommendation CM/Rec(2018)7 of the Committee of Ministers to Member States on Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment'.

[38] Article 52(3) of the CFEU addresses the potential risk of divergences that might develop between these two instruments and mentions the ECHR as a minimum standard: "*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*". This means that the case law of the ECtHR is of great importance for the interpretation of the rights in the Charter as well; Case C-400/10

framework.[39] At the level of the Council of Europe, Article 8 of the European Convention on Human Rights (ECHR) guarantees the right to respect for private life and includes the protection of personal data and Convention 108+ for the Protection of Individuals with regard to Automatic Processing of Personal Data[40] protects individuals – including children – against abuses which may accompany the collection and processing of personal data, introduces basic principles and safeguards and attributes rights to data subjects.[41] At the EU level, the Charter of Fundamental Rights of the European Union includes both the right to privacy and the right to data protection. More specifically, the right to privacy is enshrined in Article 7 CFEU, while the right to data protection is laid down in Article 8(1) CFEU.[42] In addition, the CFEU has a dedicated article on children's rights, the previously mentioned Article 24, outlining *inter alia* that actions taken by public and private institutions that relate to children should take into account the child's best interests as a primary consideration.[43]

The child's rights to privacy and data protection are then further conceptualised in EU secondary law, most notably the General Data Protection Regulation (GDPR),[44] which became applicable in all EU MS in May 2018. The EU data protection framework is a principle-based[45] system, which imposes obligations on data controllers and attributes rights to data subjects. Data controllers are those natural or legal persons, public authorities, agencies or other bodies which determine the purposes and means of the processing of personal data.[46] Private companies that offer services in the context of which they process personal data of children will hence be considered data controllers. With regard to children's personal data the GDPR states that specific protection is warranted, recognising that children are 'less aware of the risk, consequences and safeguards concerned and their rights in relation to the processing of personal data'.[47] Although the GDPR does not include an explicit definition of 'children', the Article 29 Data Protection Working Party (Art29WP) and its successor, the European Data Protection Board (EDPB), have recommended in several of their guidelines that the definition of a child

PPU *McB.*, para 53: '*Article 7 of the Charter must therefore be given the same meaning and scope as Article 8(1) of the ECHR, as interpreted by the case-law of the European Court of Human Rights*.' For more information about the relationship between these two instruments see for example Stephen Brittain, 'The Relationship Between the EU Charter of Fundamental Rights and the European Convention on Human Rights: An Originalist Analysis' (2015) 11 European Constitutional Law Review 482.

[39] E. Canetta and others, 'EU Framework of Law for Children's Rights' (European Parliament) <http://www.europarl.europa.eu/RegData/etudes/note/join/2012/462445/IPOL-LIBE_NT(2012)462445_EN.pdf> accessed 12 July 2018.

[40] Article 15 of the modernised Convention now explicitly requires the authorities to pay 'specific attention […] to the data protection rights of children and other vulnerable individuals' when it comes to raising (public) awareness.

[41] Ingrida Milkaite and Eva Lievens, 'Children's Rights to Privacy and Data Protection Around the World: Challenges in the Digital Realm' (2019) 10 European Journal of Law and Technology <https://ejlt.org/index.php/ejlt/article/view/674> accessed 5 June 2023.

[42] The EU Charter of Fundamental Rights has been given legal binding force by the Treaty of Lisbon and, as such, is incorporated into European constitutional law. David Anderson and Cian Murphy, 'The Charter of Fundamental Rights: History and Prospects in Post-Lisbon Europe' (EUI Working Paper LAW, 2011) <https://cadmus.eui.eu/bitstream/handle/1814/17597/LAW_2011_08.pdf?sequence=1&isAllowed=y> accessed 20 December 2022.

[43] This reflects Article 3 (1) UNCRC.

[44] 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).

[45] See Article 5 GDPR.

[46] Article 4 (7) GDPR.

[47] Recital 38 GDPR.

of the UNCRC should be followed (i.e. anyone under the age of 18).[48] The specific protection for children is referred to in several recitals and provisions of the GDPR, both explicitly and sometimes more implicitly (*infra*).[49]

The Chinese Constitution, encompasses a right to privacy, but only the more limited right to freedom and confidentiality of correspondence[50] and privacy of the home[51]. Until recently, China also did not have a comprehensive data protection framework. However, traces of provisions in relation to data protection could be found in both public and private law – for instance the Cybersecurity Law (CSL)[52] and the Civil Code[53] – which according to De Hert and Papakonstantinou added up to 'a data protection cumulative effect'.[54] This changed on 20 August 2021, when China passed its Personal Information Protection Law (PIPL), which supplements the abovementioned instruments[55] and represents a crucial pillar in China's efforts to regulate the access and use of personal data.[56] The PIPL is the first comprehensive data protection law in China, modelled at least in part on other data protection regimes like the GDPR. Although the PIPL applies to both the private and the public sector,[57] ZHENG highlights that the enhanced protection will mostly be limited to the private sector due to the lack of a general constitutional privacy right, which in reality means that the processing of personal information by the government cannot be effectively restrained.[58] The PIPL both explicitly and implicitly provides special protection for children (*infra*) when their personal data are processed.[59] One important safeguard is the categorisation of personal information of 'minors under the age of 14' as 'sensitive personal information'.[60] This entails that personal information

[48] Article 29 Data Protection Working Group, 'Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools)' (2010). In the guidelines on transparency and the guidelines on consent, the Art29WP recognised this definition again in 2018, see Article 29 Data Protection Working Group, 'Guidelines on Consent under Regulation 2016/679' (2018) <https://ec.europa.eu/newsroom/article29/items/623051> accessed 20 December 2022.

[49] Eva Lievens and Valerie Verdoodt, 'Looking for Needles in a Haystack : Key Issues Affecting Children's Rights in the General Data Protection Regulation' (2018) 34 Computer Law & Security Review 269.

[50] Article 40 Constitution of China.

[51] Article 39 Constitution of China.

[52] 《中华人民共和国网络安全法》(The Chinese Cybersecurity Law), National People's Congress Standing Committee. Article 13 CSL stipulates that the State strives to '*provide a safe and healthy network environment for minors'*.

[53] Article 111 of the Chinese Civil Code: '*the personal information of a natural person shall be protected by the law'*.

[54] Paul De Hert and Vagelis Papakonstantinou, 'The Data Protection Regime in China' (2015) 36 < https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf> accessed 20 December 2022.

[55] Todd Liao and others, 'Personal Information Protection Law: China's GDPR Is Coming' (*Morgan Lewis*, 24 August 2021) <https://www.morganlewis.com/pubs/2021/08/personal-information-protection-law-chinas-gdpr-is-coming> accessed 17 June 2022. As the main law for protecting personal information, the new PIPL will replace articles from former legal instruments which conflict with it.

[56] Guan Zheng, 'Trilemma and Tripartition: The Regulatory Paradigms of Cross-Border Personal Data Transfer in the EU, the U.S. and China' (2021) 43 Computer Law & Security Review.

[57] Article 33 of the PIPL provides that: '*this Law shall apply to the processing of personal information by state organs*'.

[58] More specifically, if administrative agencies which are authorised to process personal data by laws or administrative regulation violate the requirements of PIPL (e.g. purpose limitation), the data subject will not be able to request the unconstitutionality of these acts through judicial review. Zheng (n 60).

[59] UNICEF, 'The Case for Better Governance of Children's Data: A Manifesto' (2021) 44 <https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf> accessed 20 December 2022.

[60] Article 28 PIPL.

handlers[61] may only process such information if there is a specific purpose and a sufficient necessity, and when stringent protective measures are in place. Similar safeguards were already stipulated in the 2019 Provisions on the Cyber Protection of Children's Personal Information (Provisions), but this was only a low-level administrative regulation.[62] Hence, the PIPL significantly strengthens these requirements, lifting them to the highest level of law in China.[63] Moreover, the Law on the Protection of Minors – which as mentioned above was revised in 2020 to include a chapter on the protection of minors in the digital environment – provides that 'minors' lawful rights and interests in cyberspace are protected by law'.[64] The Law defines minors as 'citizens under the age of 18, including foreign national or stateless minors who are not yet 18 years old and are in the Chinese territory'.[65] The chapter on online protections complements the PIPL when it comes to protecting children's rights online, and provides rules regarding parental consent and minors' data protection rights of deletion and rectification. Recently, the Cyberspace Administration of China released the Regulations on the Protection of Minors on the Internet (Draft for Comments), [66] in order to provide more detailed explanations and implementation rules for both the PIPL and the Law on the Protection of Minors. The Regulations deal with minors' data protection rights by indicating a series of detailed obligations for 'online service providers' targeting minors.

In what follows, Section A analyses those provisions that are included in the EU and Chinese legal frameworks that have the potential to provide for specific protection for children's personal data in parallel;[67] while Section B compares these protections and summarises the findings in a comparative table (see Table 1).

A. Specific protection for children's personal data in the EU and China

1. Legal bases for processing children's personal data

First, relevant provisions for children that can be found in both frameworks relate to the principle of lawfulness. This principle entails that data controllers can only process personal data if a legal basis that is included in the data protection framework is applicable.

Article 6 GDPR[68] lists six legal bases.[69] For the processing of children's personal data by businesses, the most relevant bases are (1) contract, (2) consent and (3) legitimate interest of the controller.[70] A first legal basis for processing is when this is necessary for the performance

[61] The PIPL uses the term 'personal information handler', which refers to organisations and individuals that autonomously determine processing purposes and methods in personal information processing activities. See Article 73 PIPL.
[62] 《儿童个人信息网络保护规定》(Provisions on the Cyber Protection of Children's Personal Information), The Cyberspace Administration of China. http://www.gov.cn/gongbao/content/2019/content_5456808.htm, accessed 20 December 2022.
[63] Liao and others (n 59).
[64] Article 64 the Law on Protection of Minors.
[65] Article 2 the Law on Protection of Minors.
[66] 《未成年人网络保护条例（征求意见稿）》（Regulations on the Protection of Minors on the Internet (Draft for Comments)）,the Cyberspace Administration of China. http://www.cac.gov.cn/2022-03/14/c_1648865100662480.htm, accessed 20 December 2022.
[67] Lievens and Verdoodt (n 53).
[68] Article 5 GDPR lists the fundamental data protection principles. These principles include lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation and integrity and confidentiality relating to processing of personal data.
[69] The six bases are: consent, necessity for the performance of a contract, necessity for compliance with a legal obligation to which the controller is subject, necessity of processing in order to protect the vital interests of the data subject or of another natural person, necessity for public interest, and necessity for legitimate interests.
[70] Ingrida Milkaite, 'A Children's Rights Perspective on Privacy and Data Protection in the Digital Age : A Critical and Forward-Looking Analysis of the EU General Data Protection Regulation and Its Implementation

of contractual obligations or preparation for entering into a contract.[71] According to the EDPB, the necessity requirement is strict and data controllers must be able to demonstrate the processing is 'objectively necessary for the performance of the contract'. [72] This legal basis is often used for the data that is processed when setting up an account with a service provider. When the data subject is a child, the data controller must take into account their legal capacity to enter into a contract.[73]

Second, if the data controller opts for consent as the legal basis, this is only valid if it is freely given, specific, informed and unambiguous.[74] In addition to the general requirements, Article 8 GDPR lays down specific rules for certain instances in which consent is chosen as the legal basis for processing children's data.[75] According to Article 8(1) GDPR, in relation to the offer of information society services directly to a child, consent by a child for processing personal data shall only be lawful when he or she is at least 16 years old, otherwise parental consent is needed.[76] However, EU Member States have the opportunity to choose a lower age provided that it is not lower than 13. Article 8(2) GDPR also contains a verification requirement to ensure that the individual giving consent is the holder of parental responsibility.

Third, if data controllers want to rely on their legitimate interest[77] as the legal basis, they will need to identify this interest,[78] and conduct a balancing exercise in which they weigh their own interests against the child's interests.[79] Their own interests cannot override the interests or fundamental rights and freedoms of the child. In making this assessment the best interests of the child can be a guiding principle.[80]

---

with Respect to Children and Youth' (dissertation, Ghent University 2021) <http://hdl.handle.net/1854/LU-8714018> accessed 17 October 2021.

[71] Article 6(1)(b) GDPR.

[72] EDPB, 'Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects' (2019) <https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-22019-processing-personal-data-under-article-61b_en> accessed 21 November 2021.

[73] ICO, 'What Do We Need to Consider When Choosing a Basis for Processing Children's Personal Data?' (20 July 2020) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-do-we-need-to-consider-when-choosing-a-basis-for-processing-children-s-personal-data/> accessed 20 December 2022.

[74] Article 4(11) GDPR: *'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'*.

[75] EDPB, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (4 May 2020).

[76] 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' (Social Science Research Network 2017) SSRN Scholarly Paper ID 3107660 <https://papers.ssrn.com/abstract=3107660> accessed 20 December 2022.

[77] See Article (6)(1)(f) GDPR: '*processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child*'.

[78] Art29WP, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (9 April 2014). The legitimate interests include, for example, exercise of the right to freedom of expression or information, including in the media and the arts, conventional direct marketing and other forms of marketing or advertisement.

[79] ICO, 'What Do We Need to Consider When Choosing a Basis for Processing Children's Personal Data?' (n 77).

[80] Article 29 Data Protection Working Group, 'Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools)' (n 52).

Under Chinese law, the PIPL contains seven legal bases to process individuals' personal information.[81] Unlike the GDPR, the PIPL does not include the legitimate interests of the controller as a basis for processing, but does mention consent and contract as well as specific bases such as public health or news reporting. The PIPL does not offer further information on how to interpret these legal bases when children's personal information is processed, except for consent. If personal information handlers opt for consent, the consent shall be given voluntarily and fully informed.[82] The PIPL sets the age for lawful consent at 14 years, requiring parental consent for anyone below that age.[83] However, the PIPL does not include requirements for verification of parental consent.

Both legislative frameworks have opted for an age threshold for consent by the child to be lawful. This method, however, has been criticised as it may fail to respect the evolving capacities of children[84] on the one hand, and may overestimate parents' ability, skills and understanding in relation to the data-ecosystem, on the other hand.[85] Moreover, the enforcement of the age threshold relies on the (age and parental responsibility) verification mechanisms the apps employ, while evidence has shown in the past that such verification mechanisms are often ineffective or easily circumventable.[86]

2. Transparency and child-friendly information

A second principle that is relevant for children is that of transparency.

Under EU data protection law, transparency of personal data processing is one of the fundamental principles.[87] Article 12 of the GDPR requires data controllers to inform data subjects in a 'in a concise, transparent, intelligible and easily accessible form, using clear and plain language'. When children's data are processed, recital 58 GDPR specifies that the information 'should be in such a clear and plain language that the child can easily understand.' The different items of information that should be provided to the data subjects are listed in Articles 13 and 14 GDPR. Article 13 applies to the situation when personal data are collected from the data subject, while Article 14 lists similar items of information when data are obtained from another source.

---

[81] The seven bases are: (1) consent of the data subject; (2) necessary for the conclusion or performance of a contract; (3) necessary to fulfil statutory duties and legal obligations; (4) necessary to respond to public health emergencies or protect natural persons' life, health, and property safety under emergency circumstances; (5) within a reasonable scope to conduct news reporting, public opinion-based supervision, and other activities in the public interest; (6) in accordance with this law within a reasonable scope to process the personal information disclosed by individuals or other legally disclosed personal information; (7) any other circumstances as prescribed by law or administrative regulation. Article 13 PIPL.

[82] Article 14 PIPL.

[83] Article 31 PIPL.

[84] Milda Macenaite, 'From Universal towards Child-Specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation' (2017) 19 New Media & Society 765.

[85] Simone van der Hof (2017). I Agree. . . or Do I? — A Rights-Based Analysis of the Law on Children's Consent in the Digital World. *Wisconsin International Law Journal*. *34*(2). 101–136.

[86] Jef Ausloos and Valerie Verdoodt, 'Confusing by Design: A Data Protection Law Analysis of TikTok's Privacy Policy – Report' (BEUC 2021) <https://www.beuc.eu/publications/confusing-design-data-protection-law-analysis-tiktok%E2%80%99s-privacy-policy-%E2%80%93-report> accessed 22 November 2021; Liliana Pasquale and others, 'Digital Age of Consent and Age Verification: Can They Protect Children?' [2020] IEEE Software 0.

[87] Article 5 GDPR. See Simone van der Hof, Eva Lievens and Ingrida Milkaite, 'The Protection of Children's Personal Data in a Data-Driven World : A Closer Look at the GDPR from a Children's Rights Perspective', *Monitoring children's rights in the Netherlands : 30 years of the UN convention on the rights of the child* (Leiden University Press 2019) <http://hdl.handle.net/1854/LU-8642862> accessed 21 November 2021.

In China, the new PIPL also features openness and transparency as fundamental principles.[88] The PIPL requires that relevant information relating to the processing of personal information is disclosed, and that the purposes, means and scope of the processing are indicated.[89] Moreover, personal information handlers have to provide this information truthfully, accurately and by using clear and easily understandable language.[90] In contrast to the GDPR, the PIPL does not explicitly mention children in relation to the principle of transparency. Similarly, the Provisions also do not mention that information should be tailored to children, only that network operators should inform the children's guardians in a 'conspicuous and clear manner' (Article 9 of the Provisions). Article 10 of the Provisions lists the categories of information[91] which are to be provided to the guardians of children under 14. For children aged 14 to 18 the general transparency requirements apply.

3. Data subject rights

The EU data protection regime attributes several rights to individuals, namely the right to access,[92] the right to rectification,[93] the right to erasure,[94] the right to restrict processing,[95] the right to data portability,[96] the right to object[97] and rights in relation to automated decision-making and profiling *(infra)*.[98] Children can also claim these rights, which are sometimes especially relevant to them. This is for instance the case with Article 17 GDPR, which affords data subjects the right to 'obtain from the controller erasure of personal data concerning him or her without undue delay' in certain circumstances.[99] The right to erasure is deemed to be especially important for children, as they may not be capable of foreseeing the consequences of sharing their personal information online at a young age, and may later want it removed.[100] In such situations, data controllers should give 'particular weight' to 'requests for erasure if the processing of the data is based upon consent given by a child'.[101] In practice, requests for erasure of data should be as easy as it was to provide the data[102] and data controllers should inform data subjects of their decision or action without undue delay.[103] The right to data portability allows a data subject to transmit their personal data from one controller to another,

[88] Article 7 PIPL.
[89] Article 7 PIPL.
[90] Article 17 PIPL.
[91] The categories of information include: (1) the purpose, methods, and scope of the collection, retention, use, transfer, or disclosure of children's personal information; (2) the location and time period for storage of children's personal information, and the means by which it is processed after the period ends; (3) security safeguard measures for children's personal information; (4) the consequences of refusing; (5) channels and methods for making complaints and reports; (6) channels and means for making corrections or deletions of children's personal information; (7) other matters on which information shall be given.
[92] Article 15 GDPR.
[93] Article 16 GDPR.
[94] Article 17 GDPR.
[95] Article 18 GDPR.
[96] Article 20 GDPR.
[97] Article 21 GDPR.
[98] Article 22 GDPR.
[99] Article 17(1) GDPR. Note that this right is not absolute and needs to be balanced with other (legitimate) interests, such as the right to freedom of expression: Article 17(3) GDPR.
[100] Recital 65 GDPR, See Anna Bunn, 'The Curious Case of the Right to Be Forgotten' (2015) 31 Computer Law & Security Review 336; Eva Lievens and Carl Vander Maelen, 'A Child's Right to Be Forgotten: Letting Go of the Past and Embracing the Future?' [2019] Latin American Law Review <https://revistas.uniandes.edu.co/doi/abs/10.29263/lar02.2019.03> accessed 20 December 2022.
[101] ICO, 'Right to Erasure' (20 July 2020) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/> accessed 20 December 2022.
[102] ibid.
[103] van der Hof, Lievens and Milkaite (n 91).

and the controller must provide the data in a structured, commonly used and machine-readable format when requested.[104] It gives data subjects more control over their personal data, by enabling them to reuse it across different services.[105] From a child's rights perspective, this right could benefit children when they want to switch to more child-friendly online services.[106]

The Chinese legal framework also mentions several data protection rights across the different instruments, namely the right to be informed,[107] the right to restrict or refuse personal information processing,[108] the right to access[109] and the right to portability,[110] the right to rectification,[111] the right to deletion,[112] and the right to request an explanation from the personal information handlers of the privacy policies they develop.[113] Regarding the right to deletion, the PIPL broadens the circumstances in which individuals can exercise the right: including when the purposes have been achieved; the processing is no longer necessary; the personal information handlers cease to provide the product or services; or the individuals withdraw consent.[114] In the context of children's personal data, the Law on the Protection of Minors specifies that data controllers should delete the personal data when the child or their guardians exercise their right, in case of withdrawal of consent and termination of use of the products or services.[115]

4. Rights related to automated decision-making and profiling

Under EU data protection law, data subjects have the right not to be subject to a decision based solely on automated processing, including profiling.[116] According to Article 22 GDPR, an automated decision is prohibited when the decision is *solely* based on automated decision-making and has a legal or similarly significant effect on the data subject.[117] This includes decisions that might negatively affect children's access to healthcare or education, decisions that have discriminatory effect on certain children or denial of citizenship of a country.[118] Exceptions on this prohibition include decisions that are necessary for entering into or the performance of a contract, that are authorised by law and for which explicit consent has been obtained.[119] Recital 71 GDPR mentions that solely automated decision-making with legal or

[104] Article 20 GDPR.
[105] ICO, 'Children and the GDPR' (20 July 2020) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/> accessed 20 December 2022.
[106] Macenaite (n 88).
[107] Article 44 PIPL.
[108] Article 44 PIPL.
[109] Article 45 PIPL.
[110] Article 45 PIPL.
[111] Article 46 PIPL.
[112] Article 47 PIPL.
[113] Article 48 PIPL. According to Article 17 PIPL, personal information handlers shall truthfully, accurately and completely inform individuals for certain categories of information in a conspicuous manner and in clear and easy-to-understand language. The PIPL further specifies that the data subjects have the right to request an interpretation of such information if it is not clear enough. Osborne Clarke, 'The PRC Personal Information Protection Law, China's GDPR – in a Nutshell' (6 September 2021) <https://www.osborneclarke.com/insights/prc-personal-information-protection-law-chinas-gdpr-nutshell> accessed 21 October 2021.
[114] Article 47 PIPL.
[115] Article 72 the Law on Protection of Minors.
[116] Article 22(1) GDPR.
[117] Art29WP, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (Wp251rev.01)' (6 February 2018) <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053> accessed 20 December 2022.
[118] Ibid.
[119] Article 22(2) GDPR.

similarly significant effects should not apply to children. According to the Art29WP, this does not mean automated decision-making is absolutely prohibited when it comes to children, but that controllers should not rely on the forementioned exceptions in Article 22(2) GDPR.[120] One example of where automated decisions would be acceptable is to protect children's welfare (e.g. in the context of healthcare).[121] However, profiling is often considered to have a more significant effect on children, for instance it influences the choices or behaviour of a child.[122] The Special Rapporteur on the Right to Privacy stated in this regard is his report on children's privacy that profiling children 'limits their potential self-development in childhood, adolescence and possibly adulthood, as behavioural predictions and nudging techniques can predetermine options and choices'.[123] Such predictions might be incorrect (e.g. when based on inferred data), and nudging of which children are unaware might lead them to take decisions or make choices that they would otherwise not have taken (e.g. overspending in videogames). These is also recognised by the GDPR, with recital 38 highlighting that the specific protection of children particularly applies to 'the use of personal data of children for the purposes of marketing or creating personality or user profiles'. In that context, the Art29WP has stated that organisations should, in general, refrain from profiling them for marketing purposes, because children 'can be particularly susceptible in the online environment and more easily influenced by behavioural advertising'[124]

Under Chinese law, the new PIPL imposes specific obligations on personal information handlers using personal information for automated decision-making.[125] According to Article 24 PIPL, personal information handlers are required to ensure the transparency, fairness and impartiality of automated decision-making, and not apply unreasonable differential treatment to individuals.[126] When it comes to commercial marketing, the PIPL also grants individuals the right not to be subject to automated decision-making using information about their personal characteristics.[127] The PIPL does not explicitly mention specific protection for children's personal information in this context. However, as mentioned before, personal information of children under 14 is categorised as sensitive data in the PIPL and can only be processed where there is a specific purpose and sufficient necessity, and with strict protection measures in place.[128] Therefore, automated decisions would only be acceptable if they meet this 'sufficient necessity' test. For children older than 14, no specific protections can be found in the Chinese legal framework.

5. Data protection-by-design and by-default

The principles of data protection-by-design and by-default are essential to the EU data protection framework. They are enshrined in Article 25 GDPR, requiring that data controllers implement appropriate technical and organisational measures, *by-design*, to implement data protection principles in an effective manner and to integrate the necessary safeguards into the processing, and by-default, ensuring that only personal data which are necessary for each

[120] Art29WP, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (Wp251rev.01)' (n 121).
[121] ibid.
[122] ibid.; van der Hof, Lievens and Milkaite (n 91).
[123] United Nations Special Rapporteur on the right to privacy (2021). 'Artificial Intelligence and Privacy, and Children's Privacy' <https://undocs.org/A/HRC/46/37> accessed 7 June 2023.
[124] Art29WP, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (Wp251rev.01)' (n 101).
[125] Article 24 PIPL.
[126] Article 24 (1) PIPL.
[127] Article 24 (2) PIPL. Information handlers have to offer individuals an option not targeting the personal characteristics of the individual or an easy way to refuse receiving such business promotion.
[128] Article 28 PIPL.

specific purpose of the processing are processed. Although the GDPR does not directly contain specific requirements of data protection by design and default regarding children, these principles have a lot of potential to ensure the special protection that children merit.[129] Default settings, for instance, regarding personalised advertising, could be a way to provide children with the specific protection required by recital 38.

Up until now, similar data protection-by-design and by-default principles have not been explicitly included in the Chinese data protection framework. Article 9 PIPL does mention that personal information handlers shall 'take necessary measures to ensure security of the personal information they process', but this seems to be limited to technical measures.

6. Data protection impact assessment (DPIA)

The EU data protection framework requires data controllers in certain instances to undertake data protection impact assessments (DPIA). A DPIA is a process *'*designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them*'*.[130] Data controllers must carry out an assessment of the impact of processing operations that are likely to result in a high risk to the rights and freedoms of natural persons.[131] Although the GDPR does not explicitly require a DPIA before any processing of personal data of children, according to the Art29WP, in practice one of the criteria that should be considered when determining whether a DPIA is necessary is when vulnerable data subjects – like children – are involved.[132] Scholars and certain Data Protection Authorities have indicated that conducting a DPIA in each such case would be a good practice.[133] This would entail identifying and remedying risks of a certain processing activity not only for children's rights to privacy and data protection but for the full range of children's rights (including, for instance, non-discrimination). For example, when educational institutions would deploy facial recognition technology to check attendance rates, a DPIA would need to be carried out, in order to assess potential risks in relation to privacy (surveillance), non-discrimination, and freedom of expression and assembly (chilling effect).

---

[129] Council of Europe, 'Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment - Recommendation CM/Rec(2018)7 of the Committee of Ministers' (*COE*, 2018) <https://edoc.coe.int/en/children-and-the-internet/7921-guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-the-digital-environment-recommendation-cmrec20187-of-the-committee-of-ministers.html> accessed 21 November 2021; van der Hof and Lievens (n 60); European Data Protection Board, 'Guidelines 04/2019 on Data Protection by Design and by Default' (20 October 2020), <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf> accessed 20 December 2022.

[130] Art29WP, 'Guidelines on Data Protection Impact Assessment (DPIA) (Wp248rev.01)' (4 April 2017) <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236> accessed 20 December 2022; van der Hof and Lievens (n 53).

[131] Article 35 and recital 91 GDPR.

[132] Art29WP, 'Guidelines on Data Protection Impact Assessment (DPIA) (Wp248rev.01)' (n 134). Other criteria are: evaluation or scoring, automated-decision making with legal or similar significant effect, systematic monitoring, sensitive data, data processed on a large scale, datasets that have been matched or combined, innovative use or applying technological or organisational solutions, data transfer across borders outside the European Union when the processing in itself prevents data subjects from exercising a right or using a service or a contract.

[133] 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), p.33-43; Information Commissioner's Office, 'Age appropriate design: A code of practice for online services' (ICO, 2020) <https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf> accessed 20 December 2022. '*The nature and context of online services within the scope of this code mean they inevitably involve a type of processing likely to result in a high risk to the rights and freedoms of children*'.

The Chinese PIPL also incorporates personal information impact assessments as a data protection tool.[134] More specifically, personal information handlers are obliged to conduct an assessment when processing personal information of children under 14 years .[135] Such an assessment shall focus on '(1) whether the purposes and means of processing personal information are legitimate, justified and necessary, (2) the impact on personal rights and security risks, (3) whether the protection measures are legitimate, effective, and compatible with the level of risk'.[136]

7. Enforcement

Finally, one of the important changes brought by the GDPR in the EU is the strengthened enforcement of the obligations by Data Protection Authorities (DPAs). These DPAs have a long list of tasks and powers, including the possibility to issue quite substantial administrative fines.[137] Data subjects, including children, can also submit complaints to these DPAs in order to enforce their data subject rights. Several data protection authorities in the EU have already launched investigations into platforms such as TikTok on the basis of the GDPR protections for children. In practice, however, the GDPR's one-stop-shop mechanism has led to some obstacles.[138] For example, the Irish Data Protection Commissioner (i.e. the lead supervisory authority) recently submitted its draft decision about TikTok's data protection practices for children to the other concerned supervisory authorities as part of the process under Article 60 GDPR.[139] This could either lead to the confirmation of the draft decision – which would ensure a final decision in a relatively short period of time – or to a dispute resolution procedure under Article 65 GDPR, if the other EU regulators raise any 'relevant and reasoned objections', which could prolong the process by many months.

Unlike the EU, China does not have an independent supervision authority for the enforcement of data protection rules. Instead, enforcement duties are shared by several administrations.[140] The PIPL mentions the relevant departments that are responsible for fulfilling the personal information protection duties, which include the State cybersecurity and informatisation department, relevant State Council departments and county-level and higher People's Governments' relevant departments.[141] The PIPL also provides a long list of the tasks[142] and powers[143] of these departments. Furthermore, the PIPL imposes enhanced penalties, including

[134] Article 55 PIPL.
[135] Article 55 (1) PIPL.
[136] Article 56 PIPL.
[137] Article 58(2)(i) GDPR.
[138] Article 56 GDPR.
[139] See https://www.dataprotection.ie/en/news-media/irish-dpc-submits-article-60-draft-decision-inquiry-tiktok-0.
[140] Article 8 CSL; Article 60 PIPL; See also Lianrui Jia and Lotus Ruan, 'Going Global: Comparing Chinese Mobile Applications' Data and User Privacy Governance at Home and Abroad' [2020] Internet Policy Review <https://policyreview.info/articles/analysis/going-global-comparing-chinese-mobile-applications-data-and-user-privacy> accessed 24 November 2021.
[141] Article 60 PIPL. Including for example, Ministry of Industry and Information Technology (MIIT), Cybersecurity Administration of China (CAC).
[142] The tasks include: (1) organising personal information protection propaganda and education, and guiding and supervising personal information handlers' conduct; (2) accepting and processing personal information protection-related complaints and reports; (3) organising the evaluation of apps' efforts in terms of personal information protection and publish the results of the evaluation; (4) investigating and processing unlawful personal information processing activities; (5) other duties provided in laws or administrative regulations. See Article 61 PIPL.
[143] The powers include: (1) interviewing relevant concerned parties, investigating circumstances related to personal information processing activities; (2) consulting and reproducing a concerned party's contracts, records, receipts as well as other relevant material related to personal information processing activities; (3) conducting

administrative fines of up to 50 million RMB[144] or 5% of the personal information handler's annual turnover.[145] The PIPL also offers the possibility of tort liability,[146] public security administration sanctions,[147] or criminal liability.[148]

B. Comparison of the Legislative Frameworks

Both the EU Member States and China have ratified the UNCRC and as such are legally bound to safeguard children's rights to privacy and data protection. In relation to this, both the EU and China have recognised that children merit special protection regarding the processing of their personal data.[149] However, our analysis has shown that there are important differences between the regulatory frameworks that apply to children's personal data, even if they use the same (or very similar) online services (see Table 1 below). Since the adoption of the PIPL in China, there are more similarities with the EU framework than before. Both the Chinese and the EU frameworks provide various rights for data subjects and contain specific obligations for apps and platforms processing children's personal data. The main differences relate to the lack of an independent supervision authority, and the fact that the specific protections in China are only in place for those children under the age of 14, leaving those between 14 and 18 without specific protection. On the other hand, for the processing of data of children under 14, in China a personal information impact assessment is always obliged, whereas in the EU the obligation to conduct a DPIA when personal data of children is processed is not that clear-cut. Moreover, the fact that personal information of children under the age of 14 is considered to be sensitive data and requires stricter protection measures could at least in theory mean that Chinese children under that age will be better protected under the PIPL.

Table 1: Comparative table of the provisions in the data protection frameworks of the EU and China that are relevant to children

	EU	China
1. Legal bases for processing children's personal data	(1) Consent (child or parental consent, verification requirement); (2) contract (legal capacity of children); (3) legal obligation; (4) vital interests; (5) public interests; (6) legitimate interests (balancing exercise)	(1) Consent (child or parental consent, no verification requirement); (2) contract; (3) statutory duties and legal obligations; (4) public health emergencies or protect natural persons' life, health, and property safety under emergency circumstances; (5) within a reasonable scope to conduct news reporting, public opinion-based supervision, and other activities in

on-site inspections, conducting investigations of suspected unlawful personal information processing activities; (4) inspecting equipment and goods related to personal information processing activities; equipment and goods related to personal information activities where there is evidence to prove they are unlawful may be sealed or confiscated. See Article 62 PIPL.

[144] Approximately equivalent to 6.71 million Euro.

[145] Article 66 PIPL.

[146] Article 69 PIPL.

[147] Article 71 PIPL. According to Article 2 of the Public Security Administration Sanctions Law of the People's Republic of China (2012 Amendment), the public security organ shall impose a public security sanction on those persons who (1) disturb the public order, (2) encroach upon a person's rights or property, or (3) impair the social administration, if the act is harmful to society yet not serious enough for criminal punishment.

[148] Article 71 PIPL.

[149] Recital 38 GDPR (EU); Article 13 CSL and Article 28 PIPL (China; children under 14).

		the public interest; (6) within a reasonable scope to process the personal information disclosed by individuals or other legally disclosed personal information; (7) any other circumstances as prescribed by law or administrative regulation
	Age threshold for consent in the context of information society services: 16 (EU member states have the opportunity to lower this threshold to 15, 14 or 13)	Age threshold for consent: 14
2. Transparency and child-friendly information	Easily accessible and understandable, in such clear and plain language that children understand, applicable to all children under 18	Inform the guardians of children under 14 in a 'conspicuous and clear manner', no specific information requirements for children or guardians of children older than 14, other than the general requirement of providing information truthfully, accurately and by using clear and easily understandable language
3. Data subject rights	The right to access	The right to access and copy
	The right to rectification	The right to rectification or supplement
	The right to erasure	The right to deletion
	The right to restrict or object processing	The right to restrict or object processing
	The right to data portability	The right to portability (request the transfer of personal information to the designated personal information handler)
4. Rights related to automated decision-making and profiling	The right not to be subject to automated decision-making and profiling: solely automated decision-making with legal or similarly significant effects should not apply to children (recital 71); controllers should not rely on the forementioned exceptions in Article 22(2) GDPR	General rules regarding automated decision-making: ensure the transparency, fairness and impartiality of automated decision making, and not apply unreasonable differential treatment to individuals; commercial marketing: right not to be subject to automated decision making using information about their personal characteristics); no specific mention of children (but personal

		information of children under 14 can only be processed where there is a specific purpose and sufficient necessity, and with strict protection measures)
5. Data protection by design and by default	Data protection by design and by default (general, no specific references to children)	Focus only on security (technical measures)
6. Data protection - / personal information impact assessment	Data protection impact assessment (DPIA): personal data of children = criterion (vulnerable group)	Personal information impact assessment: compulsory when processing personal information of children under the age of 14
7. Enforcement	Enforcement by independent Data Protection Authorities a.o. administrative sanctions (e.g. fines)	Several government departments at different levels have enforcement powers Sanctions include administrative sanctions, tort liability, public security administration sanction, criminal liability

IV. CONCLUSION

Our analysis has shown that even though children in different continents have the same rights under the UNCRC and use very similar apps, differences in the regulatory frameworks that are applicable to such apps may still lead to differences in data protection for children in practice. In addition, the analysis also shows that not all elements that the CRC put forward in its GC 25 are already integrated in the legislative frameworks. That is especially the case in China. The analysis also emphasises that although certain protections for children are included in both frameworks, in the end this will mean little if they are not effectively enforced. For instance, despite age-based requirements in both frameworks, there are still no examples of digital platforms or apps that have implemented an effective age verification mechanism. Moreover, in the EU obstacles remain due to the one-stop-shop mechanism.[150] In China, there is not a single independent data protection authority similar to EU MS, and hence, it will be interesting to see in the next few years whether and how the various government authorities will take action under the new PIPL.

It is clear that both Chinese and EU policy-makers and legislators are paying more attention to the rights of children in the digital environment. In the EU, in addition to the General Data Protection Regulation, the revised Audiovisual Media Services Directive, the recently adopted Digital Services Act and the Proposal for an Artificial Intelligence Act all require private companies to take measures balancing children's fundamental rights and interests against their own freedom to conduct business (Article 16 CFREU) and commercial interests.[151] Moreover,

[150] Article 56 GDPR.

[151] See Article 28b (3): "*the appropriate measures shall be determined in light of the nature of the content in question, the harm it may cause, the characteristics of the category of persons to be protected as well as the rights and legitimate interests at stake, including those of the video-sharing platform providers and the users having created or uploaded the content as well as the general public interest*".

as part of the Better Internet for Kids + Strategy, an EU code of conduct on age-appropriate design will be developed by 2024.[152] In China, the Law on the Protection of Minors specifies that platforms such as for online games, broadcasts, audio or video works and social media shall set up "appropriate functions for managing usage time, privileges, and spending for minors using their services". [153] The Regulations on the Protection of Minors on the Internet (Draft for Comments) further provide more specific obligations towards platforms "with a large number of minor users and significant influence in the group of minors".[154] The Regulations also set rules to avoid economic exploitation, by limiting the amount of single consumption and cumulative single-day consumption of minors in the use of network products and services.[155] The State Administration of Market Regulation of China also released the Guidelines of Implementing Internet Platforms Responsibilities (Draft for Comments), which require online platforms to provide contents that "appropriate to the physical and mental health and personality development".[156]

This legislative shift in both regions towards more obligations for tech businesses is in line with the CRC Committee's General Comment No. 25. Perhaps even more important, it also reflects calls from children themselves who believe that providers of digital platforms should take up more responsibility in providing safe spaces for children and protecting their rights to privacy and personal data. [157] In this regard it is essential to involve children in the design of such platforms by listening to their opinions and user experiences. [158] This is not only required to

[152] 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+) 2022. Such an Age-Appropriate Design Code already exists in the United Kingdom, see < https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/>.

[153] Article 74 the Law on the Protection of Minors.

[154] Article 20 the Regulations on the Protection of Minors on the Internet (Draft for Comments), the obligations include "(1) In the design of Internet platform services, research and development, operation and other stages, taking fully into account the physical and mental health development characteristics of minors, regular impact assessment of the protection of minors network. (2) Provide youth mode or special area for minors, etc., to facilitate minors' access to products or services within the platform that are beneficial to their physical and mental health. (3) Establishing a sound compliance system for the online protection of minors in accordance with national regulations, and setting up an independent body composed mainly of external members to supervise the online protection of minors (4) Follow the principles of openness, fairness and impartiality, formulate special platform rules, clarify the obligations of in-platform product or service providers for the online protection of minors, and prominently indicate the online protection rights of minor users in accordance with the law and the remedies for online infringement. (5) Stop providing services to products or service providers within the platform that seriously violate laws and administrative regulations infringing on the physical and mental health of minors or violating other legitimate rights and interests of minors. (6) The annual release of a special report on the social responsibility of minors network protection, and through public comments and other means to accept social supervision."

[155] Article 51 the Regulations on the Protection of Minors on the Internet (Draft for Comments).

[156] Article 31 of the Guidelines of Implementing Internet Platforms Responsibilities (Draft for Comments)(《互联网平台落实主体责任指南》) https://www.samr.gov.cn/hd/zjdc/202110/t20211027_336137.html, accessed 20 December 2022.

[157] European Schoolnet, 'How to Make Europe's Digital Decade Fit for Children and Young People?' (2021) <https://www.betterinternetforkids.eu/documents/167024/6847388/How+to+make+Europe%E2%80%99s+Digital+Decade+fit+for+children+and+young+people+-+A+report+from+the+consultation+with+children+and+young+people+-+October+2021.pdf/ae344db2-5b56-0f67-625e-a66244aa023c?t=1633359093370> accessed 20 December 2022.; Sonia Livingstone, Mariya Stoilova and Rishita Nandagiri, 'Children's Data and Privacy Online: Growing up in a Digital Age' (*London School of Economics and Political Science*, December 2018) <https://www.lse.ac.uk/media-and-communications/research/research-projects/childprivacyonline.aspx> accessed 20 December 2022

[158] Eva Lievens and others, 'Children's Rights and Digital Technologies', *International human rights of children* (Springer 2018) <http://hdl.handle.net/1854/LU-8561031> accessed 20 December 2022.

realise children's right to be heard,[159] but might also provide valuable input to formulate relevant features and actual child-friendly privacy policies, for apps that are used by children across the world.[160]

Finally, an interesting avenue that deserves further scrutiny is how the existing UN human rights system can be used to help states hold platform providers accountable for children's rights in the design and deployment of their platforms and services offered to children. To help states ensure that global tech companies fulfil their child rights responsibilities, the UNICEF think tank has recently proposed extending the UN's existing international institutional mechanisms to these companies.[161] In practice, this would mean that platform providers would also be subject to the same monitoring and reporting procedures as State Parties, and receive direct communications from the Committee to contribute voluntarily to States' reports, on topics that relate to their platforms and services. Companies could thus also be subject to complaints and enquiry procedures and comments or recommendations from the Committee. If State Parties can motivate companies to do so, this could be a way to fulfil their duty under the UNCRC. In this context, further research is needed into the type of incentives State Parties could resort to (e.g. include reporting requirements in legislation or encourage self-regulatory reporting mechanisms), jurisdictional questions and how this reporting should work in practice.

[159] Article 12 UNCRC.
[160] Ingrida Milkaite and Eva Lievens, 'Child-Friendly Transparency of Data Processing in the EU: From Legal Requirements to Platform Policies' (2020) 14 Journal of Children and Media 5.
[161] Hartung (n 36).