Guidelines 3/2025 on the interplay between the DSA and the GDPR

Comment of Martin Husovec and Daphne Keller

We write as academics specialized in platform regulation to call attention to two specific concerns with the Board's generally well-considered and balanced Draft Guidelines on the interplay between the DSA and the GDPR.

The Draft Guidelines include a nuanced and useful discussion about platforms' efforts to automatically detect and address illegal content – either voluntarily under DSA Article 7 or potentially as the result of legal mandates. As noted in Draft Guidelines Paragraph 14, such monitoring may involve the processing of personal data and must be compliant with the GDPR. The Board's focus on this issue is a welcome development. While the threat to Internet users' data protection rights from general monitoring obligations has been mentioned repeatedly by the CJEU,[1] recent cases have largely bypassed this concern and focused instead on freedom of expression and information.[2]

Data protection concerns may arise from platforms' monitoring efforts in at least two ways. First, data protection rights are at issue when a proposed mechanism for detecting unlawful content requires searching for and perhaps reviewing personal information. This issue is particularly acute if, for example, monitoring may depend on biometric scanning of users' uploaded images (as was potentially at issue in the CJEU's *Glawischnig-Piesczek* case).[3] Second, as Paragraph 15 discusses, inevitable errors

---

[1] Case C-360/10, *SABAM v. Netlog NV*, (2012) Para. 51; Case C-70/10, *Scarlet Extended SA v. SABAM*, (2011), Para. 53, see also Case C-293/12 and C-594-12 *Digital Rights Ireland Ltd. v Ireland*, (2014), (rejecting data retention law that required electronic communications service providers to retain data about communications made by all of their subscribers).

[2] Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* (2019) ("*Glawischnig-Piesczek*"); Case C-401/19 *Poland v. European Parliament and Council* (2022). For discussion of litigation parties' lack of incentive to raise arguments based on users' data protection rights, see Daphne Keller, *Facebook Filters, Fundamental Rights, and the CJEU's* Glawischnig-Piesczek *Ruling*, GRUR International, 69(6) (2020), p. 623.

[3] *Glawischnig-Piesczek*. Austrian courts in that case had considered an injunction compelling Facebook to detect and remove all uploaded photographs depicting the applicant with particular accompanying text. Glawischnig-Piesczek, Opinion of AG Szpunar, Para. 56. For more on the prohibition of general

from imprecise automation have a range of damaging effects on user rights including data protection and freedom of expression. Concern over such harms from general monitoring was sufficiently acute to draw interventions from UN human rights officials,[4] as well as European and global civil society groups,[5] when EU lawmakers last considered adopting such a mandate.

Given the serious fundamental rights at issue, and the relative shortage of case law and other materials closely examining the data protection concerns with general monitoring, we believe it is important for the Board to avoid stating or implying any final legal conclusions on these issues. In light of this, two small revisions to the Draft Guidelines are appropriate.

First, Paragraph 18 states, "It is clear that the interest of detecting and addressing illegal content in intermediary services to protect the recipients of the service is legitimate, in particular where such content can be disseminated to the public via an online platform." This passage might be taken to endorse a legitimate interests basis for scanning private messages under the GDPR. To avoid that implication, we recommend omitting two words from the sentence: "It is clear that the interest of detecting and addressing illegal content in intermediary services to protect the recipients of the service is legitimate~~, in particular~~ where such content can be disseminated to the public via an online platform."

The second concern is slightly more complex. Paragraph 20 refers to situations in which a "provider could be obliged to process personal data pursuant to a requirement stemming from EU law". In the context of prior paragraphs, and in particular the Draft Guidelines' immediately preceding discussion of "[i]dentifying and taking down copyright-protected works" under the Copyright Directive, this could be read as referring to situations in which a general monitoring obligation may lawfully be imposed. It might further be interpreted to say that such a situation – and such a consequential mandate – arises when a data subject "exercises their right to erasure under Article 17 GDPR".

---

monitoring as a tool to protect privacy and data protection, see Martin Husovec, *Principles of the Digital Services Act* (OUP, 2024), p. 66 ff.

[4] Letter of David Kaye, Joseph Cannataci and Fionnuala Ní Aoláin, 'Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the right to privacy and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism' (7 December 2018); see also Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, '2018 thematic report to the Human Rights Council on content regulation' (United Nations Human Rights Office of the High Commissioner, 2018).

[5] Letter of Access Now and others, 'To Members of European Parliament' (4 February 2019); Letter of Article 19 and others, 'Joint letter on European Commission regulation on online terrorist content' (6 December 2018); Letter of WITNESS and others, 'To the Committee on Civil Liberties, Justice and Home Affairs' (28 January 2019).

Here again, stating or implying such a conclusion would have major implications, not only for the fundamental rights issues discussed above but for the overall legislative relationship between the GDPR and DSA.[6] Such a conclusion might depart from the principle, well-articulated in the Draft Guidelines at Paragraph 9, that EU legal acts of the same hierarchical value "should be applied in a compatible manner, which enables a coherent application of them". Such a conclusion would also relate closely to the questions currently before the CJEU in the *Russmedia* case.[7] To avoid these difficulties, we would recommend the following revision: "To comply with its obligation under Article 17 GDPR, the intermediary service provider may need to ~~detect~~ **review** the allegedly illegal content and, after carefully considering whether an exception under Article 17(3) GDPR applies, decide whether the personal data should be erased or not."

We thank the Board for the opportunity to share comments on the Draft Guidelines.

Regards,

Martin Husovec

Daphne Keller

[6] As one of us has noted, applying GDPR rules including Articles 12, 14, 15, 17, 18, and 19 too stringently in the platform notice and takedown context could have consequences for affected users that EU legislators almost certainly did not intend. Daphne Keller, *The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation*, Berkeley Technology Law Journal 33 (1), (2018) pp. 327-341. EU lawmakers subsequently established detailed rules for platforms' content moderation processes under the DSA, which are far more fit for purpose and protective of users' rights. In this area, as in questions about general monitoring, it seems reasonable to assume that legislators did not intend to exclude GDPR Article 17 or Article 21 requests from the protections of the DSA.

[7] Case C-492/23, *Russmedia Digital and Inform Media Pres*s.