User notification and redress: 'Restrictions of visibility'	*Art. 15, 17, 18; Rec. 42, 44*

- The Council and Parliament texts propose expanding user notification and redress requirements beyond restrictions of availability (including, content removals, disabling of access to content, "shadow-banning", etc.) to also cover 'any restrictions of the visibility' of content. While well-intentioned, this may inadvertently result in user notification and redress obligations for organic ranking and recommendations of content, too.
- This would be a bad outcome for users and unworkable for services. The basic operation of many modern online services involves constant updating of content optimized for users. This provision could lead to users being bombarded with an untold number of notifications each day and to service providers being unable to effectively organize and present content on their services. It could also limit platforms' ability to reduce the spread of harmful content, such as disinformation, on their services.
- **The final text should more precisely and proportionately define what restrictions may trigger user notification and redress, by referring to restrictions of the 'availability' of content and removing references to 'visibility', 'ranking' and 'demotions'.**

User redress: User notifications	*Arts. 17, 18; Rec. 44*

- The Council text proposes expanding appeals and out-of-court redress from content uploaders to all persons notifying platforms of content that is allegedly illegal or policy-violating, where the platforms decided not to take action on said content. The reality is that, of the large volume of user notifications (for violations of T&C in particular) received by platforms each day, many are inaccurate and simply add 'noise' to (rather than positively contribute to) content moderation systems. Recital 44 of the Council text does not require notifiers of content to provide detailed information to substantiate the claim, and even requires platforms not to request detailed explanations from users in that regard.
- **Policymakers should forgo the expansion of redress to user notifications.** Information about user notifications would still be retained as part of transparency reporting under the DSA, in line with the principle of proportionality.

User redress: Out-of-court redress	*Art. 18, Rec. 44*

- The out-of-court redress provision proposed by the Commission is the most expansive and unbounded proposal of its kind in Europe. The Council moves in the right direction, by adding safeguards that would ensure online platforms are not subject to multiple proceedings over the same dispute, and would deter bad actors by allowing reimbursement of fees from users who acted in manifestly bad faith.
- **We however consider that more robust safeguards should be added, including to** (a) require users whose content was removed or demonetized to first go through the internal appeals process provided for under Art. 17; (b) set time limits for initiating Art. 18 proceedings; (c) allow platforms to avail themselves of judicial recourse; and (d) provide carve-outs for spam content and repeat offenders.

Trader identification and "know your business customer's *products*"	*Art. 22 (new Art. 24a in the Council text), Rec. 49, 50* *New Article 13a, Rec. 39a in the Parliament text*

- The Parliament would require *all* intermediary service providers (not just online marketplaces) to carry out checks of business users, prior to their use of the service. The Parliament would also require *online marketplaces* to move from 'know your business customer' to 'know your business customer's *products*,' and even require them to make 'best efforts' to identify and prevent the dissemination of illegal products and services, e.g., through spot checks.
- These not only amount to impermissible general monitoring obligations, they would also require the impossible of services, e.g,. search services that do not have a direct relationship with business users that are listed in search results, and online marketplaces that facilitate sales of goods by traders, but do not have the goods in their physical control. **We support the Commission and Council texts**, which provide for robust but proportionate trader identification requirements.

Online marketplaces: Definitions	*Art. 2(ia)*

- **The three institutions could add legal certainty for services** by specifying that the definition of an online marketplace is one where the contract between the trader and the consumer is concluded *on the online platform.* The current wording is ambiguous, inconsistent with existing EU legislation, and risks pulling

products that redirect consumers to third-party traders' websites (such as ads) in the scope of the obligations intended for online marketplaces.

Online Advertising	*Art. 24, Rec. 52;* *New Art. 24(1) and Rec. 52(a) in the Parliament text*

- **We understand that the Parliament text proposes a ban on the collection of personal data for the purposes of delivering behaviorally-targeted advertising to minors, and a ban on the targeting of advertising based on sensitive user data**.
- To the extent the Council agrees with the above, we would caution that the text should reflect the challenges presented by age verification, and attempts to ascertain the age of all users. Any obligations should only apply to 'known minors' in order to be proportionate and not lead to more user-data collection.
- When it comes to matters of user consent, the DSA should provide for clear language consistent with GDPR to ensure legal certainty, a realistic burden of proof, taking into account the need for data minimization and the current state of the art. GDPR definitions should also apply when it comes to 'sensitive data categories' and 'vulnerable groups'.

Cross-border access to data by national authorities	*Art. 9, Rec. 29-30* *Art. 21 (new Art. 15a), Rec.48 (new 42a)*

- **Safeguards for cross-border access to user data are urgently needed.** The existing provisions on national authorities' orders to receive user information and to be proactively notified of suspected crimes risk user privacy and turning services into an arm of state law enforcement.
- **The Parliament moves in the right direction in Art. 21**, clarifying that proactive disclosure requires an 'imminent' threat to life, putting the provision closer to (but still not in complete line with) the Terrorist Content Online regulation.
- We do however caution against provisions in both the Council and Parliament texts that would require proactive notification requirements to be imposed on all hosting services (and not just online platforms), as that could imply proactive scanning of users' private, not publicly disseminated, files.

Access to data: Researchers and 'non-profits'	*Art. 31*

- **We support the Council text**, which adds important safeguards around access to data by researchers. The Parliament text moves in a dangerous direction, by expanding access from researchers to include 'non-profit' organizations, a category so broad it puts user data and privacy and confidentiality of information at risk. The Parliament also appears to allow 'direct access' to systems, putting security and privacy at risk.
- More robust safeguards would require researchers to disclose funding sources; allow online platforms to object to insecure data transmission and set limits on data distribution, in line with the GDPR purpose-limitation principle; and allow online platforms to appeal the vetting of researchers.

Risk assessments	*Art. 26, Rec. 57*

- **We support the Commission and Council texts**. The Parliament significantly expands the risk assessment obligation in ways that could harm innovation in Europe without adding protections for users. We are particularly concerned about the requirements to run risk assessments *before* launching new services and on a Member State level, given their disproportionate nature.
- We urge the Council to ensure that the text does not become overly prescriptive and that the risk assessment obligation remains flexible and future-proof.

Dark patterns and compliance by design	*New Art. 13a in the Parliament text* *New Art. 24b and Rec. 50a in the Council text*

- We support the goal of providing users with clear information and tools to make free and informed choices about the processing of their personal data. We also believe declining consent should be easy for users.
- **However, "dark patterns" is an imprecise term and the current language (in particular in the Parliament's Article 13a) is too broad.** If a ban on "dark patterns" is incorporated into the DSA, the text should specify that the term refers to manipulative design choices that materially distort the behavior of an average user, without however outright banning particular practices which may be justified in some circumstances.
- We also **caution against the broad wording in the Council text on compliance by design for online marketplaces,** and the risk that it could be misinterpreted to ban common features of such services.

Deep fakes	*New Art. 30a in the Parliament text*
● While undoubtedly well-intentioned, the Parliament text on labeling deep fakes presents significant challenges and risks. From a technological perspective, detection and verification systems remain imperfect. This highlights the risks of forcing action. Imprecise definitions could also end up capturing non-deceptive deep fakes, such as art or satire. We therefore caution against inclusion of this provision in the DSA.	
Ancillary features	*Art. 2(h) and Rec. 13*
● **We support the Parliament and Commission texts**, and welcome further clarity on ancillary features. We recommend a flexible approach, in line with the principle of proportionality and the objective to promote innovation in the EU, that would allow features of online platforms that are ancillary to the primary purpose of the platform to be subject to the DSA requirements applicable to hosting services only. We caution against naming specific features of online platforms that could never qualify as ancillary, and rather advocate to allow room for a case-by-case assessment, grounded on the specifics of each service at hand.	