# EFF and Article 19 Comments on the Intermediary Liability Implications of the EU General Data Protection Regulation (GDPR)

## Introduction

The Electronic Frontier Foundation (EFF) and ARTICLE 19 provide our comment on the content removal processes defined under the current draft of the new EU General Data Protection Regulation (GDPR). At the outset, we fully support the adoption of a strong data protection framework in the EU. In the digital age, data protection is vital for the protection of individuals' privacy and personal autonomy. However, we are concerned that in the absence of basic procedural safeguards, the notice-and-delete procedure under the 'right to be forgotten' will have profoundly negative consequences on freedom of expression and citizens' right to access information online. In our view, this problem stems from the fact that the data protection right of erasure was originally designed to deal with personal data held in back-end storage systems and not publicly available, rather than personal data published by *third parties*. This distinction is crucial to understand the need for notice to the person whose content is being de-listed or removed. We are further concerned that the procedure under the GDPR will be used as a substitute for the content removal procedure under the E-Commerce Directive, which, whilst flawed in many respects, contains more safeguards than the GDPR. In any event, the GDPR is unclear on the relationship between both procedures.

These issues have been explored in depth in a series of analyses by Daphne Keller, the Director of Intermediary Liability at the Stanford Center for Internet and Society, to which the reader is referred for more detailed information.[1]

In this comment we analyse the GDPR as against the Manila Principles on Intermediary Liability[2] a set of high level principles developed by over 100 organisations, including EFF and ARTICLE 19, with a view to promote fair content restriction procedures. The Principles are designed to balance the rights of content providers and persons requesting content removal, with the objective of promoting freedom of expression and the right to access information online. When compared with either the recommendations of the Manila Principles, or indeed even with existing intermediary

---

1 See http://cyberlaw.stanford.edu/blog/2015/10/intermediary-liability-and-user-content-under-europe%E2%80%99s-new-data-protection-law, http://cyberlaw.stanford.edu/blog/2015/10/gdpr%E2%80%99s-notice-and-takedown-rules-bad-news-free-expression-not-beyond-repair, and https://cyberlaw.stanford.edu/blog/2015/10/notice-and-takedown-under-gdpr-operational-overview. For comments on the GDPR from a data protection perspective, we refer the reader to a submission of EDRi et al, and we do not endeavor to cover those issues here: EDRi, Access Now, Panoptykon Foundation and Privacy International. *General Data Protection Regulation—Red Lines*. (2015).

2 See https://www.manilaprinciples.org.

liability standards under the European e-Commerce Directive, it will be found that the GDPR falls short of what is needed to provide an adequate legal framework for content restriction that balances the rights and freedoms of the parties and fosters a free and open Internet.

## What the GDPR provides

One of the most troublesome aspects of the GDPR is the harsh yet vague procedure that it institutes for the automatic and immediate restriction of content about an individual by an intermediary, when it receives a request for the restriction of that content by that individual—even if it the content was provided by a third party (Art. 17 in the Parliament version[3]). This conflicts with the Manila Principles, which provide that laws should not require the intermediary to take action on a content restriction order or request until so ordered by an independent and impartial judicial authority. Far from this, under the GDPR, not only is the claim of the party requesting removal not assessed by a judicial authority, but not even by the intermediary themselves, before they required to act on it.

Following its initial restriction, it is then left to the discretion of the intermediary to determine whether the vague conditions in the GDPR Article 17 requiring final erasure of the content are satisfied, and to implement that erasure, in most cases silently and without notice to the content provider. This assessment is made in the shadow of crippling fines in the event that their decision is found to have been mistaken. Intermediaries may reject a request for restriction of the content to protect the "public interest" but there is no clarity about what this means.

Exacerbating this, when a person requests content restriction on the basis of a privacy or data protection complaint, there is no specification of the information that they must provide to document their complaint, such as their name and contact information, the exact location of the content such as a URL, and presumed legal basis for the restriction request. Specifying these details would decrease the number of groundless and bad faith restriction requests received by intermediaries, and establish some clarity about the procedure to be followed before action is taken.

The lack of notice to the content provider, either at the stage of initial restriction or before final erasure, gives them no opportunity to contest the intermediary's decision (contrasting with the general intermediary liability regime established by Article 14(1)(b) of the E-Commerce Directive). To add insult to injury, the intermediary may however be required to disclose the content provider's contact information to the party who requested the removal, resulting in a very lopsided protection of user privacy indeed.

According to the Manila Principles an intermediary should forward a content removal request to the content provider, and in doing so provide a clear and accessible explanation of the content provider's rights, including a description of any available counter-notice or appeal mechanisms. Such mechanisms are a vital safeguard for freedom

---

3 See https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/ 2015/15-07-27_GDPR_Recommendations_Annex_EN.pdf.

of expression in allowing content providers to contest mistaken and abusive notices and have their content reinstated, and they are entirely lacking from the GDPR.

## Conclusion

Although its effects are abbreviated here, enough has been expressed to illustrate that the GDPR as currently expressed poses a significant risk of misuse to stifle free expression online, without due process or review. We therefore recommend that:

1. Even if an *ex ante* judicial order is not required (which would be strongly preferable), at a minimum the GDPR should provide for notice to the content provider and a counter-notice mechanism that allows them to contest a removal request. If the counter-notice were contested by the party requesting removal, a judicial assessment of the claim should then follow.

2. There should not be any requirement for an intermediary to effect an interim restriction of content immediately on receipt of a request, prior to applying the relevant legal standards that would justify permanent restriction.

3. Alongside this, procedures should also be established to standardize the information required in a content restriction request, and provide much more clarity about the standards of assessment that the intermediary is to apply before the law requires them to take action upon an uncontested request.