TDH NL Feedback on the Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR

Terre des Hommes Netherlands (TdH NL) welcomes the European Data Protection Board's initiative to clarify the interpretation of Article 6(1)(f) of the GDPR[1], particularly regarding children's data protection. Children are especially vulnerable online and thus require a robust legal framework that promotes their rights and safety. Specifically, it is essential to create a legal basis that enables platforms to process data to combat criminal activities involving children. Until such a legal basis is established, the interpretation of the notion of legitimate interest under Article 6(1)(f) of the GDPR is essential to bridge the current gap in protection and fulfil the pressing need for children's safety online.

While the guidelines lay important groundwork, we notice and are concerned that the current interpretation contradicts existing jurisprudence and still leaves a gap that allows potential crimes against children to go unaddressed. Specifically we note and recommend :

1. The necessity of a legal basis for data processing is inconsistent with existing jurisprudence and weakens children's protection

We welcome that the guidelines link the notion of legitimate interest to the principle of best interest of the child[2]. This approach aligns with article 24(2) of the EU Charter establishing that **the child's best interests must be a primary consideration**, in all actions relating to children. The guidelines emphasise the need to carefully process children's data. However, the interpretation could further protect children by fighting major violation to their right to privacy such as disclosure of personal information and material (i.e., sexual abuse photos or videos and non-consensual sharing of intimate content).This approach is the one taken by both the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR).

The EDPB guidelines' emphasis on a specific legal basis for data processing in the context of crime prevention does not align with existing EU jurisprudence and undermines the protection of children online. The guidelines' current stance on the need for a specific legal basis contradicts established jurisprudence, which supports a broader, rights-based approach to data processing. The EU Charter, supported by case law from both the CJEU and the ECtHR, provides an interpretative framework emphasising fundamental rights and the protection of vulnerable individuals such as children.

---

[1] EDPB, Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, 8 October 2024,https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf

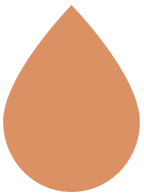
[2] EDPB, Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, 8 October 2024, §95,https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf

The CJEU has acknowledged that online child sexual exploitation involves severe breaches of children's fundamental rights, particularly the right to protection of private and family life, individual physical and mental integrity, and the prohibition of torture and inhuman or degrading treatment[3]. The Court observes that for online crimes, collecting data like IP addresses may be essential for identifying the perpetrators[4]. Thus, it recognised that the retention of data for the purpose of their possible transmission to the competent national authorities satisfies an objective of general interest, namely the fight against serious crime and, ultimately, public security[5] . This approach is consistent with ECtHR case law. The latter found that the searching of a personal computer by the police after a technician had found CSAM on it and informed the authorities pursued the legitimate aim of 'crime prevention'. The Court emphasised the importance of State protection for children victim of online sexual exploitation[6]. By limiting legitimate interest to contexts of direct legal obligation, the guidelines constrain data processing that would otherwise enhance children's online safety. This approach does not acknowledge the risks faced by children as vulnerable users and inadvertently reduces protective measures available to them. Harmonising the interpretation of GDPR's provisions with the EU Charter's principles and ECtHR rulings would provide a more consistent and effective approach to children's online protection under article 6(1)(f) of the GDPR.

2. Expanding the interpretation of legitimate interest to support platforms' role in protecting children and preventing crime

The interpretation of article 6(1)(f) provides that a specific legal obligation connecting authorities with platforms is necessary for crime prevention activities to be justified as a legitimate interest. This narrow scope creates a gap that **jeopardises children's safety** by limiting platforms' abilities to process data to detect and prevent abuse. Indeed, even though the derogations to the ePrivacy Directive allow platforms to detect, report, and remove content related to OCSE[7], a broader interpretation of article 6(1)(f) of the GDPR could enable more sustainable and proactive measures in the fight against OCSE. The current legal framework should be amended to allow voluntary detection on a permanent basis. Indeed, law enforcement heavily rely on voluntary detection by platforms and, to avoid any protection gaps, it is crucial this

[3] CJEU, Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v Premier Ministre and Others, 6 October 2020, pt. 126.
[4] CJEU, Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v Premier Ministre and Others, 6 October 2020, pt.154.
[5] CJEU, joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, 8th April 2014, pt. 44.
[6] ECtHR, Trabajo Rueda v Spain, 30 May 2017.
[7] European Union, Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse, 14 July 2021.



possibility is maintained as one of the key tools to fight online child sexual abuse. It is estimated that information provided by detection and reports on social media platforms lead to 1,200 children safeguarded and 800 offenders arrested every month in the UK alone[8]. Voluntary detection has been the main driver of the high volume of reported CSAM to NCMEC, reaching 105.6 millions in 2023[9]. Voluntary detection must be part of any long-term solution to tackle this crisis. As technology evolves companies need to be able to react and innovate quickly. Without voluntary detection, there will be significant protection gaps for offenders to exploit.

In addition, the derogations to the ePrivacy Directive provide specific rules for electronic communications. However, article 6(1)(f) of the GDPR remains relevant for processing outside this specific scope or where platforms seek to act proactively beyond mere compliance with the derogations. Thus, it is relevant to keep in mind that while the temporary derogations under the ePrivacy Directive have provided an essential stopgap measure, allowing platforms to detect and report OCSE, these derogations alone are insufficient for a sustainable approach to child protection. Interpreting article 6(1)(f) of the GDPR to explicitly recognize that the protection of children from online crimes could constitute a legitimate interest would complement the derogations, address gaps in prevention, and provide a long-term solution.

The counterpoint to this view is that the court and guidelines maintain that platforms, by nature of their commercial purpose, lack a clear basis to justify a legitimate interest to collect and share data specifically to combat crimes, as this function falls outside their primary business objective[10]. However, this perspective does not fully acknowledge the role these **platforms already play beyond mere commerce,** particularly in safeguarding their users, including children, against significant harm. While it is true that platforms are commercially driven, they also serve as primary environments where children interact, learn, and play. Given this central role, it is crucial to recognize that **platforms are in a unique position** to contribute meaningfully to crime prevention, especially for vulnerable users like children.

Finally, in this context, the interests of third parties—specifically, legal authorities' interests in combating crimes—become directly relevant. The GDPR's framework itself indicates that legitimate interest can be expanded to include third-party interests, especially when these align with broader societal values like safety and justice. Protecting children's rights to safety and privacy is a legitimate third-party interest, which fits squarely within the framework of Article 6(1)(f). It is impractical and harmful to ignore third-party interests of this magnitude. Children's protection is too critical an interest to defer until legislation formalises a permanent obligation.

---

[8] UK Home Office, 2023. Key Facts and stats.
[9] NCMEC, CyberTipline 2023. Reports by Electronic Service Providers.
[10] CJEU, judgement of 4 July 2023, Case C-252/21, Meta v. Bundeskartellamt (ECLI:EU:C:2023:537), para. 124.

While the derogations to the ePrivacy directive enable urgent action, a broader interpretation of legitimate interest under the GDPR provides a framework for sustainable and proactive measures beyond the scope of temporary exceptions. Additionally, the GDPR's legitimate interest framework provides many safeguards including proportionality and necessity tests, that ensure that any data processing under Article 6(1)(f) is lawful, targeted, and balanced against privacy rights. This approach would help bridge the gap, providing immediate protections without over relying on temporary measures and, while still respecting the GDPR's intent and the principles underpinning it.

3. The need for preventative measures to support children's fundamental rights online

Although the guidelines on Article 6(1)(f) rightly emphasise protecting children from excessive data collection, they overlook the need for **preventative measures** that promote children's safety online. While the current framework, which includes the temporary derogations to the ePrivacy Directive, provides a crucial legal basis for specific actions, it leaves critical gaps in addressing the **prevention** of OCSE. Platforms need the flexibility to develop and deploy tools aimed at preventing OCSE across their services. Recognizing the necessity of data collection for preventive purposes, such as age verification, is crucial to create **age-appropriate online spaces for children.** Without these measures, children's right to online safety is inadequately supported. While shielding children from excessive data collection is essential, they are not merely users in need of protection from data misuse—they are vulnerable individuals who also require proactive protections enabled by limited, targeted data processing. **Children's rights to privacy and online safety are interdependent.** A more comprehensive interpretation of Article 6(1)(f) that allows limited, purposeful data collection in line with preventive protections would be better suited to supporting children's rights holistically and addressing the reality of risks they face online.

In conclusion, while we appreciate the protective intent behind these guidelines, the current interpretation of Article 6(1)(f) does not adequately address the specific vulnerabilities children face online. We urge a more comprehensive approach that incorporates voluntary detection as a legitimate interest, aligns GDPR interpretation with the EU Charter and existing jurisprudence, and regards preventative data collection as a necessary part of upholding children's fundamental rights.

TdH NL works and advocates for the prevention of all forms of online violence against children,particularly situations where children are at risk of exploitation and abuse.