Schibsted

March 2022

Schibsted comments on EP proposals in the Digital Services Act (DSA)
'Compliance by design', consent and GDPR

Schibsted is a family of digital consumer brands based in the Nordics with world-class Scandinavian media houses, leading classifieds marketplaces and tech start-ups in the field of personal finance and collaborative economies. We welcome the proposal for a Digital Services Act (DSA) and the overall objective of clarifying and strengthening the online liability framework.

Schibsted fully understands the concerns of decision-makers about intrusive targeted online advertising and the collection of users' online data. At the same time, the legitimate use of data is key to develop new digital products and services for the benefit of users. It is therefore vital that any proposals are clearly defined, consistent with the existing legal framework, and proportionate for businesses operating online.

In this paper, we share for your consideration and information in the trilogue negotiations our remarks on:

- Ensuring consistency with the EU's existing legal framework in addressing 'compliance by design' and manipulative design practices and interfaces (Art. 13a, Parliament; Art. 24b, Council).
- Protection of minors online (Art. 13a.3, Parliament).
- Ensuring that the rules on targeted online advertising are proportionate and do not amount to a general prohibition (Art. 24.1a (new), Parliament).
- Ensuring clarity in the interaction between the DSA and the General Data Protection Regulation (GDPR).

The proposals of the European Parliament and Council are well intentioned to mitigate legitimate concerns over certain misleading online business practices. At the same time, decision-makers should strike the appropriate balance between user protection and disproportionate obligations for intermediary services. Overly burdensome consent mechanisms, such as repeated pop-ups, do not bring benefits to the products and services offered, but rather risk generating friction in the user experience, creating user fatigue, and worsening overall service delivery.

1. 'Compliance by design' / Online interface design and organisation (Art. 13a, Parliament; Art. 24b, Council)

These amendments, as drafted, would likely add unnecessary complexity to the existing regulatory framework. The GDPR already sets out requirements for intermediary services to collect legally valid consents, backed by guidance from the European Data Protection Board (EDPB)[1]. User consent must be "freely given, specific, informed and unambiguous indication

[1] EDPB, Guidelines on Consent under Regulation 2016/679

of the data subject's wishes" (GDPR Art. 4(11)) and be "as easy to withdraw as to give" (GDPR Art. 7(3)). Provided they are well enforced by supervisory authorities, national courts and ultimately the European Court of Justice, these requirements are already sufficiently flexible to identify invalid consent mechanisms or processes that cannot be said to provide a free choice for users. The proposed ePrivacy Regulation, currently under legislative scrutiny by the Parliament and Council, also contains additional provisions.

The Parliament's proposals in Art. 13a go beyond the provisions in the GDPR and contradict existing guidance from the EDPB and national data protection authorities. Adding further provisions, not aligned with GDPR, are likely to result in regulatory fragmentation and regulatory distorsions among digital actors. For instance:

- It is highly unclear in the Parliament's Art. 13a.1(c) text what would constitute "urging" a recipient of the service to change a setting or configuration of the service. There are many scenarios where it would be reasonable for an intermediary service to prompt a user to make new decisions on consent options, for instance if the user tries to access a feature or service that would not otherwise function effectively. Furthermore, it is our view that the GDPR already addresses the central objective of Art. 13a.1(c).
- The Parliament's proposal in Art. 13a.1(e), requiring services to refrain from requesting user consent if a user has already objected "by automated means using technical specifications", seems contrary to the interests and autonomy of the user. In practice, this provision would make it impossible for intermediary services to highlight their value proposition to users, and make it impossible for the user to exercise choice in diverging from their automatic settings to benefit from a feature or service those settings would normally disallow. Such a provision risks denying users the benefits of personalised online services.
- The Council's text in Art. 24b proposes a specific regime for online marketplaces that would prevent online interfaces that "purposefully or in effect deceives or manipulate recipients of the service" (Art. 24b.1). As drafted, this is overly general and, if broadly interpreted, would likely be disproportionate to the known risks. In addition, the European Commission already has authority to enforce against manipulative design practices, both in the Unfair Commercial Practices Directive (UCPD) and the GDPR. The inclusion of new provisions in the DSA targeting only providers of online marketplaces would therefore add complexity to the legislative landscape.

Any new requirements must be achievable and proportionate to known and identified risks. Legislative proposals to address 'compliance by design' concerns should be horizontally applied to the whole online ecosystem, either through a revision of the UCPD or the GDPR, and accompanied with a full evaluation and impact assessment to consider and understand the possible harms.

We therefore recommend <u>not</u> to include the provisions in Art 13(a) (Parliament) or Art. 24(b) (Council) in the DSA text.

2. Protection of minors (Art. 13a.3, Parliament)

Schibsted agrees it is important to take particular care in protecting children in the online context. At the same time, any provisions in the DSA should be consistent with the GDPR, including Art. 8 ("Conditions applicable to child's consent in relation to information society services") and Art. 12(1). As currently drafted, the Parliament's provisions in Art. 13a.3 are unclear and difficult to understand if they intend to set out new or different requirements to those already in the GDPR. Such repetition could create a lack of clarity over the implementation of the DSA and its interaction with the GDPR.

3. Consistency between the DSA and GDPR (Art. 24.1a (new), Parliament)

The Parliament's proposals in Art. 24.1a (new) are ambiguous and not coherent with the application of the GDPR. The adopted text transforms the established concept of easily "withdrawing" consent, as defined in Art. 7 of the GDPR, into easily "refusing" consent. The Parliament has also introduced a further requirement that users refusing or withdrawing consent should be given "other fair and reasonable options to access the online platform". This would undermine the existing GDPR legal framework and produce wide-ranging consequences for the viability of online platforms that rely on advertising revenues to fund products and services for users. In practice, it may constitute a prohibition on "cookie walls" (making access to a site conditional upon accepting the use of cookies and other identifiers). This is particularly problematic for the services of online platforms that are wholly or partly financed by online advertising, which would likely be required to shift to an unproven and possibly unviable user payment model.

Regulating "consent" in the DSA also risks double regulatory scrutiny and enforcement challenges at a national level. The GDPR is enforced by national data protection authorities whereas the DSA could be enforced by a different national authority, the Digital Services Coordinator (DSC). This would inevitably lead to legal uncertainty over which authority is responsible for enforcing rules around consent for the use of personal data.

We therefore recommend <u>not</u> to include the proposals in Art. 24.1a (new) (Parliament) in the DSA text.

Principles established in the GDPR should remain the benchmark for the use of personal data by online intermediary services. This will preserve the coherent, effective implementation of existing rules, including through European and national guidance. Any modifications to EU data protection legislation should be accompanied by a detailed analysis of possible legislative gaps and expected consequences of new legislation.